NEMZETI KÖZSZOLGÁLATI EGYETEM

KATONAI MŰSZAKI DOKTORI ISKOLA

Szerzői ismertető

Papp Zoltán István

A KIBERTERRORIZMUS MÓDSZEREI, LEHETSÉGES ESZKÖZEI ÉS AZ EZEK ELLEN TÖRTÉNŐ VÉDEKEZÉS ALTERNATÍVÁI

című doktori (PhD) értekezéséhez

Témavezető:

Prof. Dr. Kovács László mk. ezredes Ph.D.
egyetemi tanár

Budapest, 2018.

A tudományos probléma megfogalmazása

Az információs társadalom magas szintű működésében az információs infrastruktúrákra kiemelt szerep hárul, és e fontosságból adódóan változatos módszerekkel végrehajtott rosszindulatú és ártó tevékenység fókuszába is kerülnek, melyek mögött különböző támadók sokszínű motivációi húzódnak meg. Azonban legveszélyesebb jelenségként ezek köréből a kiberterrorizmus emelhető ki, mivel – a „hagyományos" terrorizmussal összhangban – ennek repertoárjában jelenik meg a legtöbb eszköz és módszer, továbbá a kibertér által nyújtott lehetőségek a kiberterroristákat a jogellenes cselekményeikben a földrajzi tértől függetleníti és nagyfokú anonimitást is képes számukra nyújtani.

Az információs infrastruktúrákat különböző célok elérése érdekében, különböző indokokra hivatkozva támadhatják őket kifejezetten e célra létrehozott – adott ország szövetségi rendszerén kívüli – állami szervek, szervezetek (katonai alakulatok, hírszerző szolgálatok), melyek tevékenységüket professzionális céleszközökkel valósítják meg. E körbe tartozó támadó jellegű tevékenységek hatásfokát nagyban növeli az a körülmény, hogy az állami szerveknek a céleszközök beszerzésére, tervezésére, fejlesztésére gyakorlatilag korlátlan humán- és anyagi erőforrások állnak rendelkezésükre, sok esetben műszaki, technológiai és személyi háttéradatbázisokkal is rendelkeznek. További hatásfokot növelő tényező, hogy az állam olyan jogszabályi és alkalmazási környezetet tud teremteni, melyek ez irányú tevékenységüket támogatják.

Azonban fenyegetések nem csak ellenérdekelt országok szervezeteinek irányából érkezhetnek, mert az információs infrastruktúrát kibertérben működő terrorcsoportok mellett más személyek, irreguláris szervezetek is megközelíthetik rosszindulatúan, jogellenes módon azzal a szándékkal, hogy annak szolgáltatásait akadályozzák, az abban tárolt információkat megszerezzék, megsemmisítsék, manipulálják.

A támadótevékenységet, azon túl, hogy a jogszabályi környezet büntetni rendeli, az is nehezíti, hogy a potenciális elkövetők számára a megfelelő professzionális céleszközök legtöbb esetben haditechnikai eszközöknek minősülnek, így beszerzésük – a nagy anyagi ráfordításon túl – gyakorlatilag meg sem valósítható. Ugyanakkor az elkövetőknek motiváltságuk mélységétől függően jogi és erkölcsi aggályai is egyre kevésbe vannak, így nem veszik figyelembe a jogszabályok tiltásait, tettük büntetőjogi következményeivel érdemben nem számolnak, így az információs infrastruktúrák elleni jogellenes cselekményt a

birtokukba lévő információkkal, a rendelkezésükre álló eszközökkel – céljaik elérése érdekében – mindenképpen végrehajtják.
A potenciális elkövetőket számos körülmény segíti, hiszen az információs társadalom által használt információs rendszerekben – kisebb-nagyobb mértékű idő- és pénz ráfordításával – elérhető információtömeg, szolgáltatás és egyéb más lehetőség mind-mind felhasználható. Egyrészt az információs infrastruktúrákat nem csak a bennük tárolt információk tartalma által támadhatók, hanem más egyéb jellemző, paraméter által is, másrészt pedig érdemi és hasznos információkat szerezhetnek meg az érintett infrastruktúráról, a beépített berendezésekről, az alkalmazott technológiákról az ott foglalkoztatott személyekről. Az előzőeken túl megnyerhetnek ügyüknek szimpatizánsokat, megteremthetik anyagi lehetőségeiket is, de megszerezhetik azokat az ismereteket is, elsajátíthatják azokat a módszereket, melyek egy sikeres támadáshoz elengedhetetlenek.

A jogellenes cselekményeket továbbá az is segíti, hogy számos olyan fizikai hatáson alapuló és logikai eszköz és módszer áll rendelkezésre, melyek birtokában az információs infrastruktúrák működésébe bele lehet avatkozni. A fizikai hatáson alapuló eszközök egy részének kereskedelme, birtoklása jogszabályokba ütközik, ám számos közülük kereskedelmi forgalomban elérhető alkatrészekből megalkotható, vagy épp kereskedelmi forgalomban kapható más berendezések átalakítása révén kiváltható.
A logikai eszközök (támadókódok) tekintetében, a fizikai hatáson alapuló eszközökhöz képest az információs infrastruktúra támadói könnyebb helyzetben vannak. A végrehajtás eszköze, a számítógép mindenki számára elérhető, e kategóriába tartozó logikai eszközök létezése a fizikai térben nem érzékelhető, birtoklásuk gyakorlatilag ellenőrizhetetlen, bár megalkotásukhoz mélyreható szakismeretre van szükség, azonban alkalmazásukra már közel sem. Számos program már „alkalmazásra kész” formában elérhető, és már csak a célpont meghatározására van szükség, de a különböző toolkit-ekből összeállítható támadókódok és egyéb elérhető, megvásárolható sérülékenységek is komoly fenyegetést jelenthetnek az információs infrastruktúrákra.

Tekintettel az információs infrastruktúráknak az információs társadalomban betöltött szerepére, folyamatosan biztosítani kell az információk megszerzését, áramlását és felhasználását, illetve e műveleteket végző rendszerek, berendezések és átviteli csatornák folyamatos rendelkezésre állását, valamint ezek háttérfeltételeit. Azonban a folyamatosságra,

az üzembiztonságra, illetve az általánosságban értendő biztonságra számos – az üzemeltetők által befolyásolható, vagy épp nem befolyásolható – körülmény van kihatással.
Az információs infrastruktúrák védelmét nehezíti az is, hogy számos olyan körülmény létezik, melyről konkrét megjelenéséig vagy nem is tudnak, vagy bekövetkeztével érdemben nem számolnak, vagy épp az infrastruktúra megalkotásakor még nem is létezett. Ezért a védelmi intézkedések kidolgozásakor, a védelmi alrendszerek tervezésekor a lehető legmesszebbmenőkig előrelátva a biztonsági szakterületek mindegyikének vonatkozásában meg kell jósolni a várható veszélyeket, fenyegetéseket, melynek elengedhetetlen feltétele a jelenlegi állapotok ismerete, a várható tendenciák helyes prognosztizálása.

A biztonság fenntartása mind a fizikai, mind pedig a kibertérben kihívást jelent. A biztonságot befolyásoló körülmények rendkívül összetettek. Lehetnek belső és külső körülmények, melyeknek állapota kihatással van az információs infrastruktúra biztonsági helyzetére, de lehet egy, a külső és belső körülmények együtthatásának eredője is olyan jelenség, mely negatívan hat ki a biztonságra.

Azonban az infrastruktúrák biztonságos működése nem csak az üzemeltetők érdeke, hanem az információs társadalom tagjait képviselő államé is, így e területen az illetékes szervekre, szervezetekre és hatóságokra is feladat hárul. A védelem területén az érintettek már együttműködnek, együttműködni kényszerülnek, azonban a felek eltérő érdekei, lehetőségei – illetve azok hiánya miatt – nem az ideális állapot gyors kialakulásának irányába hatnak.

Fentiek tükrében a tudomány eszközire van szükség annak érdekében, hogy azonosítsuk a fenti tényezők együttes összefüggéseit, kölcsönhatásait. Tudományos kutatást igényel az, hogy az információs társadalom tagjai milyen feltételek, hatások mellett léphetnek a kiberterrorizmus útjára, ekkor az információs infrastruktúrákban kezelt információ mely tulajdonságait, milyen módszerekkel és eszközökkel támadhatják, valamint azt is vizsgálni kell, hogy az infrastruktúra üzemeltetőinek, illetve az államnak milyen lehetőségei, új módszerei lehetnek a védekezésben, valamint vannak-e olyan körülmények, melyek a biztonság ellen hatnak.

Hipotézisek

Az információs infrastruktúrákban kezelt, általánosságban értelmezett információnak, vagy ezen információnak a feldolgozásához kapcsolódó, ideiglenesen létező egyéb információknak a tartalmán túl vannak olyan egyéb minőségi jellemzői, tulajdonságai, melyek manipulálása révén a kiberterrorizmus akadályozni tudja az infrastruktúrák rendeltetésszerű működését, a bennük zajló információs folyamatokat.

Az információs társadalom tagjait érő és őket befolyásoló szociológiai hatások, valamint a számukra a kibertérben elérhető lehetőségek, rendelkezésükre álló eszközök, megszerezhető információk megkönnyítik azt, hogy egy személy – az őt ért hatások megfelelő konstellációjában – kiberterroristává váljon. Ugyanakkor ezek a szociológiai hatások nagy valószínűséggel azt is predesztinálják, hogy az érintett személy, milyen infrastruktúrák ellen, milyen célzattal és milyen módszerrel hajt végre támadást.

A komplex információbiztonság sémájához kapcsolódóan – az üzemeltetők és az állami szervek részéről – be lehet vezetni olyan új szempontokat, munkafolyamatokat, melyek növelik az információs infrastruktúrák biztonság szintjét.

Az információs infrastruktúrák üzemeltetéséhez és védelméhez kapcsolódó jellemzők tanulmányozása révén fel lehet tárni olyan összefüggéseket és kockázatokat a saját belső folyamatokban, illetve más kapcsolódó infrastruktúrák vonatkozásában, melyek kihatással lehetnek a biztonsági helyzetre. E tényezők aktuális állapotának, illetve esetleges változásainak folyamatos nyomon követése mindenképpen szükséges annak érdekében, hogy a biztonsági helyzetben negatív változás ne álljon be.

Kutatás célok

Az információ azon jellemzőinek feltárása, melyek manipulálása révén a kiberterrorizmus elérheti az információs infrastruktúrák működésének, illetve a felhasználók tevékenységének zavarát.

A potenciális elkövetők vonatkozásában annak meghatározása, hogy a kibertérben végrehajtott jogellenes cselekmények, kibertámadások esetében az elköteleződés, a

„végrehajtani akarás” mértéke elkövetőnkként miként változhat, milyen összefüggésben lehet az érintett személyek – általános, vagy éppen megélt – szociális folyamataival, hátterével.

Annak eldöntése, hogy a szociális folyamatok, hátterek vizsgálata indokolt-e abban az esetben, amikor egy adott személyi kör, társadalmi réteg jelentette veszélyt, támadási potenciálját kell felmérni, illetve a szociális alapú vizsgálat indirekt módon is használható-e, tehát egy adott funkciót betöltő információs infrastruktúra esetében felmérhető-e az, hogy milyen szociális háttérrel rendelkező személy kör – például képzettségük, szélsőséges politikai nézeteik és/vagy anyagi helyzetük okán – jelenti rájuk a legnagyobb veszélyt.

A kiberterrorizmus keretei között értelmezett tevékenységek, különböző módszerek csoportosítása, valamint a kiberterroristák által felhasználható fizikai hatáson alapuló és logikai eszközök osztályozása.

Az állam és az üzemeltetők részéről a megelőzés és fenyegetések felderítése terén végrehajtandó intézkedések meghatározása, illetve a potenciális együttműködési felületek azonosítása, és annak feltárása, hogy melyek a szorosabb együttműködés, a folyamatosság, a biztonság és a védelem ellen ható tényezők.

Olyan metódusok kidolgozása, melyek mind az üzemeltetői, mind pedig az állami oldal részéről elősegítik a védelmi intézkedések hatékonyságának növekedését, vagy a kockázatok csökkentését.

Kutatási módszerek

A választott témakör ismeretanyagának előzetes áttekintése során már felismerhető volt, hogy a kiberterrorizmus, illetve az ellene történő védekezés különböző aspektusainak felméréséhez több kutatási módszer kombinatív alkalmazására lesz szükség.

A kutatómunka során a nemzetközi és hazai szakirodalmat, illetve joganyagokat, továbbá a mérvadónak tekinthető média publikációit elektronikus és írott formában tanulmányoztam, mely a látókör bővítése, más forrásból származó információk visszaigazolása tekintetében, valamint az esettanulmányok szempontjából kiemelt jelentőséggel bírt.

A tudományos konferenciákon és szakmai összejöveteleken (workshop, fókuszcsoportos beszélgetés) szakértők részéről elhangzott információkat összegyűjtöttem, ami folyamatosan orientálta a kutatási tevékenységem irányát.

A munkavégzésem során a kiberterrorizmus vonatkozásában birtokomba került információkat elemeztem, értékeltem, a megszerzett tapasztalatokra, következtetésekre tudományos választ kerestem.

A munkavégzés során a hazai társszervekkel, illetve a külföldi partnerszolgálatokkal történt együttműködés során felmerült információkat és tapasztalatokat – a szakirodalomban lévő állítások, következtetések összevetésével, megállapításaim megerősítése, illetve megcáfolása érdekében – elemeztem.

A munkavégzésem során strukturált interjúkat készítettem információs infrastruktúrák üzemeltetésének különböző szakterületein foglalkozatott, különböző vezetői szintekhez tartozó személyekkel, akiknek tapasztalatait, információt elemeztem, értékeltem és felhasználtam a kutatómunka során. A munkavégzéshez kapcsolódóan interjúkat készítettem olyan személyekkel is, akik a kibertérben végrehajtott különböző bűncselekményekben voltak érintettek, mely információkat, tapasztalatok felhasználásra kerültek a kutatómunka során.

A fent bemutatott kutatási módszerekkel nyert információk szintetizálásával és értékelésével fogalmaztam meg részkövetkeztetéseimet, amelyek elvezettek a tudományos probléma megválaszolásáig.

Az elvégzett vizsgálat tömör leírása fejezetenként

I. Fejezet

Az információ és az információs társadalom

Az első fejezetben áttekintettem az információs társadalom tudományáganként eltérő definíciói mögött lévő megközelítéseket, azonosítva azokat a kritériumokat, melyek a társadalom ezen új formáját meghatározzák. Vizsgáltam, hogy az információs társadalom miként alakítja át a társadalom tagjai között kialakult viszonyokat, valamint azt, hogy melyek azok jelenségeket, amik fenyegetésként értékelhetők az információs társadalom számára, illetve azt, hogy ezek miként fejtik ki hatásukat. Tanulmányoztam a kiberteret, mint azt a

közeget, ahol ez az új társadalmi forma értelmet nyer. Elemeztem a kibertér polgári és katonai megközelítések között eltéréseket.

Foglalkoztam az információ mibenlétével, és hogy miért bír a modern társadalom számára kiemelt jelentőséggel. Ennek keretében vizsgáltam az információ gyakorlati hasznosítása szempontjából elengedhetetlenül fontos minőségi követelményeket, és ezek miként befolyásolhatják a vezetési ciklust.

Áttekintettem a kibertérnek helyt adó információs infrastruktúrák jelentését, típusait, funkcióit, a kritikusságra vonatkozó ismérveket. Továbbá vizsgáltam a kritikus információs infrastruktúrák vonatkozásában értelmezhető veszélyeket, ezek közül kiemelve a szándékos, illetve ártó jellegű cselekményekkel, tevékenységekkel összefüggő veszélyeket. Analizáltam az e típusú cselekmények végrehajtóit, illetve motivációikat, valamint a cselekmények jellegzetességeit.

II. Fejezet
A kiberterrorizmus

Tanulmányoztam a terrorizmus jelenségét, céljait, típusait, jogi meghatározásait, valamint azokat a momentumokat, melyek az országonként eltérő jogi definíciókra rányomják bélyegét, kivetülnek az adott ország terror-értelmezésére. Vizsgáltam a terrorizmus és az aszimmetrikus hadviselés közötti esetleges párhuzamot.

A terrorizmus, a technológiai fejlődés, illetve az információs társadalom kialakulásával törvényszerűen megjelenő kiberterrorizmust vizsgálva áttekintettem a szakirodalomban megjelenő különböző definíciókat, és a konklúziók levonását, valamint saját tapasztalatok értékelését követően megalkottam a kiberterrorizmus jelenségét – megítélésem szerint leginkább bemutató – definícióját.

Tanulmányoztam azokat a szociális hatásokat, körülményeket, élethelyzeteket, melyek tükrében az információs társadalom tagjai a kiberterroristává válás útjára léphetnek. Megvizsgáltam a kiberterroristák különböző kasztjaiba tartozó személyek élethelyzeteit, illetve a kasztosodást befolyásoló tényezőket. Ennek keretében több olyan körülményt

azonosítottam, melyek elősegíthetik azt, hogy a társadalom egy tagja kibertérben végrehajtott terrorcselekmény elkövetője legyen.

III. Fejezet
A kiberterrorizmus eszközei

A hazai jogi szabályozásból levezetve három részre, támogatás, finanszírozás és logisztikai, valamint végrehajtásra osztottam fel a kiberterrorizmus módszereinek potenciális körét.

Támogató módszerek körében a terrorizmus és a média kapcsolata alapján a terrorcsoportok kibertérben végrehajtott propaganda tevékenységét tanulmányoztam két módszerre koncentrálva. Az ideológia terjesztése körébe tartozó módszerek esetében vizsgáltam azokat a sajátosságokat, jellegzetességeket, melyek megkönnyítik azt, hogy a terroristák az üzeneteiket a kibertéren keresztül az információs társadalom széles köre számára elérhetővé tegyék. A támogatók toborzásának körébe tartozó tevékenységek elemezve rámutattam, hogy ez minőségében miben mutat túl jelentősen az ideológia terjesztésén.

A finanszírozás és logisztikai módszerek részben azokat a tevékenységeket kerestem, melyek a kibertérben működő terrorszervezetek szervezettségének, működő- vagy akcióképességének, valamint finanszírozhatóságának fenntartását teszik lehetővé. A kommunikáció, információk megosztása módszerek körében azonosítottam azokat kapcsolattartási lehetőségeket, melyeket a jogellenes cselekmények során az érintettek biztonságosan használhatnak. Az erőforrások gyűjtése, szolgáltatások igénybevétele tekintetében olyan megoldásokat kutattam, amik alkalmasak lehetnek arra, hogy a terrorcselekmények előkészítsék, a szükséges feltételeket megteremtsék. A finanszírozási források megteremtéséhez kapcsolódó módszernél tanulmányoztam azokat a tevékenységek, melyek révén a terrorcsoport pénzügyi erőforrásokhoz juthat hozzá.

A támadó módszerek tekintetében azokat a tevékenységeket vizsgáltam, melyek alkalmasak a terrorizmus filozófiájának megjelenítésére az információ társadalomban. A célpontok keresése és azokról információk gyűjtése körébe tartozó módszerek összegyűjtöttem, hatékonyságukat elemeztem. A célpontok támadásához kapcsolódó tevékenységek tanulmányozását követően osztályoztam azokat, továbbá e tevékenységek körében vizsgáltam az interdependencia jelenségét.

IV. Fejezet

A kiberterrorizmus eszközei

A fejezetben azokat a logikai és fizikai hatáson alapuló eszközöket, illetve alkalmazhatóságukat és hatékonyságukat tanulmányoztam, melyeket a kiberterroristák bevethetnek az információs infrastruktúrák ellen, ugyanakkor beszerzésük elháríthatatlan akadályokba nem ütközik számukra. Megvizsgáltam a professzionális és a nem professzionális eszközök közötti különbözőségeket.

A fizikai hatáson alapuló eszközök körében kerestem a potenciálisan a szóba jöhető módszereket, melyek közül az elektronikai ellentevékenységre, ezen belül pedig az elektronikai pusztításhoz tartozó berendezésekre helyeztem a hangsúlyt.

A logikai eszközök esetében kutattam azokat az előnyöket, melyek az alkalmazhatóságuk mellett szólnak, illetve elemeztem azokat az anomáliákat, melyek az esetleges felhasználásukkal kapcsolatosak, illetve
Áttekintettem azokat a támadástípusokat, melyek alkalmasak lehetnek az információs infrastruktúrák ellen végrehajtott terrortámadások kivitelezésére.

V. Fejezet

A kiberterrorizmus elleni védekezés megoldásai

Tanulmányoztam az információs infrastruktúrák vonatkozásában megjelenő fenyegetések összetevőit, valamint azt, hogy ezek milyen hatásokat indukálnak a különböző állapotjelzőkben.

A komplex információbiztonság szakterületeinek áttekintése során megvizsgáltam, hogy ezekre a kiberterrorizmus milyen jellegű fenyegetést jelent. A szakterületek specialitásának áttekintését követően szükségesnek tartottam a védelmi intézkedéseket a nemzetbiztonsági védelemmel, az aszimmetria vizsgálattal, valamint a működési és biztonsági interdependencia térképpel kibővíteni.

A védekezés lehetséges megoldásai között a megelőzés fontosságát felismerve, az üzemeltetők és az állami szereplők részéről kerestem azokat a lehetséges módszereket, melyek hozzájárulhatnak az információs infrastruktúrák biztonsági helyzetének javításához.

Összegzett következtetések

A terrorizmusnak, mint jelenségnek a tanulmányozásakor levonható az a következtetés, hogy annak metodikája, célkitűzése kialakulása óta alapvetően nem változott. Az adott ideológia nevében, céltalanul, véletlenszerűen alkalmazott erőszak révén mindig is bizonyos társadalmi csoportok elnyomása, félelemben, bizonytalanságban tartása és a csoport tagjainak fizikai pusztítása volt a célja, mely alapvető cél az idők során mit sem változott, így ez a megállapítás a jelenkorra is igaz. Azonban a jelenségben egy momentum folyamatosan, korszakról-korszakra fejlődött, mégpedig az alkalmazott eszközökben, mivel az adott kor vívmányai, technológiai színvonala, tudományos eredményei mindig visszatükröződtek, illetve eszköztárában a mindenkori csúcstechnika – feltalálásukat, kifejlesztésüket követően – rövidesen megjelent.

Az információs folyamatok fejlődésével, illetve ezeket a folyamatokat befogadó, támogató, egyre modernebb és hatékonyabb infrastruktúrák kialakulásával, majd globalizálódásával megszületett a kibertér. Az információs infrastruktúrákban megjelent új technológiák, műszaki megoldások segítették az információs folyamatokat, majd mikor ezek átléptek egy kritikus méretet, köréjük, illetve szolgáltatásaik köré szerveződött a társadalom végtelenül sok funkciója, mely révén így a társadalom megkapta az információs jelzőt. Ennek már nemcsak a fejlődéséhez, de zavarok nélküli működéséhez is elengedhetetlen a kellő mennyiségű információ folyamatos megszerzése, áramlása és rendelkezésre állása.
Fenti megállapításokból ugyanakkor levezethető, hogy a terrorizmus számára – céljainak elérése érdekében – szükségszerű, hogy az információs társadalomban is „gyökeret eresszen”, mind úgy, hogy a terroristák maguk is belépnek, integrálódnak e társadalomba, ki- és felhasználják lehetőségeit, valamint eszközeit, mind pedig úgy is, hogy e társadalom ellen fejtik ki tevékenységüket, hogy megzavarják folyamatait, mely révén elérik alapcéljukat, félelmet és bizonytalanságot gerjesztenek. Tehát a kiberterrorizmusnak, mint a terrorizmus és a kibertér közös halmazának a megjelenése gyakorlatilag a műszaki-technológiai fejlődés törvényszerű velejárója.

Levezethető, hogy a kibertér sajátosságaiból adódóan megkönnyíti azt, hogy az információs társadalom tagjai bizonyos radikalizálódási hajlam és megfelelő hatások mellett kiberterroristává válhassanak. Egyrészt a különböző terrorcsoportok a kibertérben könnyebben fejtik ki propaganda és toborzótevékenységüket, mivel a földrajzi és államhatárok nem jelentenek akadályt, célcsoportjaik „igényei", valamint szimpatizánsaik elvárásai szerint könnyen tudják üzeneteik tartalmát, illetve a közlés módját differenciálni, ami jelentősen növeli hatékonyságukat, mivel könnyen „egymásra találnak" szimpatizánsaikkal. Másrészt a kibertérben végrehajtott jogellenes cselekmények végrehajtása egyfajta biztonságos burokban – sokszor az „otthon melegében" – történik, ezért az elkövetők fizikálisan meg sem közelítik az áldozatot, nem kerülnek vele kapcsolatba. E körülmény következtében másként – jellemzően nem negatívan élik – meg tettüket az elkövetők, pszichésen nem alakul ki bennük tudat, hogy a cselekményükkel kárt, sérelmet okoznak, másokat veszélybe sodornak, és ez fokozottan igaz, ha cselekményük jogellenes mivoltával, vagy annak következményeivel – tájékozatlanságuk okán – alapvetően nincsenek is tisztában. Harmadrészt az elkövetések eszköze logikai támadások esetében gyakorlatilag az információs társadalom „alapeszköze", a bárki számára hozzáférhető számítógép, míg fizikai hatáson alapuló támadások esetében ezek az eszközök viszonylag könnyen beszerezhetők, átalakíthatók, megalkothatók. Negyedrészt pedig a kibertér számos olyan szolgáltatást és lehetőséget nyújt, mely a terrorcsoportok számára a megkönnyíti kapcsolattartást, tevékenységük finanszírozását, illetve lehetővé teszi számukra konkrét terrortámadások kivitelezését is. Továbbá a kibertér az anonimizálódásra, a digitális nyomok elrejtésére is kiváló lehetőségeket biztosít, mely egyrészt az elkövetők folyamatos, lebukás nélküli – akár önképzésen alapuló – kísérletezgetését teszi lehetővé, másrészt pedig az „először kipróbálókat" bátorítja a jogellenes cselekményük végrehajtására. A fentiek tükrében pedig prognosztizálható, hogy a kiberterrorizmus a terrorizmuson belül – az információs társadalom fejlődésével összhangban – egyre nagyobb részt fog kihasítani.

A kiberterrorizmus eszközrendszerét vizsgálva nagy valószínűséggel előjelezhető, hogy a terrorcselekmények, illetve az erre irányuló kísérletek jelentős részét várhatóan a logikai eszközök alkalmazása révén fogják végrehajtani. Ennek oka, hogy a fizikai hatáson alapuló eszközök alkalmazása lényegesen nagyobb szervezést, háttérismeretet, alkalmazhatóságra vonatkozó információt, anyagi ráfordítást és ebből fakadóan pedig jóval nagyobb elköteleződést igényel, mint a logikai eszközök alkalmazása. A kiberterroristák döntő hányada számára a logikai eszközök alkalmazása lényegesen könnyebb, mivel az interneten

keresztül a különféle módszerek, leírásai, alkalmazhatósági feltételei, továbbá a különböző sérülékenységekre vonatkozó információk könnyen elérhetőek, illetve maguk a támadókódok is viszonylag könnyen beszerezhetők (akár toolkit-ek formájában), meglévő, vagy megszerezhető szakismeret birtokában a már rendelkezésre állók átalakíthatók, „testre szabhatóak", de akár meg is alkothatók és többször, vagy párhuzamosan is alkalmazhatóak. Mindezek mellett birtoklásuk és fejlesztésük szinte egyáltalán nem kimutatható, alkalmazásuk megfelelő intézkedések mellett biztonságos, kockázatmentes.

A kiberterroristává válás folyamatának, valamint a fizikai hatáson alapuló és a logikai eszközök metodikájának, képességeinek tanulmányozása által levonható az a következtetés, hogy a széles körben elérhető, vagy megalkotható eszközök révén a kiberterroristák – professzionális eszközök és mélyreható szakismeretek hiányában – jelenleg az információs infrastruktúrákat rendszerszinten nem képesek veszélyeztetni. Ugyanakkor lokálisan, vagy bizonyos alrendszerek tekintetében képesek érzékelhető, kimutatható zavarokat és viszonylag nagy kárt is okozni, melyek – bár médiaérdeklődésre számot tartanak – az információs társadalom globális folyamatait nem zökkentik medrükből, mindannak ellenére sem, hogy a társadalom egyes entitásait a támadás anyagilag, érzelmileg érzékenyen érintheti.

Az okozott kár, illetve zavar azonban jelentősen növelhető, ha a kiberterroristák találnak olyan biztonsági réseket, aszimmetriákat és interdependencia kapcsolatokat, melyekről az üzemeltetők, illetve az incidensben érintettek (például rendészeti szervek, üzleti partnerek) nem tudtak, illetve nem kezeltek.
Az előzőekből levonható az a következtetés, hogy az aszimmetria jelensége, illetve annak különböző dimenziói az információs infrastruktúrák aktív és passzív védelme, illetve a már bekövetkezetett kibertámadások hatásainak felmérése, elhárítása, a károk enyhítése, valamint az elkövetőik azonosítása terén egyre nagyobb problémát fog jelenteni. Amennyiben a támadók képesek azonosítani a védelem gyengeségeit, az interdependens kapcsolatokat, az aszimmetria potenciális területeit és cselekményeiket ezek figyelembevételével tervezni, akkor rendkívüli mértékben megnehezíthetik az információs infrastruktúrák működését, védelmét, illetve az ellenük fellépni kívánó hatóságok tevékenységét.
Ez pedig rá is világít a komplex, az egyenszilárdságú védelem szükségességére. Az alkalmazott védelmi rendszernek minden, a tervezésekor bekalkulált körülmény megjelenésekor garantálnia kell az információs infrastruktúra szolgáltatásainak folytonosságát, a kezelt információk biztonságát. A védelmi rendszer kiépítése azonban nem

csak egy egyszeri feladat, hanem folyamatos monitorozó, információgyűjtő, tervező és fejlesztő tevékenység, mely a biztonság minden dimenzióját kell, hogy érintse.

Új tudományos eredmények

1. A kibertérben végrehajtott, a terrorizmussal összefüggésbe hozható jogellenes tevékenységek, cselekménysorozatok tanulmányozása során megszerzett tapasztalatok, ismeretanyagok összegzését követően megalkottam a kiberterrorizmus definícióját. A definícióban egyesítve jelenik meg az a sajátosság, hogy a kiberterrorizmus az információs infrastruktúrákra egy időben tekint célpontként és a végrehajtás eszközeként.

2. A különböző terrorcsoportok kibertérben folytatott tevékenységének, illetve kifejezetten a kiberterrorizmushoz kapcsolódó cselekmények tanulmányozása során megszerzett tudásanyag, valamint a saját tapasztalatok szintetizálását követően kategorizáltam a kiberterrorizmus módszereit, illetve a kategóriákba tartozó tevékenységeket.

3. Az információs infrastruktúrák vonatkozásában mind az üzemeltetők, mind pedig a védelmi, rendészeti feladatokban érintett állami szervek számára – működésük hatékonyságának és teljesítőképesség növelése érdekében – aszimmetria vizsgálat lefolytatását javaslom, melynek eredményeképpen napvilágra kerülhetnek olyan momentumok, illetve ezeknek különféle kombinációi, melyek nem várt módon gátolhatják, gyengíthetik a különböző incidensekre, behatásokra adandó válaszok eredményességét.

4. Az információs infrastruktúrák üzemeltetési és biztonsági körülményeiben rejlő összefüggések, valamint a különböző külső-belső hatások következményeinek feltárása érdekében működési és biztonsági interdependencia térkép bevezetésére teszek javaslatot, melynek célja, hogy mind az infrastruktúrák védelmében közreműködő állami szereplők, mind pedig az üzemeltetők a különböző szakterületeket érintő esetlegesen megjelenő negatív hatások eredőjét a működés, illetve a komplex információbiztonság teljes spektrumában láthassák.

Ajánlások, eredmények gyakorlati felhasználhatósága

Javaslom a doktori értekezésben összefoglaltakat felhasználni az információs infrastruktúrákhoz, valamint a kiberterrorizmushoz, illetve e szakterületekhez kapcsolódó egyéb egyetemi alap és mesterképzések tananyagaként.

Javaslom az értekezés kiberterrorizmus mibenlétét, módszereit és eszközeit tárgyaló részeit a rendészeti és a nemzetbiztonsági szervek e területen foglalkoztatott állományának továbbképzési tananyagaiba beintegrálni.

Javaslom az értekezésben megfogalmazott észrevételeket, ajánlásokat felhasználni az információs infrastruktúrák információbiztonsági szakembereinek tanfolyami képzésein, továbbképzésein.

Javaslom az értekezés megállapításait az információs infrastruktúrák komplex védelmének tervezésekor, az üzemeltetésre vonatkozó stratégiák megalkotásakor, illetve a jogszabályi feltételek, környezet kialakításakor felhasználni.

Az értekezés témájában született publikációk jegyzéke

- Papp Zoltán: RFID – Új technológia veszélyei: RFID és az elektronikus útlevél, „Hadmérnök” V. évfolyam 4. szám, 2010. december, - pp 248-254., ISSN 1788-1919
- Papp Zoltán: Irányított energiájú fegyverek veszélyei a kommunikációs hálózatokra, „Hadmérnök” VI. évfolyam 4. szám, 2011. december, - pp 233-238., ISSN 1788-1919
- Papp Zoltán: Az információ támadása annak tulajdonságain keresztül, „Hadmérnök” VI. évfolyam 4. szám, 2011. december, - pp 224-232., ISSN 1788-1919
- Papp Zoltán: A helyzet-meghatározó rendszerek zavarása, „Hadmérnök” VII. évfolyam 1. szám, 2012. március, - pp 214-221., ISSN 1788-1919
- Papp Zoltán: A számítógép-hálózatok tűzfalainak támadása, „Hadmérnök” VII. évfolyam 2. szám, 2012. június, - pp 335-341., ISSN 1788-1919
- Papp Zoltán – Pándi Erik – Kerti András: A számítógép-hálózatok elleni támadások módszertana, „Kommunikáció 2009.” nemzetközi szakmai-tudományos konferencia, 2009. október 14., - pp. 143-154. ZMNE Budapest, ISBN 978-963-7060-57-1
- Papp Zoltán – Pándi Erik – Töreki Ákos: A fenyegetettség egyes aspektusai az információs infrastruktúrák tekintetében, „Kommunikáció 2009.” nemzetközi szakmai-

tudományos konferencia, 2009. október 14., - pp. 155-163., ZMNE Budapest, ISBN 978-963-7060-57-1

- Papp Zoltán: Virtuális magánhálózati kapcsolatok, „Hírvillám" ZMNE Híradó Tanszék Tudományos Szakmai Kiadványa, I. évfolyam 1. szám, 2010. december, - pp 156-162., ZMNE Budapest, ISSN 2061-9499
- Papp Zoltán: RFID – Új technológia veszélyei, „Hírvillám" ZMNE Híradó Tanszék Tudományos Szakmai Kiadványa, I. évfolyam 1. szám, 2010. december, - pp 271-275., ZMNE Budapest, ISSN 2061-9499
- Papp Zoltán – Pándi Erik – Dorkó Zsolt: Információs rendszerek alkalmazási feltételeinek korlátozása, Tanulmány – 2010. – 92 p., ZMNE Egyetemi Könyvtár, Budapest
- Papp Zoltán: Information terrorism, „Hadmérnök" VIII. Évfolyam 4. szám, 2013. december, - pp. 217-222., ISSN 1788-1919
- Papp Zoltán: Professional areas of protection against information terrorism, „Hadmérnök" IX. Évfolyam 3. szám, 2014. szeptember, - pp. 207-213., ISSN 1788-1919

Szakmai-tudományos önéletrajz

Középiskolai tanulmányaimat a szegedi Déri Miksa Ipari Szakközépiskolában végeztem, ahol 1993-ban érettségiztem le, mellyel párhuzamosan az általános gépszerelő és karbantartó szakmunkás végzettséget is megszereztem. Középfokú tanulmányaim alatt több évben is eredményesen vettem részt különböző országos szakmai tanulmányi versenyeken.
Tanulmányaim alapján felvételt nyertem a Bánki Donát Műszaki Főiskola szervező és informatika szakára, ahol 1996-ban mérnöki végzettséget szereztem. Harmadévesen kezdtem el kutatómunkával foglalkozni, amikor is Dr. Rudas Imre professzor irányításával, a „Fuzzy halmazok entrópiája és hasonlósági mértékei" című pályamunkával az Országos Diákköri Konferencia döntőjébe jutottam.

1997-ben kerültem a Nemzetbiztonsági Hivatal állományába, ahol a kiképzési idő végeztével a rendvédelmi szervek és kiemelt kormányzati objektumok és intézmények nemzetbiztonsági védelmével foglalkozó szakterületen helyezkedtem el. Munkám kiterjedt a komplex információbiztonság minden dimenziójára, ennek keretében gyűjtöttem, értékeltem, elemeztem az érintett szervezetek biztonsági helyzetére vonatkozó információkat,

körülményeket, továbbá tájékoztatási és intézkedési javaslatokat tettem a különböző kockázatok, illetve fenyegetések felszámolása érdekében.
Mivel a komplex információbiztonság szakterületei közül az elektronikus információbiztonság után érdeklődtem leginkább, ezért szakismereteimet ez irányba mélyítettem el, így 2009-ben a Zrínyi Miklós Nemzetvédelmi Egyetemen védelmi rendszertervező végzettséget szereztem.
2010-től szakterületet váltottam, amikor is a nemzetgazdaság szempontjából kiemelt energetikai és közlekedési, majd 2012-től pedig a kiemelt infokommunikációs infrastruktúrák nemzetbiztonsági védelmével foglalkoztam.

Szakmai tevékenységemhez kapcsolódóan folyamatosan részt vettem különböző tudományos konferenciákon, a szolgáltatók által életre hívott szakmai napokon, illetve hazai társszervek, illetve külföldi partnerszolgálatok által szervezett szakmai konzultációkon és továbbképzéseken.

2010-ben felvételt nyertem a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájába PhD hallgatónak, ahol Dr. Kovács László ezredes lett a témavezetőm, témám a kiberterrorizmus, ennek módszerei és a védekezés lehetséges alternatívái.

2017-től a Belügyminisztérium rendszerbiztonsági felügyelőjeként a minősített adatokat kezelő elektronikus rendszerek biztonsági helyzetét érintő tevékenységekben veszek részt.

Budapest, 2018. szeptember 1.

Papp Zoltán István