PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK
DOKTORI ISKOLÁJA

Gyaraki Réka Eszter

A SZÁMÍTÓGÉPES BŰNÖZÉS NYOMOZÁSÁNAK PROBLÉMÁI

Tézisek

Témavezető:

Dr. Nagy Zoltán András

Habilitált egyetemi docens

Tanszékvezető

Pécs, 2018

Tartalomjegyzék

1 BEVEZETÉS

1.1 A kutatási témaválasztás indoka

Napjaink számítástechnikai és informatikai fejlődésének ugrásszerű növekedésének köszönhetően, azok technikai tulajdonságaik révén gyorsabban és kényelmesebben elérhetőek a különböző kereskedelemi szolgáltatások, a pénzügyek intézése, az egymással történő szóbeli vagy írásbeli kommunikáció, az ügyintézések különböző formáihoz, amelynél sokszor a személyes jelenlét sem szükséges.

Az előnyök mellett ugyanakkor megjelentek a számítástechnikai bűncselekmények is, amelyek egyre nagyobb teret hódítanak a világban[1]. Olyan globális problémává vált a számítástechnikai bűnözés, hogy arra már nemcsak az egyes államoknak, de az Európai Unió országainak, a katonai-, gazdasági szövetségeknek is reagálni kell rá nemcsak jogalkotói, hanem jogalkalmazói szinten.

A számítástechnikai bűnözők által okozott károk már a 2016-os IOCTA[2] szerint meghaladják az Európai Unió egyes tagállamaiban a hagyományos bűncselekmények által okozott károkat, a számok mind az elkövetői, mind a sértetti oldalon folyamatosan nőnek, az elkövetési magatartás pedig egyre jobban bővül, így szükséges a még hatékonyabb fellépés a jogalkotók, a nyomozóhatóságok, az ügyészségek és további jogalkalmazók részéről.

1.2 A kutatás során alkalmazott eszközök és kutatási módszerek

A kutatás során az alkalmazott módszerek kiválasztásánál több szempontot is vizsgáltam. Így a kérdőíves módszert, az interjúkészítést és az aktakutatás/dokumentumkutatást, mint lehetőségeket. A módszerek számbavétele során azonban szem előtt tartottam, hogy az általam választott téma a jogtudomány és a kriminalisztika ötvözete, hiszen leginkább a nyomozóhatóság, így a rendőrség és a Nemzeti Adó-és Vámhivatal (NAV) bűnüldözéssel foglalkozó szervei.

[1] Symantec szerint: 2018-ban 978 millió embert érintett 20 országban a számítógépes bűnözés, csak az elmúlt 12 hónapban a fogyasztók 44% -át érintette a számítógépes bűnözés. A számítógépes bűnözés áldozatául esett fogyasztók globálisan 172 milliárd dollárt vesztettek! (forrás: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf, letöltve: 2018. július 31)

[2] Internet Organised Crime Threat Assessment

A kérdőíves módszer tekintetében mérlegeltem, hogy a hazai szervezetek közül a jogszabályi előírásoknak megfelelően ki és milyen esetekben jogosult a büntetőeljárás lefolytatására és a saját erőforrások tekintetében sikeres lehet-e annak végrehajtása.

1.3 A kutatás célja

Ray Kurzweil[3] a technológia fejlődésével kapcsolatos véleménye: „Sok tudósra és mérnökre jellemző az, amit én a „tudósok pesszimizmusának" nevezek. Gyakran annyira elmerülnek egy jelenbeli kihívás nehézségeiben és apró részleteiben, hogy nem ismerik fel saját munkájuk és a tágabb értelemben vett tudományterületük hosszú távú hatásait, mint ahogy azokat a sokkal erősebb eszközöket sem veszik számításba, amelyek a technológia minden egyes új nemzedékével hozzáférhetővé válnak."[4]
Kurzweil fenti megállapítása, amely a Mesterséges Intelligenciával foglalkozó könyvében olvasható, az értekezés írása és a kutatások során sok helyen beigazolódott, annyiban, hogy nemcsak a kutatásokat, a kutatókat érinti ez a „beszűkülés", hanem a rendőrséget, azon jogalkotókat is, akik bár érzik a kiberbűnözés jelenlegi negatív hatásait, de sajnos nem kellő időben, vagy nem a hatékony eszközökkel, a jogalkotási rendszer évtizedes sémáját eldobva próbálják meg felvenni a harcot a számítógépes bűnözéssel.

A kutatás során célul tűztem ki, hogy megkeressem azokat a gyenge pontokat a számítógépes bűnözéssel összefüggő jogszabályok területén, amelyek a kiberbűnözés dinamikus fejlődése miatt gondot okozhat a hatóságoknak a nyomozások során. Ezért elsősorban a hazai jogszabályokat tekintettem át, külföldi „jó joggyakorlattal" összevetve.
A nehézségek feltárása és megismerése közelebb vihet ahhoz, hogy a számítógépes bűncselekmények elleni nemzeti és nemzetközi fellépés sikeres legyen.

Mivel egy viszonylag friss és dinamikusan fejlődő bűncselekmény típusokról van szó, így a hipotézisek és tézisek tekintetében szükséges volt, a változékonyságához alkalmazkodó kérdéseket feltenni.

[3] Ray Kurzweil a Google fejlesztő igazgatója, futurológus, a technológia jövőben játszott szerepének egyik vizsgálója
[4] Ray Kurzweil: A szingularitás küszöbén- Amikor az emberiség meghaladja a biológiát (Ad Astra 2014, 37.oldal)

Az értekezés során az alábbi pontokat vizsgáltam:

1. A számítógépes bűncselekmények esetében az új büntetőeljárásjogi törvényben bevezetett kényszerintézkedések hatékonyságának vizsgálata és javaslatok kidolgozása külföldi példák figyelembevételével.
2. A szakértő kirendelések szükségességének vizsgálata, és a bíróság előtti eljárásban a bizonyítékok összegyűjtése, értékelése. Meddig terjedhet a nyomozóhatóság kompetenciája a számítógépes bűncselekményekben?
3. Az egyes kiberbűncselekmények során más és más sarkalatos problémák merülnek fel, eltérő eljárási cselekmények válnak szükségessé az elkövető kézrekerítése, valamint a bűncselekmény bizonyítása érdekében.
4. A rendőrség kiberbűnözés nyomozásával kapcsolatos oktatásának fontossága, amely első lépése lehet a bűncselekmény eredményes felderítésének.

1.4 A kutatási hipotézisek

A kutatás céljához mérten fogalmaztam meg a hipotéziseket is, amelyből majd a feltevéseim helyessége esetén javaslat megfogalmazása vált célommá, vagy pedig a külföldi példák alapján egy jobb gyakorlat kialakítása.

- a számítógépes bűncselekmények elkövetésének térben és időben történő pontos meghatározása, a törvényben használt fogalmak, kifejezések pontosítása a további nyomozási és felderítési eljárás szabályozáshoz hozzájárul. (a pontos fogalommeghatározás szükséges a számítógépes bűncselekmények felderítésének és nyomozásának sikeressége érdekében),
- a kényszerintézkedések jogi szabályozásánál az elektronikus bizonyítékokat nem szabad a hagyományos deliktumok elkövetése során keletkező bizonyítékokkal összehasonlítani (a számítógépes bűncselekmények, mint fogalom, túlontúl általános. Az eljárás szempontjából véleményem szerint szükséges különbséget tenni aközött, hogy a deliktum elkövetése a kibertérben történik, és aközött, hogy egy jogellenes cselekmény a „valós”, fizikai térben következik be, de a bizonyíték a kibertérből szerezhető be.),

- a hazai, merev jogszabályok nem alkalmasak az olyan fejlődő és kihívásokkal teli deliktumok nyomozásának esetében, ahol maga az elkövetés eszköze, az elkövetők és módszerek folyamatos változáson mennek keresztül,
- az elektronikus bizonyítékok beszerzésénél azok eredetisége és hitelessége megőrzése érdekében a hagyományos bizonyítékok beszerzésétől és lefoglalásától eltérő módon végezhető csak el,
- a szakértő igénybevételének pontos és elfogadott szabályai nincsenek rögzítve egyetlen magyar jogszabályban sem. Ez különösen fontos lenne a számítógépes bűncselekmények nyomozása során.

2 A KUTATÁSSAL ELÉRT EREDMÉNYEK BEMUTATÁSA

A felállított hipotézisek és a levont következtetések és javaslatok[5]:

Első hipotézisem: *a számítógépes bűncselekmények elkövetésének térben és időben történő meghatározása, a törvényben használt fogalmak, kifejezések pontosítása a további nyomozási és felderítési eljárás szabályozáshoz hozzájárul.*

Ennek a feltételezésnek megfelelően kimondható, hogy a kibertérből származó bűncselekmények üldözése nem lehet hatékony, addig, amíg magát a kiberteret a fizikai térrel azonosítjuk, azaz megpróbálunk határokat szabni és azok között tartva megállapítani a hatóságok illetékességi területét. Ilyenkor fordul elő az, hogy ismeretlen tettes ellen indított nyomozás során a szolgáltató székhelye szerinti hatóság jár el az ügyben, ami nem zárja ki, hogy az elkövető a hatóság illetékességi területén kívül követte el a bűncselekményt.

A jelenlegi szabályozás szerint:

***„3. §** (1) A nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt - sorozat-bűncselekmények esetén a bűncselekmények többségét - elkövették.*

(2) Ha az elkövető a bűncselekményt több nyomozó hatóság illetékességi területén követte el vagy több nyomozó hatóság illetékességi területén követett el bűncselekményeket, vagy az elkövetés helye nem állapítható meg, a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelyik az ügyben korábban intézkedett, intézkedés hiányában pedig az, amelynek a bűncselekmény saját észlelése vagy bejelentés, feljelentés alapján legkorábban a tudomására jutott.

(3) Ha az elkövető a bűncselekményt Magyarország határain kívül követte el, a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek - miniszteri rendeletben meghatározott - illetékességi területén az elkövetőt fogva tartják, ennek hiányában pedig, amelynek - miniszteri rendeletben meghatározott - illetékességi területén az elkövető utolsó ismert belföldi lakó- vagy tartózkodási helye van."[6]

1. Javaslat: a BM rendelet fent leírt szabálya azonban nem alkalmazható vagy legalábbis nem minden esetben alkalmazható. Így megfontolandó lenne annak rögzítése, hogy a kibertérben elkövetett bűncselekmények esetében eltérő szabályokat vezessenek be, így:

[5] előfordulhat, hogy a 11. Fejezetben leírt megállapítások már korábban is megfogalmazásra kerültek vagy teljes egészében vagy kisebb-nagyobb eltérésekkel

[6] 5/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről

- az ismeretlen tettes ellen indított nyomozás során annak a hatóságnak kötelessége eljárni, ahol a feljelentést először tették, vagy ahol a bűncselekményt először észlelték.
- az előkészítő eljárás során pedig annak a hatóságnak kell eljárni, amelyik az eljárás során a jogellenes cselekményről először tudomást szerzett.
- amennyiben a cselekmény elkövetése határokon átnyúló bűnözésre mutat, úgy nemzetközi jogsegély, együttműködés keretében van mód az eljárás lefolytatására.

Az idő, mint nyomozást nehezítő tényező, szintén problémát okoz a számítógépes bűncselekmények esetében. Az időnek is jelentősége van, mind az elévülési idő számításakor, mind pedig a felderítés során alkalmazandó cselekmények végrehajtása során. Az sem tisztázott, hogy mikor következik be a jogsértő cselekmény, mi tekinthető kezdő időpontnak?
Az idő jelentőségének egyrészt az elkövetés idejének megállapításakor van jelentősége: a jogellenes cselekmény elkövetésének meghatározásakor érdekes kérdés, hogy mikor tekinthetjük elkövetettnek például az információs rendszer felhasználásával elkövetett csalást abban az esetben, amikor

- a *bűncselekmény elkövetés idejének* különös jelentősége van, hiszen főszabályként az ekkor hatályban lévő törvényt kell alkalmazni. A bűncselekmény elkövetési idejének meghatározása az egymozzanatú bűncselekményeknél nem okoz problémát, mert ez esetekben a törvényi tényállás elemei egyszerre valósulnak meg (például egy lövéssel megölt ember, aki a sérülésbe azonnal belehal). Kérdéses azonban az elkövetési idő olyan bűncselekmények törvényi tényállásánál, ahol a tényállási elemek nem egy időben valósulnak meg. A jogtudomány több elméletet dolgozott ki e problémák megoldására.
- A *magatartás- (vagy tevékenység-) elmélet* szerint az elkövetési idő, amikor az elkövetési magatartás utolsó mozzanatát is kifejtik, azaz az adott tényálláshoz tartozó valamennyi magatartást megvalósították. Például lassú, több hónapon át tartó méregadagolással elkövetett emberölés esetén az utolsó adag méreg beadása lesz az elkövetési időpont.
- A *cselekményegység-elmélet* szerint a bűncselekmény elkövetésének ideje az, amikor az elkövető az adott tényálláshoz tartozó bármely magatartási elemet megvalósította. Az előző példánál maradva: ennek az elméletnek az alapján elkövetési időnek számít az első adag, de az utolsó adag beadása is.
- Az *okfolyamat-elmélet* szerint a bűncselekmény elkövetési ideje az, amikor az okfolyamat már önállóan, a tettes magatartásától függetlenül fejlődik. Az eddigi példát

használva elkövetés időpontjának számít annak az adagnak a beadása, amellyel már a halálos eredményhez elegendő méreganyag gyűlik fel a sértett szervezetében.

- Az *eredményelmélet* alapján a bűncselekmény elkövetési ideje a törvényi tényállás megvalósulásához szükséges eredmény bekövetkezése, azaz a megmérgezett sértett halálának bekövetkezésének időpontja.

A számítógépes bűncselekmények elkövetése során az időnek az elévülés és a bizonyítékok beszerzése tekintetében van különleges jelentősége, így a hipotézisemnek ezt a részét bizonyítani nem tudtam.

Második hipotézisem: a kényszerintézkedések jogi szabályozásánál az elektronikus bizonyítékokat nem szabad a hagyományos deliktumok elkövetése során keletkező bizonyítékokkal összehasonlítani (a számítógépes bűncselekmények, mint fogalom, túlontúl általános. Az eljárás szempontjából véleményem szerint szükséges különbséget tenni aközött, hogy a deliktum elkövetése a kibertérben történik, és aközött, hogy egy jogellenes cselekmény a „valós", fizikai térben következik be, de a bizonyíték a kibertérből szerezhető be.)

Ebben nyújt segítséget, hogy a számítógépes bűncselekmények és a kiberbűncselekmények fogalma között mégis különbséget tettem, még akkor is, ha ezt a két fogalmat ma már egymás szinonimájaként használják a külföldi jogalkotók és kutatók.

A számtógépes bűncselekmény és a kiberbűncselekmény között az alábbiak szerint teszek különbséget:

- Számítógépes bűncselekmény- azaz, ahol magának a számítógépnek, mint elkövetés eszközének jelentősége van, minden olyan bűncselekmény, ami már létezett a számítógép előtt is már ismertek voltak. Ilyenek a sikkasztás, a csalás (Btk. 373.§), a személyazonosság lopás.
- A kiberbűncselekményeknek pedig azok a bűncselekmények tekinthetőek, amelyek már az IT fejlődésével párhuzamosan alakultak ki, és amelyek azok fejlődésével folyamatosan változnak is. Ilyen bűncselekmények például az adathalászat, amelyek az SMS-küldéstől (smishing) kezdve a hanghíváson (vishing) át az e-mailen keresztül megvalósulhat, a malware-ek írása és alkalmazása, a kiberháború, vírusok, férgek és célzott alapú támadások stb.

Ha a két fogalom közötti különbségeket ízlelgetjük, akkor érezhető, hogy a számítógépes bűncselekmények hagyományosabb elkövetést feltételeznek, így a bizonyítékok gyűjtése és értékelése során a „tárgyi" bizonyítási eszköz kifejezés helytálló, hiszen a fizikailag

körülhatárolható eszköz, így a számítógép, mint „eszköz” jelenik meg, a valós térben is bekövetkezik a jogellenes cselekmény és ott is érezhető annak hatása.
A kiberbűncselekmény esetében az elkövetés a kibertérben történik és az elektronikus információs rendszereket, elektronikus adatokat érinti. Hatása érezhető a valós térben, így a például a 2017-ben bekövetkezett Wannacry zsarolóvírus támadás a kórházak, mint kritikus infrastruktúrák ellen, zavart okozott a betegellátásban.
A bizonyítékok értékelése és a büntetőeljárásban nevesített kényszerintézkedések végrehajtása a két „bűncselekmény típus” között eltérő, nem lehet tipikus rendszerbe besorolni, így a fentiek fényében séma szinten említeni a bizonyítás tárgyát sem lehet.
A számítógépes bűncselekmények nyomozásánál és felderítésénél, a bizonyítékok összegyűjtéséhez szükséges a kreatív, nem vonalas, tipikus eljárások bevezetése, kivitelezése. Amennyiben sikerülne különválasztani a kibertérből beszerezhető bizonyítékokat és a bizonyítási eljárásokat a hagyományos bűncselekményektől, úgy lenne értelme a „jó gyakorlat” kialakításának.
Javaslat: a digitális bizonyíték és az elektronikus információs rendszerben keletkező bizonyítékok fogalmának megalkotása és beemelése a büntetőeljárásról szóló törvénybe. Ezek legáltalánosabb összetevője a következők lehetnek:

- olyan adatok, információk, amelyek a rendszer használata során, a rendszerből vagy arról a számítástechnikai eszközről szerezhető be, amelyen az érintett rendszer fut
- olyan számítógépes programok, amelyek a felhasználók tevékenységét, digitális lábnyomát tartalmazza
- azok az információk, amelyek bár változékonyak és eredetiségük megtartása nehezebben megoldható, mint a tárgyi bizonyítási eszközök esetében
- Az útmutatók készítése- mint ahogyan az ENISA által készített bizonyítással kapcsolatos útmutató ismertetése során is említettem, így a 7.7 alfejezetben ismertetett megoldási javaslatok egy részének bevezetése és tovább gondolása is segíthetné a számítógépes bűnözés elleni küzdelmet.

Harmadik hipotézisem: a hazai, merev jogszabályok nem alkalmasak az olyan fejlődő és kihívásokkal teli deliktumok nyomozásának esetében, ahol maga az elkövetés eszköze, az elkövetők és módszerek folyamatos változáson mennek keresztül.
A disszertáció témája szempontjából természetesen a 2012. évi C. törvény, a hazai büntetőtörvénykönyvünk és a 2017. évi XC. törvény, a büntetőeljárásról szóló törvény,

valamint azok egyes rendelkezései állnak a vizsgálatom középpontjában a harmadik hipotézis eldöntésénél.

A feltételezésem alátámasztását szolgálja a külföldi, leginkább Európai Uniós szabályozások és az egyes uniós tagállamok számítógépes bűncselekményekkel foglalkozó szabályozása.

Mivel hazánk is az Európai Unió tagja, így az Unió által hozott irányelvek, rendeletek implementálásával próbál megfelelni a kötelezettségeknek, így jogszabályainkban is sok helyen visszaköszön, ha másképp nem is, a szószerinti angolnyelvű szöveg magyarra történő fordítása által, az uniós szabályok.

A feltételezésem elsődleges és egyben legfontosabb igazolása a 2014-2019-re vonatkozó Európai Parlament jelentése a kiberbűnözés elleni küzdelemről, amelyben felismerik, hogy a merev jogszabályalkotással nem érhető el hathatós eredmény.

Javaslat: Olyan keretjogszabály megalkotása, amelyben a változó információs technológiai környezetnek olyan szinten lenne képes eleget tenni, hogy a fejlődő számítógépes bűncselekmények és a kialakuló újabb és újabb elkövetési módszerek ne maradjanak büntetlenül. Mindamellett, hogy nem elég jelenleg, ha ez a változás csak az egyes országokon belül történik meg, hanem szükséges lenne akár Uniós, akár valamennyi ország tekintetében az azonos deliktumokat közös néven nevezni és egy ténylegesen közös büntetőpolitika kialakítása irányába haladnánk.

Ezen felül megoldást jelenthetne, ha a Számítástechnikai Bűnözésről szóló Egyezmény 2001-ben aláírt szövegét és javaslatait újra gondolnák és konkrétabb célokat és szabályokat alkotnának meg, amely nemcsak a bűncselekmény bekövetkezése esetén szükséges lépéseket fogalmazna meg, hanem a megelőzésre is hangsúlyt fektetne.

Negyedik hipotézisem: *az elektronikus bizonyítékok beszerzésénél azok eredetisége és hitelessége megőrzése érdekében a hagyományos bizonyítékok beszerzésétől és lefoglalásától eltérő módon végezhető csak el.*

Ahogy már említettem a Be. az elektronikus irat fogalmát meghatározza, amelybe beletartozik a papír alapon készült dokumentum digitalizált változata (szkennelés, pdf., vagy jpeg., stb. kiterjesztéssel) és épp úgy beleértendő az elektronikusan elkészített dokumentum időbélyeggel ellátva, amelyeket ugyanannak elnevezve nem épp szerencsés. De épp úgy nem a legjobb. Mint ahogyan az sem a legjobb megoldás, hogy eltárgyiasítjuk azokat, holott legtöbb esetben a vizsgálatuk, bizonyítékként történő használatuk sem a kézzel fogható dologként kezelendő.

További segítséget nyújtott Erdei Árpád, aki az új Be.-vel kapcsolatban, a tárgyi bizonyítási eszköz és az elektronikus adat közti problémát érzékelteti, amikor is kifejti a következő gondolatait:

„A tárgyi bizonyítási eszközt meghatározó 204.§ (2) bekezdése szerint *irat minden olyan tárgyi bizonyítási eszköz*, amely bármilyen eljárással adatokat rögzít, „így különösen a papíralapú vagy *elektronikus adatként létező szöveg, rajz ábra*". A rendelkezés ekként félreérthetetlenül tárgyi bizonyítási eszköznek minősíti az elektronikus adatot. Az elektronikus adatról szóló 205.§ (2) bekezdése szerint viszont, ahol a Be. „tárgyi bizonyítási eszközt említ, azon [...] az elektronikus adatot kell érteni, „kivéve, ha a Be. másként rendelkezik.

Mindezt jelzi, hogy a tárgyi bizonyítási eszköz és az elektronikus adat közötti különbséget a törvény nem tudja megragadni vagy pontosan kifejezni."[7]

Azaz a fentiekből is látható, hogy az elektronikus iratot tárgyi bizonyítási eszközként kezeli, így összemosódik, pedig a digitálisan (elektronikusan) keletkezett bizonyítékok kevésbé statikusak, a bizonyítási eljárás során a hatóságokok vagy az eljárásban bevont szakértő által nem könnyen reprodukálhatók, ugyanakkor könnyen manipulálhatók.

A hagyományos bizonyítékoktól eltérőek, alapvető tulajdonságaik sokszor nehezen meghatározhatók. *A digitális bizonyítékok változékony és átmeneti természete ellentétben áll az egyéb tudományágakban alkalmazott tartós fizikai jellemzőkkel – pl.: az ujjnyomatkészítés gerincmintáival...*[8].

Az elektronikus bizonyítékok esetében már annak vizsgálatának pontos dokumentálása már a bíróság előtti hitelesség megkérdőjelezhetetlenségéhez elég kell, hogy legyen. A pontos dokumentálás legalább a képrögzítő (pl.: videó felvétel készítése) eszközzel biztosíthatja a vizsgálat valódiságát.

Ötödik hipotézisem: a szakértő igénybevételének pontos és elfogadott szabályai nincsenek rögzítve egyetlen magyar jogszabályban sem. Ez különösen fontos lenne a számítógépes bűncselekmények nyomozása során, mivel a 2017. évi XC. törvény, a büntetőeljárásról szóló törvényben is a szakértő kirendeléssel kapcsolatos szakaszokban csak a „különleges szakértelem" kifejezés szerepel, ami ugyanakkor az információs társadalom fejlődésével összefüggésben nem lehet egyértelműen értelmezni, meghatározni, hogy a nyomozók által elvégzett kényszerintézkedés során mikor szükséges ténylegesen a szakértő vagy szaktanácsadó igénybevétele és milyen esetben elfogadható az, ha az ügyben eljáró szerv maga végzi el a vizsgálatot?

[7] Bánáti-Belegi-Belovics-Erdei-Farkas-Kónya: A büntetőeljárási törvény magyarázata (Hvgorac kiadó, Budapest 2018, 290. oldal)

[8] Eva A. Vincze (2016) Challenges in digital forensics, Police Practice and Research, 17:2, 183-194, DOI: 10.1080/15614263.2015.1128163

Természetesen a legkézenfekvőbb megoldás, ha a nyomozóhatóságok maguk is rendelkeznének olyan szakértelemmel, amely képessé tenné őket a szakértő helyett eljárva a vélemény elkészítésére. De: egyrészt sérülne a pártatlanság elve, hiszen a bizonyítás annak a feladata is lenne egyúttal, aki a vádhatóságot képviseli. Másrészt a hatóság által végzett szakértésnél nagyobb eséllyel fordulna elő a hanyagság, pontatlanság.

A további nehézségeket még hosszan lehetne sorolni (így például a pénz és oktatás hiányossága), de addig, amíg a különleges szakértelem nem kerül meghatározásra egyetlen jogszabályban sem, addig a szakértő által nyújtott „pluszt" kell elfogadni.

A szakértő kirendelésének szükségessége kérdésénél érdemes megemlíteni a dr. Simon Béla rendőr őrnagy úrral és Kiss Tibor rendőr őrnagy úrral folytatott közös kérdőívünket[9], amely a rendőrség hivatásos állományának számítógépes bűncselekmények. Nyomozásának képzéséhez járul hozzá, és amelynek célja, hogy felmérjük a kérdőív készítésekor a Nemzeti Közszolgálati Egyetem Rendészettudományi Karának hallgatói és a Rendőrség hivatásos állományához tartozó állomány tekintetében a kiberbűnözéssel, a tudatossággal kapcsolatos ismereteit.

[9] A két említett kollégám hozzájárult, hogy a kérdőívet a disszertációban felhasználjam

3 ÖSSZEGZÉS

„Egyre inkább függünk az internethez kapcsolt számítógép-rendszerektől; ezeken kommunikálunk, bankolunk, fizetjük az adóinkat, foglaljuk le utazásainkat, és rajtuk keresztül vásárolunk. Eközben fel sem merül bennünk, hogy ezek a rendszerek esetleg nem lesznek elérhetőek, és talán nem is mindig biztonságosak, nem mindig óvják meg személyes adatainkat. Az internet és az internetre épülő technológiák erőssége az, hogy általuk rengeteg dologhoz kapcsolódunk. Ám ez az erősség gyakran fogyatékosság is: mindig és mindenhonnan ki vannak téve támadásoknak. Ráadásul az internetes rendszereket olcsón meg lehet támadni. Az internet segít abban is, hogy névtelenek maradjunk.[10]”

A fenti idézet és Mark Russinovich Nulladik nap című könyve tökéletesen bemutatja azokat a kihívásokat, amelyekkel az internet felhasználók minden egyes nap látatlanul találkoznak és amellyel a kiberbűnözés elleni harccal foglalkozó szervezetek minden nap szembesülnek.

A számítógépes bűncselekmények az egyik legdinamikusabban fejlődő bűnözési típus, amely az informatikai eszközök elterjedésének, elérhetőségének és a folyamatos fejlesztéseknek köszönhetően kihívást jelent az államoknak, a gazdaságnak, a magán-és államiszférának, a társadalomnak, de igazi kihívást jelent a jogalkotóknak és a jogalkalmazóknak.

A XX. század sci-fi és fantasztikus filmei, regényei, jóslatai a XXI. század technikai fejlődésével kapcsolatban jóval meghaladta az akkor elképzelhető mértéket.

A nyomozóhatóság számára jelenleg igazi kihívást jelent, hogy felvegyék a harcot a kiberbűnözőkkel, akik a különböző technikai kihívásokat kihasználva maradnak láthatatlanok és anonimok a kibertérben, miközben a tevékenységük káros hatása érezhető, látható.

A kiberbűncselekmények üldözését célul tűzte ki az Európai Unió valamennyi tagállama, amely nemcsak a számítógépes bűncselekmények törvénybe történő nevesítésében, az uniós ajánlásokban, irányelvekben és rendeletek sorozatos megalkotásában, az államok Kiberbiztonsági Stratégiájában nyilvánul meg. A felsőoktatási intézmények keretein belül a szakemberek képzésével, az oktatók folyamatos kutatásával és szakmai fórumok szervezésben észlelhető az a pozitív szemlélet, amely biztosíthatja a hatékony fellépést a kiberbűnözőkkel szemben.

Pilisszentkereszt, 2018. október 22.

[10] Howard A. Schmidt, az Information Security Forum elnök-vezérigazgatója által írt előszó Mark Russinovich: Zero day c. Könyvébe (2012)

Summary

„Clearly, we are more and more dependent than ever on Internet-connected computer systems: it is the way we communicate, do our banking, pay our taxes, book our travel, and buy merchandise. We take for granted that these systems will always be there and are set to protect our privacy and are secure. The strength of the Internet and Internet technologies is that we are so connected. However, this strength is also a weakness – these systems are vulnerable to attack from anywhere by anyone, and with little capital investment. The Internet also facilitates maintaining anonymity [...][11]

This quote and Mark Russinovich's Zero Day novel perfectly demonstrate the hidden challenges that Internet users meet every day, and with which organizations fighting cyber - crimes have to face on a daily basis.

Cyber-crime is the fastest growing type of crime, and because of the prevalence, accessibility and continuous development of IT devices, they pose a real challenge to the different states, economies, private and government sectors, society, but especially, law makers and law enforcement.

The prediction of the 20th century sci-fi and fantasy movies and novels regarding the 21st century's technical development far exceeded what they thought would be possible then. It is now a real challenge for the investigating authorities to battle cyber criminals who remain invisible and anonymous in cyberspace by utilizing various technical challenges while the detrimental effect of their activity is clearly visible.

All member states of the European Union has set fighting cybercrime as a goal, not only by defining computer crimes in laws, giving EU recommendations and directives, creating a series of regulations, or the states' Cyber Security Strategy. We can now see a positive approach in higher education institutions in training specialists, providing ongoing research opportunities to trainers and organizing professional forums which can all lead to an effective fight against cybercriminals.

[11] Foreword by Howard A. Schmidt, Chairman of the board of the International Information Systems Security Certification Consortiumin, in Mark Russinovich's novel, Zero day (2012)

4 A SZERZŐ SAJÁT PUBLIKÁCIÓI

Gyaraki Réka: A nyomozóhatóság és a katasztrófavédelemm feladata a kiberbűncselekmények vonatkozásában (SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 15:(4) pp. 113-127.

Gyaraki Réka: Jogi szabályozás a nemzeti elektronikus adatvagyon, az azt kezelő információs rendszerek, létfontosságú információs rendszerek és rendszerelemek biztonságáról (*SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA* 15:(3) pp. 140-154.)

Gyaraki Réka: Az ördög pénze? A Bitcoin (DETEKTOR PLUSZ 23: pp. 1-3.)

Gyaraki Réka: Money of devil? (In: Radu I Motica, Lucian Bercea, Viorel Pasca (szerk.) Studii și Cercetări Juridice Europene = European Legal Studies and Research: Conferința Internațională a Doctoranzilor în Drept = International Conference of PhD Students in Law. 619 p. Konferencia helye, ideje: Bukarest, Románia, 2016.11.25-2016.11.26. Temesvár: Universitatea de Vest din Timisoara, Facultatea de Drept, 2016. pp. 173-178. (Facultatea de drept Univ. de vest din Timisoara = Faculty of Law West Univ. Timisoara)

Gyaraki Réka, Rottler Violetta: Drónok kora- személy-és vagyonbiztonság a XXI. században In: Bányász Péter, Kiss Dávid, Orbók Ákos (szerk.), A tudomány kapujában: Poszter kiadvány. 108 p. Konferencia helye, ideje: Budapest, Magyarország, 2015.10.28 Budapest: Magyar Hadtudományi Társaság, 2016. pp. 76-77. (ISBN:978-963-12-4965-1)

Gyaraki Réka: Az informatikai bűnözés a hazai jogi szabályozás aspektusából (In: Ács Kamilla, Bencze Noémi, Bódog Ferenc, Haffner Tamás, Hegyi Dávid, Horváth Orsolya Melinda, Hüber Gabriella Margit, Kovács Áron, Kis Kelemen Bence, Lajkó Adrienn, Schilli Gabriella Krisztina, Szendi Anna, Szilágyi Tamás Gábor, Varga Zoltán (szerk.), Book of Abstracts = Absztraktkötet: V. Interdiszciplináris Doktorandusz Konferencia. 191p. Konferencia helye, ideje: Pécs, Magyarország, 2016.05.27-2016.05.29. (Pécsi Tudományegyetem Doktorandusz Önkormányzat) Pécs: Pécsi Tudományegyetem Doktorandusz Önkormányzat, 2016. p. 43. (ISBN:978-963-429-038-4)

dr Gyaraki Réka: The legal regulation of rendering electronic data inaccessible(DE IURISPRUDENTIA ET IURE PUBLICO: JOG- ÉS POLITIKATUDOMÁNYI FOLYÓIRAT 10:(1) Paper 03. 7 p. (2016)

Gyaraki Réka: A drónok használatának hazai szabályozása(MAGYAR RENDÉSZET 2016:(1) pp. 43-54. (2016)

Gyaraki Réka: Cyber attacks against financial institutions(KRITISCHE ZEITEN: ZEITSCHRIFT FUR HUMANWISSENSCHAFTEN 7:(3-4) pp. 134-140. (2016)

Gyaraki Réka: Az elektronikus adat hozzáférhetetlenné tételének jogi szabályozása(TÁRSADALOM ÉS HONVÉDELEM 19:(2) pp. 57-64. (2015)

Gyaraki Réka: Számítógépes bűncselekmények és az ellenük való védekezés(In: Christián László (szerk.)Információvédelem. 262 p. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2015. pp. 175-189. (ISBN:978-615-5527-24-1)

Gyaraki Réka: Számítástechnikai környezetben elkövetett gazdasági bűncselekmények(In: Erik Stenpien, Miskolczi Bodnár Péter (szerk.)X. Jogász Doktoranduszok Országos Szakmai Találkozója. Konferencia helye, ideje: Budapest, Magyarország, 2015.05.16 Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2015. pp. 42-52.(Jog és Állam; 20.)

Gyaraki Réka: Az elektronikus adat hozzáférhetetlenné tételének jogi szabályozása(In: Kiss Dávid, Orbók Ákos (szerk.),A haza szolgálatában 2014 konferencia rezümékötet. 170 p. Konferencia helye, ideje: Budapest, Magyarország, 2014.10.31 Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 48-50. (ISBN:978-615-5491--88-7)

Gyaraki Réka: Az informatikai biztonság szükségessége(In: Kiss Dávid, Orbók Ákos (szerk.) A haza szolgálatában 2014 konferencia rezümékötet. 170 p. Konferencia helye, ideje: Budapest, Magyarország, 2014.10.31 Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 156-158. (ISBN:978-615-5491--88-7)

Gyaraki Réka: Gyermekek biztonsága a kibertérben: Önkormányzati rendészeti kutatás a Nemzeti Közszolgálati Egyetem Rendészetelméleti Kutatóműhely szervezésében, A kiberbiztonság aktuális kérdései, 2014. november 12. 23 p.(2014))

Gyaraki Réka: A probléma megoldva?!(TÁRSADALOM ÉS HONVÉDELEM 17:(3-4) pp. 535-543. (2013)

Gyaraki Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények(In: Gaál Gyula, Hautzinger Zoltán (szerk.), Tanulmányok "A biztonság rendészettudományi dimenziói - változások és hatások" című tudományos konferenciáról. 524 p. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2012. pp. 235-249.(Pécsi Határőr Tudományos Közlemények; 13.)

Gyaraki Réka: A számítógépes bűnözés elleni harc az új büntetőtörvénykönyvvel(MAGYAR RENDÉSZET 12:(4) pp. 55-62. (2012))

Gyaraki Réka: Internetes csalás vagy SCAM(MAGYAR RENDÉSZET 12:(1) pp. 40-47. (2012))

Gyaraki Réka: A tiltott pornográf felvétellel visszaélés bűncselekménye(In: Ádám Antal (szerk.)PhD tanulmányok 11. 671 p. Pécs: PTE ÁJK Doktori Iskola, 2012. pp. 339-360.)

Gyaraki Réka: Az on-line elkövetett szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye (INFOKOMMUNIKÁCIÓ ÉS JOG 6:(41) pp. 215-221. (2010))