MTA DOKTORI ÉRTEKEZÉS
TÉZISEI

A KIBERBIZTONSÁG STRATÉGIAI MEGKÖZELÍTÉSE

Kovács László

Budapest
2018

I. A KUTATÁS RÖVID ÖSSZEFOGLALÓJA

A kibertér, illetve az abban lévő szolgáltatások és a digitális alapú folyamatok életünk minden szegmensére kihatással vannak. Ez a hatás igaz a gazdaságra, a politikára, a kultúrára, de a magánéletünk egyes elemeire és az emberek egymáshoz való viszonyára is. Ennek megfelelően a kibertér biztonságával kapcsolatban az egyik legnagyobb kihívást az jelenti, hogy a kibertérben meglévő szolgáltatások és az ezeket lehetővé tevő rendszerek összessége egyre nagyobb függőséget jelent a számunkra. Amennyiben ezek a szolgáltatások és rendszerek akár csak időlegesen is működésképtelenné, vagy elérhetetlenné válnak, akkor azok súlyos fennakadásokat okoznak a mindennapjainkban és az anyagi károkon túl komoly veszélyt jelentenek az emberek életére is.

Mindezek alapján a kibertér és annak biztonsága a fejlett információs infrastruktúrával rendelkező országok számára meghatározó fontosságú, amely a különböző országok kiberbiztonságról való stratégiai elképzeléseiben tükröződik vissza. Azonban a nemzeti kiberbiztonsági stratégiák – legyen szó akár a nagyhatalmakról, akár a kisebb országokról – eltérő válaszokat és megoldásokat sorakoztatnak fel a kibertéri kihívásokra. Mindezek mellett ezek a stratégiák többnyire statikus dokumentumok, amelyek nem, vagy csak részben képesek kezelni azt a dinamizmust, amely a kiberteret jellemzi. Azonban a kibertér jellegéből adódóan, azaz a globalitás, az országhatárok nélküliség, rendkívül gyors technológiai változások, mint legfőbb jellemzők igénylik azt, hogy általános, regionális vagy globális alapértékek mellett egységes modellt határozzunk meg a kiberbiztonsági stratégiák megalkotásához.

A fentiekben megfogalmazottaknak megfelelően *kutatásom fő célja* olyan kiberbiztonsági stratégia modelljének megalkotása, amely tartalmazza azokat a tényezőket, alapvetéseket, amelyek mind nemzetközi, mind nemzeti szinten képesek választ adni a kibertér biztonságát meghatározó kihívásokra a közeli és a távolabbi jövőben egyaránt. A modell megalkotása során a stratégia összetevőire, felépítésére és annak életciklusára fókuszáltam. A fő cél elérése érdekében a következő részcélokat határoztam meg:

- bemutatni és elemezni a digitalizáció társadalmi hatásait és feltárni a kibertérben megjelenő stratégiai veszélyeket és kihívásokat;
- megvizsgálni és elemezni a nemzetközi szakmai szervezetek nemzeti kiberbiztonsági stratégiára elkészítésére, illetve felépítésére tett ajánlásait;

- nemzetközi szövetségek kiberbiztonsági politikáinak és stratégiáinak az elemzése, valamint ezekben az olyan közös elemek azonosítása, amelyek hatással vannak a nemzeti kiberbiztonsági stratégiákra;
- nagyhatalmak – Amerikai Egyesült Államok, Kína, Oroszország – kiberbiztonságról alkotott elképzeléseinek, az elmúlt években a kibertérben megvalósított tevékenységeik elemzése, majd ezekből következtetések levonása;
- összegezni az eddig megvizsgált országok nemzeti biztonsági stratégiáit és nemzeti kiberbiztonsági stratégiáit, ezek alapján az olyan közös elemek azonosítását elvégezni, amelyek a fenti fő cél felé mutatnak, azaz az általános nemzeti kiberbiztonsági stratégia alapjai lehetnek;
- egy elvi stratégiai modell felvázolása, amely alapján egy adott ország nemzeti kiberbiztonsági stratégiája elkészíthető és a folyamatos technikai, gazdasági, társadalmi változásoktól függetlenül fenntartható;
- a nemzeti kiberbiztonsági stratégia végrehajtása érdekében egy általános akcióterv elvi alapjainak a kidolgozása;
- egy olyan mérőrendszer elvi alapjainak és összetevőinek (indikátorainak) a kidolgozása, amely alapján a nemzeti kiberbiztonsági stratégia és annak végrehajtásának hatékonysága mérhetővé válik.

Természetszerűleg a kutatásaim eddigi eredményei nagymértékben befolyásolták azokat a kutatási irányokat, amelyek a kibertér különböző területeinek vizsgálatai során követtem. E munka során az alapvető irodalmi források feldolgozásán túl a hazai nemzeti kiberbiztonsági stratégia módosításában vettem részt, mint véleményező. Ezen kívül az Európai Unió Horizont 2020 kutatás-fejlesztési programja egyes alprogramjai szakértőjeként az Európai Bizottság meghívására személyesen a gyakorlatban, közvetlen közelről tanulmányozhattam számos olyan területet, amely értekezésem viszonyában is releváns.

II. AZ ELVÉGZETT KUTATÁSOK

Az értekezésemben összefoglaltam mindazokat a kutatási eredményeimet, amelyeket az elmúlt években a kiberbiztonság különböző részterületein végeztem. Emellett az értekezésben megfogalmazottak nagyban építenek a 2018-ban megjelent, általam 2017-ben és 2018-ban írt két monográfiára – *A kibertér védelme*, valamint a *Kiberbiztonság és -stratégia* –, amelyekben az addigi kutatásaim eredményeire építve igyekeztem bemutatni tudományos igénnyel, de mégis közérthető módon a kibertér egyes területeit.

Az értekezés *1. fejezetében* összefoglaltam a kibertér meghatározásának problémáit és tudományos értelemben vett nehézségeit. A kibertér biztonságának növelése kiemelten fontos a társadalom egésze számára nemzeti és nemzetközi szinten egyaránt. Ennek megfelelően meghatároztam a kiberbiztonság és annak kapcsolódó fogalmait a dolgozat vonatkozásában. Korábbi kutatásaim alapján már megállapítottam, hogy a kiberteret alkotó különböző technológiákra alapuló eszközök, rendszerek és szolgáltatások között a határok eltűnnek. Így létrejött az úgynevezett digitális ökoszisztéma, amely az IKT (infokommunikációs technológia) révén hálózatba kapcsolja a felhasználókat, és a hálózatok segítségével biztosítja a társadalom tagjai számára az egyre inkább alapvetővé váló digitális szolgáltatásokat. Megvizsgáltam, hogy milyen módszerek léteznek a digitális ökoszisztéma mérésére, amellyel arra is választ kerestem, hogy ezek a módszerek alkalmasak-e a kiberbiztonság helyzetének megítélésére, vagy mérésére. Az említett digitális szolgáltatások ma már azonban függőséget is jelentenek, így azok biztonsága elemi érdek. Feltártam azokat a tényezőket, amelyek stratégiai szintű veszélyként illetve kihívásként jelentkezhetnek ma és a közeljövőben. Olyan veszélyeket azonosítottam, mint például a kiberhadviselés, a kiberfegyverek terjedése, a kibertérben történő politikai befolyásolás vagy a kiberbűnözés. Ezek után megvizsgáltam azokat a stratégiai védelmi megoldásokat, amelyek a kiberbiztonság megteremtése érdekében a feltárt veszélyek kezelésére alkalmasak lehetnek.

A *2. fejezetben* megvizsgáltam három nagyhatalom – Kína, Oroszország és az Amerikai Egyesült Államok – nemzeti szintű biztonsági, katonai és kibertérrel kapcsolatos stratégiáit. Ezek alapján megállapítottam, hogy mind a három nagyhatlom eltérő módon közelíti meg a kiberteret. Ugyanakkor az elvégzett elemzéseim alapján azt a következtetést vontam le, hogy a nagyhatalmak is a nemzeti biztonságuk alapvető összetevőjeként

tekintenek a kibertérre és annak biztonságára. Mindezeken túl a kibertérben folytatott információszerző, befolyásoló és támadó tevékenységükkel, illetve e tevékenységekkel kapcsolatos képességeikkel a nemzetközi biztonsági, gazdasági és politikai viszonyrendszerben is számolnak.

Ebben a fejezetben megvizsgáltam továbbá az Európai Unió és a NATO, valamint 10 európai uniós ország – Ausztria, Csehország, Egyesült Királyság, Észtország, Franciaország, Hollandia, Magyarország, Lengyelország, Németország, Szlovákia – nemzeti biztonsági stratégiáit és nemzeti kiberbiztonsági stratégiáit. Ezekből a vizsgálatokból levont következtetések alapján megállapítottam, hogy bár ezek az országok is eltérő módon közelítik meg a kibertér biztonságát, de annak stratégiai megközelítésében számos olyan elem azonosítható, amelyek nagyban hasonlítanak egymásra. Megállapítottam, hogy ezek az azonos elemek, függően azok szerepétől és azok hatékonyságától, alapjai lehetnek egy nemzeti kiberbiztonsági stratégia modelljének.

A *3. fejezetben* megvizsgáltam a nemzeti kiberbiztonsági stratégia kialakítására és felépítésére vonatkozó – elsősorban nemzetközi – tanulmányokat, amelyek kiindulási alapot nyújthatnak egy egységes kiberbiztonsági stratégia modelljének elkészítéséhez. Ezek legfontosabb elemeit szintetizáltan jelenítettem meg a dolgozatban. A kiberbiztonság vonatkozásában megvizsgált nagyhatalmak – Kína, Oroszország, Egyesült Államok –, a NATO és az Európai Unió, valamint az EU egyes tagországainak nemzeti biztonsági és nemzeti kiberbiztonsági stratégiái alapján olyan szintetizált következtetések levonása lehetséges, amelyek alapjául szolgálhatnak a kutatási céljaim között szereplő általános érvényű nemzeti kiberbiztonsági stratégia modelljének felállításához.

A fejezet további részeiben javaslatokat fogalmaztam meg a nemzeti kiberbiztonsági stratégia modelljére, amelyben annak összetevőire és elemeire külön meghatározásokat adtam. Szintén javaslatot tettem a stratégia életciklusára és az abban megvalósítandó különböző feladatokra. Ezeken kívül meghatároztam a kiberbiztonsági stratégia végrehajtásához szükséges akcióterv elemeit, majd egy olyan indikátor-rendszerre tettem javaslatot, amelyekkel az akciótervben foglaltak, közvetetett módon pedig a kiberbiztonsági stratégia végrehajtásának hatékonysága válik mérhetővé.

III. A TUDOMÁNYOS EREDMÉNYEK ÖSSZEFOGLALÁSA

A korábbi kutatásaimra, valamint az értekezésemben megfogalmazott szintetizált következtetésekre építve a következő tudományos eredményekkel, valamint az azokban megfogalmazott javaslatokkal kívánok a kiberbiztonság stratégiai szintű növeléséhez hozzájárulni:

1. A kutatómunkám során elemzett nemzeti kiberbiztonsági stratégiák és politikák alapján **kidolgoztam és javaslatot tettem egy általános érvényű nemzeti kiberbiztonsági stratégia modelljére**. Ezen belül **azonosítottam azokat a tartalmi elemeket**, amelyek egy hatékony nemzeti kiberbiztonsági stratégia kialakítása során szükségesek.

   Javaslatom alapján a nemzeti kiberbiztonsági stratégia a következő elemeket kell, hogy tartalmazza:

   - terminológiai gyűjtemény, amelyben a kibertér, valamint a kiberbiztonság meghatározása is megtörténik;
   - stratégiai környezet értékelése: a kibertéri veszélyek és kihívások bemutatása, illetve azok rövid stratégiai szempontú értékelése;
   - olyan stratégiai célok meghatározása, amelyek a kiberbiztonság megteremtése és folyamatos emelése révén a nemzeti biztonsági stratégiai célok eléréséhez hozzájárulnak;
   - a kiberbiztonság szervezeti hátterének megvalósítására vonatkozó stratégiai elképzelések;
   - a kritikus információs infrastruktúrákra és ezáltal a kritikus infrastruktúrák védelmére vonatkozó meghatározások;
   - kiberbiztonsággal kapcsolatos kutatás-fejlesztés-innováció stratégiai támogatása;
   - a kiberbiztonság oktatásának stratégiája, amely a kiberbiztonsági tudatosság fejlesztését, illetve növelését is célozza;
   - a köz- és a magánszféra kiberbiztonság területén történő szoros és kölcsönös együttműködésének (PPP) stratégiai ösztönzése;
   - a nemzetközi kiberbiztonsági együttműködés iránti elkötelezettség deklarálása;
   - a stratégiai célok elérése érdekében történő akcióterv elkészítésének meghatározása;

- értékelési rendszer kidolgozása, amely egyrészt a stratégiában, másrészt az akciótervben megfogalmazottak végrehajtásának ellenőrzéséhez ad mutatókat.

Mindezek mellett, nem általános érvényű elemként, de fontos hangsúlyozni, hogy az adott ország politikai döntésétől függően a hadsereg szerepe az ország kibervédelmében célszerűen megjelenítendő. Ez a következő kérdésekre (területekre és a hozzá kapcsolódó célokra) irányulhat:

- a hadsereg kiberműveleti képességeinek kialakítása, beleértve a kibertámadó képességeket is;
- a hadsereg feladatai az adott ország kibervédelmében és esetlegesen a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmében;
- a hadsereg feladatai egy, az adott országot érő kibertámadás során, amely akár válaszcsapás kialakítását is jelentheti;
- a hadsereg kiberműveleti képességei – a megfelelően robosztus állami kibervédelmi szervezetekkel és azok kibervédelmi képességeivel együtt – elrettentést jelentenek.

A fentieknek megfelelően a javasolt modell tartalmazza a kibertámadási képességekre vonatkozó meghatározást is. A hatékony kiberbiztonsági stratégiához szükséges, hogy az adott ország – nyilvánvalóan politikai döntéstől, illetve az adott ország alkotmányától függően – kialakítsa és rendelkezzen azokkal a kiberreagálási képességekkel, amelyek nem csak a támadások elhárítását, hanem az azokra adandó proaktív válaszokat, a korai előrejelzés képességét és akár a megelőző támadásokat is magába foglalják a potenciális támadókkal szemben (itt elsősorban az állami támogatású, a stratégiai fontosságú infrastruktúrákat célzó támadások elleni tevékenységek jelennek meg célként). Ezek a képességek befolyásolják, nagymértékben lerontják vagy megakadályozzák a szembenálló felet a támadások kivitelezésében, illetve abbéli képességeikben. A támadó képességek az elrettentés célját is szolgálják.

2. Kidolgoztam és javaslatot tettem a **nemzeti kiberbiztonsági stratégia életciklusára**.

Ennek az életciklusnak a fázisaira és az azokban szükséges tevékenységre a következőket határoztam meg:

1. fázis: Az új stratégia megalkotása/régi stratégia módosítása:

- A stratégia általános céljának meghatározása, szükség esetén annak felülvizsgálata.
- A stratégiai célok meghatározása, azok pontosítása.
- Az érdekelt felek körének azonosítása, szükség szerinti felülvizsgálata, új szereplők szükség szerinti bevonása.
- A meglévő szakpolitikák, szabályzók felülvizsgálata és az ezek végrehajtásához szükséges képességek meghatározása.
- Nemzeti szintű kockázatértékelési és kockázatkezelési módszertan kialakítása és meghatározása.
- A kritikus információs infrastruktúrák védelmének növelése és interdependenciájuk felmérése.
- Az információmegosztási mechanizmusok felülvizsgálata, szükség esetén azok meghatározása vagy átalakítása.
- A kiberbiztonság növelése érdekében szükséges biztonsági követelmények megállapítása.

Az 1. fázishoz tartozó visszacsatolás: a stratégia frissítése

- Hazai és nemzetközi érdekelt felek azonosítása és bevonása.
- Nemzeti szintű kockázatelemzés elkészítése.
- Jogszabályi megfelelőség vizsgálat.

2. fázis: Az új stratégia bevezetése és végrehajtása (korábbi stratégia szükség szerinti módosítása)

- Átlátható és a feladatokban/jogosultságokban egymást jelentősen nem átfedő irányítási és szervezeti struktúra kialakítása, illetve a felülvizsgálat eredményeként annak esetleges átalakítása.
- Kiberbiztonsági vészhelyzetkezelési tervek kidolgozása, pontosítása.
- A kiberbiztonságra vonatkozó értékelési séma (rendszer) kidolgozása, bevezetése és alkalmazása.
- A fő teljesítménymutatók (KPI) rendszerének kidolgozása.
- Incidenskezelési képességek kialakítása, fejlesztése.
- Kiberincidensek jelentési mechanizmusainak pontosítása.
- A kiberterületen folytatott K+F-tevékenység ösztönzőrendszerének kidolgozása, bevezetése, növelése.

- A kiberbűnözés elleni hatékony fellépés és tevékenység fokozása hazai és nemzetközi területen egyaránt.
- A kiberbiztonság területén nemzetközi együttműködésekben való aktív részvétel.
- A köz- és magánszféra közötti partnerség kialakítása.
- A közszféra intézményei közötti együttműködés hatékonyságának növelése.
- A magánszektor kiberbiztonsági területekbe való befektetésének ösztönzése.

A 2. fázishoz tartozó visszacsatolás: a cselekvési tervek frissítése

- Akcióterv készítése (módosítása):
  - szervezeti háttér módosítása.
  - technikai kihívások kezelése;
  - mérési eredmények alapján a fókuszterületek finomhangolása.

3. fázis: Az új (módosított) stratégia alapján történő kiberbiztonsági rendszer működtetése

- Kiberbiztonsági gyakorlatok megszervezése.
- A kiberképzési és -oktatási programok bevezetése és ösztönzése.
- Az állampolgárok kiberbiztonsági tudatosságának növelése.

A 3. fázishoz tartozó visszacsatolás: időszakos / rendszeres felülvizsgálat

- Kiberbiztonsági mérések a következő területeken:
  - a biztonság változása;
  - szervezeti hatékonyság;
  - hazai és nemzetközi együttműködés hatékonyság;
  - K+F helyzet és hatékonyság.

4. fázis: A stratégia, illetve annak hatékonyságának értékelése

- A stratégia folyamatos fejlesztése.
- A nemzeti kiberbiztonsági stratégia finomhangolása a főbb teljesítménymutatók eredményeinek felhasználásával.

- A kibergyakorlatok során megszerzett tapasztalatok feldolgozása és ezek alapján hatékonyságnövelő intézkedések kidolgozása.

A 4. fázishoz tartozó visszacsatolás: folyamatos fejlesztés

- Változáskövetés valamint az új veszélyek és kihívások azonosítása:
  - biztonságpolitikában;
  - gazdaságban;
  - IKT-ban;
  - társadalmi/digitális ökoszisztémában.

3. **Kidolgoztam és javaslatot** tettem a nemzeti kiberbiztonsági stratégia végrehajtása érdekében szükséges **akcióterv tartalmi elemeire**.

A nemzeti kiberbiztonsági stratégia végrehajtása érdekében egy akciótervet szükséges meghatározni, amely a stratégiában megfogalmazott stratégiai célok végrehajtását operatív szinten, kézzelfogható feladatok elrendelésével támogatják. Az akciótervben megfogalmazott feladatokhoz felelős szervezeteket kell kijelölni, és meg kell határozni az adott feladat végrehajtásának határidejét. Fontos a feladatok közötti átfedések minimális szintre csökkentése, ugyanakkor a feladatok – stratégiai célok irányába történő – maximális hatásának elérése érdekében szükséges a feladatok összehangolása és koordinálása. Ehhez ki kell jelölni egy vezető szervezetet, amely szervezet megfelelő politikai-, gazdasági- és humánerőforrás birtokában van, illetve ezek a számára biztosíthatók.

Mindezeknek megfelelően a nemzeti kiberbiztonsági stratégia céljainak elérése és ez által a kiberbiztonság szintjének növelése érdekében megfogalmazott akciótervnek javaslatom szerint a következő elemekből kell állnia:

- a stratégiai célok végrehajtása érdekében minden célhoz felelős kormányzati szervezetet – például minisztériumot, központi ügynökséget, hivatalt stb. – kell hozzárendelni;
- a stratégiai célokat részcélokra kell osztani;
- mind a stratégiai célok, mind a részcélok esetében meg kell határozni a végrehajtás határidejét;
- a célok és részcélok elérése érdekében tevékenységeket (akciókat/feladatokat) kell azok mellé rendelni;
- a feladatok mellé anyagi erőforrásokat kell hozzárendelni;

- a feladatok végrehajtása érdekében humán erőforrásokat kell azokhoz rendelni;
- a célokhoz olyan mutatókat kell hozzárendelni, amelyekkel mérhető a célok elérése, illetve azoknak a tevékenységeknek a hatékonysága, amelyek ezen célok elérése érdekében meghatározásra kerültek;
- a végrehajtás hatékonysága mérésére alkalmazott mutatókat elemezni kell, majd az elemzések függvényében a stratégia egyes pontjai számára visszajelzéseket kell adni a finomhangolás vagy az esetleges nagyobb stratégiai korrekció végrehajtása érdekében.

4. **Kidolgoztam** és javaslatot tettem a nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló **indikátor-rendszerre és annak mutatóira**.

Az eddigi kutatásaim eredményeinek összefoglalása révén az értekezésemben megfogalmazott javaslatok, amelyeket a nemzeti kiberbiztonsági stratégia elvi alapjaira és annak életciklusára, valamint a stratégia végrehajtása érdekében javasolt akciótervre tettem hozzájárulnak egy ország kiberbiztonsági szintjének emeléséhez. Azonban ennek a biztonsági szintnek az emelkedését (változását) szükséges folyamatosan figyelemmel kísérni és mérni, ahogy azt az általam javasolt kiberbiztonsági stratégia életciklusának 4. fázisa is tartalmazza. Ehhez a méréshez szükség van egy indikátor-rendszerre, amely a különböző célok eléréséhez rendelt feladatok hatékonyságát különböző mutatók (indikátorok) segítségével értékeli. A nemzeti kiberbiztonsági stratégia célja nyilvánvalóan a kiberbiztonság, így a nemzeti biztonság emelése és annak növelése. Ugyanakkor sok esetben ennek egyes területein bekövetkezett változások jelenleg csak becsléssel, vagy rosszabb esetben szubjektív véleménnyel ítélhetők meg.

Mindezek alapján javaslatot tettem a nemzeti kiberbiztonsági stratégia végrehajtása hatékonyságának mérésére szolgáló indikátor-rendszer elvi alapjaira, amely a következő fő célterületeket foglalja magába:

- a nemzeti kiberbiztonsági stratégia felülvizsgálata:
  - megtörtént-e;
  - van-e ehhez központi koordináló szervezet hozzárendelve és ehhez tartozik-e meghatározott eljárásrend;

  - stratégiai célok építenek-e a nemzeti biztonsági stratégia céljaira;
  - akcióterv hozzárendelésre került-e (célok, részcélok, felelősök, határidők);
  - nemzetközi követelmények beépítésre kerültek-e;
- a kiberbiztonság szervezeti háttere és annak képességei:
  - korai kiberveszély előrejelzést és elemzést végző szervezet és/vagy képesség megvan-e;
  - központi incidenskezelési szervezet megléte;
  - ágazati incidenskezelő szervezetek megléte;
  - az incidens kezelés átlagos ideje;
  - együttműködés hatékonysága: például az ágazati szinten bejelentett központi incidenskezelést igénylő esetekben ez mennyire valósul meg;
- kibertéri kockázatok és veszélyek felmérése:
  - nemzeti kockázatelemzési metódus megléte;
  - a nem kezelt súlyos kockázatok aránya;
- kritikus infrastruktúra védelem feladatai:
  - központi incidenskezelés megvalósul-e;
  - ágazati incidenskezelő szervezetek kialakultak-e;
  - információs rendszer (sérülékenységekre figyelmeztető, tudatosító) működik-e;
  - az EU CIWIN hálózatban résztvevő kritikus infrastruktúra elemek száma;
  - sérülékenységek számának változása;
  - incidensek számának változása;
  - kritikus infrastruktúra IKT rendszereinek kiberbiztonsági megfelelőségi aránya;
- kiberbűnözés:
  - van-e a kiberbűncselekmények nyilvántartására központi adatbázis;
  - kiberbűncselekmények száma, illetve azok számának és/vagy súlyosságának változása;
  - jogi eljárás alá vont kiberbűncselekmények száma;
  - a kiberbűncselekményekkel szakmailag foglalkozó rendőri erők létszáma;
  - a kiberbűncselekményekkel szakmailag foglalkozó rendőri erők szakmai továbbképzéseinek száma;
  - a kiberbűncselekményekkel szakmailag foglalkozó bírók és ügyészek szakmai továbbképzéseinek száma;

- a hadsereg kiberműveleti kompetenciái:
    - a hadsereg kiberműveleti képességeihez szükséges szakemberek számának változása, beleértve az incidenskezeléshez, valamint a kibertámadó képességekhez szükséges szakembereket is;
    - a hadsereg kibertámadó képességeinek változása;
    - a hadsereg információs és vezetési rendszereit ért súlyos incidensek számának változása;
- kiberbiztonsági gyakorlatok:
    - hazai kiberbiztonsági gyakorlatok száma;
    - nemzetközi kiberbiztonsági gyakorlatok száma;
    - kiberbiztonsági versenyek száma;
- oktatás-képzés, tudatosítás:
    - a társadalom azon aránya, aki szerint biztonságos az IKT eszközök használata;
    - új, egyetemi szintű képzések száma;
    - új, a közoktatásba bevont kiberbiztonsági ismeretkörök száma;
    - továbbképzések száma a közigazgatás szereplői számára;
    - tudatosító kampányok száma;
- K+F tevékenység:
    - új, az IKT szektor biztonságával foglalkozó KKV-k száma;
    - elnyert nemzetközi források száma és összege;
    - hazai ösztönzőrendszer megléte és annak hatékonysága;
    - a közigazgatási IKT rendszerek fejlesztése során a kiberbiztonsági elemek megjelenése;
- nemzetközi együttműködés:
    - új bilaterális együttműködések száma;
    - új multilaterális együttműködések száma;
    - nemzetközi kiberbiztonsági fórumokban való részvétel.

IV. AZ ÉRTEKEZÉS TÉMÁJÁBAN SZÜLETETT FONTOSABB TUDOMÁNYOS PUBLIKÁCIÓIM JEGYZÉKE

Monográfia, könyv

Kovács László (2018): *Kiberbiztonság és -stratégia*. Budapest: Dialóg Campus Kiadó; Nordex Kft., 350 p. ISBN 978-615-5920-93-6

Kovács László (2018): *A kibertér védelme*. Budapest: Dialóg Campus Kiadó; Nordex Kft., 354 p. ISBN 978-615-5889-63-9

Haig Zsolt, Kovács László, Ványa László, Vass Sándor, Németh András (szerk.) (2014): *Elektronikai hadviselés*. Budapest: Nemzeti Közszolgálati Egyetem, 271 p. ISBN 978-615-5305-87-0

Haig Zsolt, Kovács László, Munk Sándor, Ványa László, [Kovács László, Tózsa István (szerk.)] (2013): *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest: Nemzeti Közszolgálati Egyetem, 173 p. ISBN 978-615-5305-02-3

Könyvfejezet / Szerkesztett könyvben cikk

Kovács László (2014): *Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései*. In: Nemeslaki András (szerk.) E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek. 353 p. Budapest: Nemzeti Közszolgálati Egyetem, pp. 227-248.

Kovács László (2013): *Cyber challenges to the armed forces.* In: Marek Kulczkycki (szerk.) Armed Forces in the system of international security. 223 p. Wrocław: Wroclaw University Press, pp. 157-173. ISBN 978-83-63900-52-6

Haig Zsolt, Kovács László (2008): Energiaellátó rendszerek rendszerirányítása: 3.7.4. fejezet. In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 51-75. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Internet Magyarországon: 3.7.5. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve:*

Informatikai biztonsági tanácsadó A-Z. Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 77-100. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Védelmi szféra infrastruktúrák: 3.7.6. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 101-136. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): A vezetékes távközlő rendszerek áttekintése: 5.3.3 fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-5. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): A mobil cellás rádiótelefon rendszerek áttekintése és néhány gyakorlati alkalmazás: 5.3.4 fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-22. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Kritikus információs infrastruktúrák elleni fenyegetések: 3.7.7. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 137-148. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Kritikus információs infrastruktúrák védelme: 3.7.8. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 149-170. ISBN 963 9313 12 2

Haig Zsolt, Kovács László (2008): Műholdas távközlési rendszerek: 5.3.5. fejezet In: Szenes Katalin (szerk.) *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-Z.* Budapest: Verlag Dashöfer Szakkiadó Kft, 2008. pp. 1-8. ISBN 963 9313 12 2

Nemzetközi folyóiratcikk

Kovács László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre / Land Forces Academy Review*, XXIII. 1 (89) pp. 16-24.

Kovács László (2018): National Cyber Security as the Cornerstone of National Security. *Revista Academiei Fortelor Terestre / Land Forces Academy Review*, XXIII. 2. (90) pp. 113-120.

Kovács László (2018): Comparative Study on Digital Economy and Society of Austria and the Visegrad Countries. *Economics and Management,* 2017. 2. pp. 36-47.

Haig Zsolt, Kovács László (2007): New Way of Terrorism: Internet- and cyber-terrorism. *Military Technical Academy Review*, 17. 2. pp. 125-137.

chnical Academy Review, 17. 2. pp. 125-137.

Hazai folyóiratcikk

Kovács László, Krasznay Csaba (2017): Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Stratégiai Védelmi Kutató Központ (Elemzések) / Center for Strategic and Defense Studies Analyses*, 2017. 9. pp. 1-11.

Kovács László, Krasznay Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2017. 1. pp. 3-16.

László Kovács, András Nemeslaki, Ákos Orbók, András Szabó (2017): Structuration Theory and Strategic Alignment in Information Security Management: a Comprehensive Research Approach and Program. *Academic and Applied Research In Military And Public Management Science*, 16. 1. pp. 5-16.

Nagyné Takács Veronika, Kovács László (2015): Az információbiztonság vezető szakirányú továbbképzés tapasztalatai. *Pro Publico Bono: Magyar Közigazgatás*, 2015. 4. pp. 85-99.

Kovács László (2012): Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I. *Hadmérnök*, VII. 2. pp. 302-311.

Haig Zsolt, Kovács László, Ványa László (2011): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle*, 10. évf. 1-2.sz. pp. 183-209.

Kovács László, Illési Zsolt (2011): Cyberhadviselés. *Hadtudomány*. XXI. 1-2. pp. 29-41.

Kovács László, Sipos Marianna (2011): A Stuxnet és ami mögötte van II.: Célok és teendők. *Hadmérnök*, VI. 1. pp. 222-231.

Kovács László (2011): Kiberháború? Internetes támadások a Wikileaks ellen és mellett. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2011. 1. pp. 3-8.

Kovács László, Krasznay Csaba (2010): Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2010. 1. pp. 44-56.

Kovács László, Sipos Marianna (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* V. 4. pp. 163-172.

Kovács László (2009): Electronic warfare and the asymmetric challenges. *Bolyai Szemle*, 2009. 3. pp. 135-151.

Kovács László (2009): Információs hadviselés kínai módra. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 2. 7. pp. 35-44.

Kovács László (2009): Obama's new cybersecurity policy. *Hadtudományi Szemle,* 2. 3. pp. 15-20.

Haig Zsolt, Kovács László (2008): Fenyegetések a cybertérből. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* 1. 5. pp.

Kovács László (2008): Az információs terrorizmus elleni tevékenység kormányzati feladatai. *Hadmérnök*, 2008. 2. pp. 138-148.

Kovács László (2008): Kritikus információs infrastruktúrák Magyarországon. *Hadmérnök*, 2007. (Különszám) pp. 1-20 p.

Kovács László (2007): Az információs terrorizmus eszköztára. *Hadmérnök*, 2007. 1. pp. 1-18.

Konferencia kiadványban megjelent cikk

Kovács László (2013): Cyberterrorizmus: valós vagy túldimenzionált veszély? *Magyar Rendészet,* XIII. (különszám) pp. 85-93.

Tanulmány

Kovács László, Szentgáli Gergely (2015): *National Cyber Security Organisation: Hungary*. NATO CCDCOE, Észtország, pp. 1-14.

Haig Zsolt, Kovács László, Ványa László (szerk.) (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Tanulmány. Budapest: Nemzeti Közszolgálati Egyetem, 2012. 298 p.

Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nándor (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana*. Budapest: ENO Advisory Kft. 198 p.

Budapest, 2018. november 21.