HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám

SIMON BÉLA[1]

A rendőrség állományának felkészültsége a kiberbűnözésre

The Preparedness of Police Personnel to Cybercrime Threat

Absztrakt

Magyarország a Nemzeti Kiberbiztonsági Stratégia[2] *megalkotásának időpontjában európai szinten is előremutató intézkedéseket tett a kibervédelem, kiberbiztonság területén. Számos intézkedés történt annak érdekében, hogy a kibertér, mint a gazdasági és társadalmi élet meghatározó pillére szabad, biztonságos és innovatív környezetté váljon. Az új Kiberbiztonsági Stratégia alkotásának időszakában is szükséges számot vetni arról, hogy az állam egyik legfontosabb rendészeti szerve: a rendőrség személyi állományának képzettsége menynyiben felel meg a korábban meghatározott célok megvalósításához. A vizsgálat eredményeit kérdőíves felmérés és személyes interjúk adják. A megállapítások szerint a rendőrség személyi állománya a nem specializált egységeken kívül nem rendelkezik a kiberbűncselekmények visszaszorításához szükséges magas szintű ismeretekkel.*

Kulcsszavak: rendőrség, felmérés, kiberbiztonság tudatosság, kiberbűncselekmények, ismeretszint

Abstract

At the time when the National Cybersecurity Strategy was created, Hungary made progressive measures in the field of cyber security, cyber security. Numerous measures have been taken to make cyberspace as the determining pillar of economic and social life a free, secure and innovative environment. During the creation of the new Cyber Security Strategy, it is also necessary to review whether it is one of the most important law enforcement agencies in the state: the

[1] Nemzeti Közszolgálati Egyetem – National University of Public Service, E-mail: Simon.Bela@uni-nke.hu ORCID: 0000-0002-1555-3690

A mű a KÖFOP-2.1.2-VEKOP- azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett Ludovika Kiberbiztonsági Kiemelt Kutatóműhely keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám

police staff's qualifications meet the goals set out above. The results of the survey are provided by questionnaire surveys and personal interviews. According to the findings, the police personnel do not have the high level of knowledge required to curb cybercrime. However, this statement does not apply to specific anti-cybercrime units.

Key words: police, survey, cyber security awareness, cyber crime, knowledge level

Minden fejlett bűnüldöző szerv vezetőjének hosszú távú stratégiájában vizionálnia kell, hogy az egyes jogsértő cselekmények milyen változásait prognosztizálja és azokra milyen ellenlépéseket kíván tenni. A veszélyeztetettség és a fertőzöttség szintjére tekintettel milyen erőforrásokat delegál egy területre, vagy a meglévőket miként fejleszti, vagy alakítja át. Nincs ez másként a kiberbűnözés elleni fellépés területén sem. Az azonban különösen nehéz feladat, hogy kiszámításuk, miként fognak alakulni a kibertérhez kapcsolódó bűncselekmények, hiszen az elmúlt évek statisztikai adatsoraiból pontos trendek nem rajzolhatók ki.[3]

Az mindenképp valószínűsíthető, hogy e cselekmények száma a következő években emelkedni fog, amint az is kijelenthető, hogy egyre jobban felértékelődik a bűnüldöző szervek állományában az a tudás, ami a digitális forrásból származó bizonyítékok kinyerésére, rögzítésére, elemzésére és értékelésére képes.

Napjainkban a kriminalisztika olyan forradalmi változáson esik át, amelyhez foghatót az információk továbbításában az internet létrejötte okozott. Továbbra sem lebecsülhetők a kriminalisztika klasszikus és speciális eszközei[4], de az jól látható, hogy az infokommunikációs eszközökből, adatbázisokból kivonható bizonyítékok felé tolódik el a súlypont[5].

A vizsgálat célja, hogy segítséget nyújtson a döntéshozóknak abban a kérdésben, hogy mely területeken és mely szinteken indokolt a rendőrség személyi állományának képzését fejleszteni, illetve segítségül szolgálhat a rendészeti szervek oktatásában résztvevő személyeknek a képzési portfolió fókuszálásában.

Természetesen a teljes és átfogó képhez nagy segítséget nyújtana egy e tárgykörben készített korábbi – akár 5 évvel ezelőtti – vizsgálat, de ilyen nem készült.

---

[3] Simon Béla: A kiberbűnözés aktuális trendjei. Magyar Rendészet, 2018. „A Haza szolgálatában 2017" konferencia kötet – megjelenés alatt.

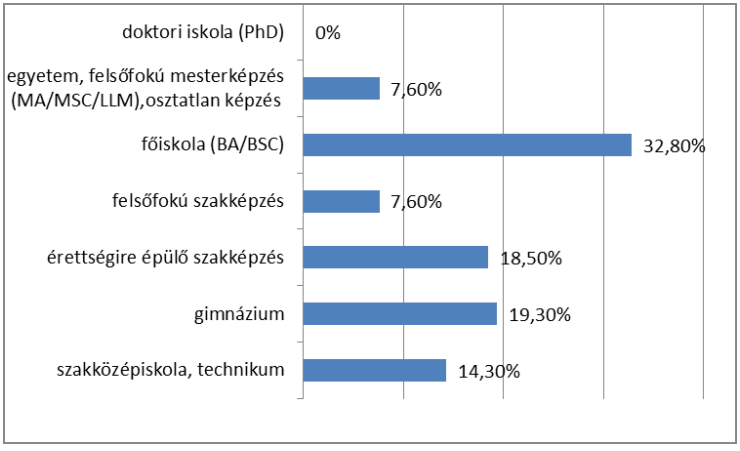
[4] „A bűncselekmények felderítése, bizonyítása új lehetőséghez, erőforráshoz jutott a rendőrségről szóló 1994. évi XXXIV. törvény és a végrehajtását szabályozó normák szerint folytatott titkos információgyűjtő tevékenység, valamint a büntetőeljárásról szóló 1998. évi XIX. törvény által szabályozott nyomozóhatóság egyéb, illetve titkos adatszerző tevékenységei által." Nyeste Péter: A bűnügyi hírszerzés. Magyar Rendészet, 2012/4. 30. o.

[5] minden IT eszközöket, mobiltelefont használó emberről megállapítható (és az egyes szolgáltatók, és szolgálatok meg is állapítják), hogy merre jár, kivel kommunikál, mennyit mozog, milyen az egészségi állapota, érdeklődési köre, anyagi helyzete, hangulata, irányultsága, politikai nézetei, - melyekből következtetéseket vonhatnak le várható tevékenységére, szándékaira.

A kérdőíves vizsgálat a Nemzeti Közszolgálati Egyetem - Rendészettudományi Kar – Kiberbűnözés Elleni Tanszéke által[6] összeállított online felületen elérhető kérdésekre támaszkodott, melyet a megkérdezettek 2018. január hónapjában töltöttek ki. A kérdőív címzettjei a Kar levelező munkarendben tanulmányokat folytató alap (BA) és mester (MA) szakos hallgatói – összesen 119 fő. A felkérés online felületen jutott el a címzettekhez, melyben a kérés arra irányult, hogy ezzel a kitöltéssel önkéntesen segítség a Kiberbűnözés Elleni Tanszék munkáját a képzések kialakításában. Bár a cél a rendőrség állományába tartozó személyek ismereteinek vizsgálata volt, de volt a Nemzeti Adó- és Vámhivatal (4fő), Büntetésvégrehajtási Szervezet(1fő), Katasztrófavédelem(1fő), Katonai Rendészet (1fő), önkormányzati rendészet (1fő) részéről is kitöltő.

A tanulmány első kérdései a megkérdezettek demogarafiai adatait célozták. 1994-ben a magyar rendőri összlétszám mindössze 8%-a volt nő. A rendőrség személyi állományának összetételéről 2004-ben készült statisztikai elemzés kimutatta, hogy 10 év alatt megduplázódott a rendőrnők aránya, 16%-ra nőtt.[7] Az azóta eltelt időszakban ez az arány a törvényi rendelkezésekkel összhangban[8] a nők arányának növekedését eredményezte. A rendőrség hivatásos állományában a férfiak és nők aránya 78%-22%, amelytől a felmérésben szereplők aránya nem tért el szignifikánsan, mivel a nemre vonatkozó kérdésre válaszoló 118 válaszadó 19,5%-a volt nő.

A legmagasabb iskolai végzettségre vonatkozó kérdésre 119 fő adott választ, melyeknek megoszlását az alábbi ábra mutatja:

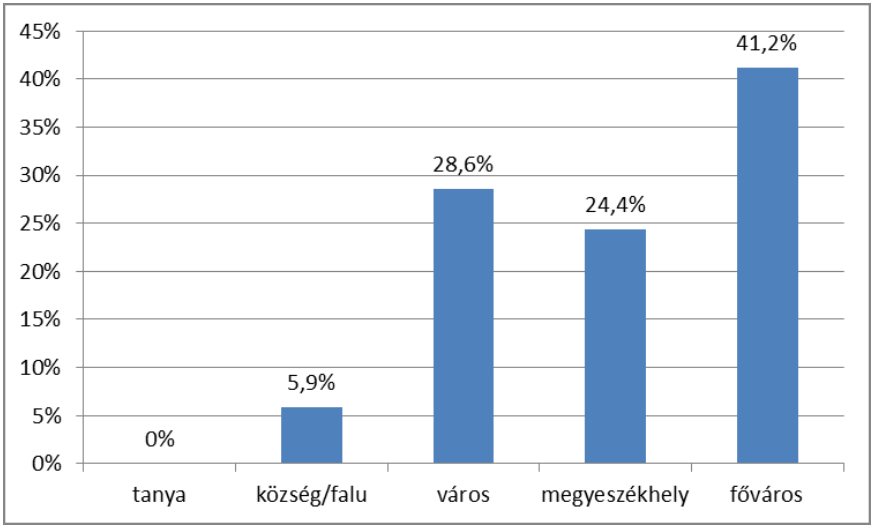


Forrás: saját felmérés

[6] Az összeállításban részt vettek: dr. Gyaraki Réka, Kiss Tibor és dr. Simon Béla.
[7] Sárközi Irén: Nők a rendészetben. Doktori (PhD) értekezés, Zrinyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, Budapest, 2008. 9. o.
[8] Az egyenlő bánásmód követelménye a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról 2015. évi XLII. törvény 5.§ (2) bekezdés.

A következő kérdés a munkahely településtípusára vonatkozott. Az eredmények tükrözik a rendőri szervek eloszlását. Magyarországon az Országos Rendőrfőkapitányság alárendeltségében területi szintként 19 megyei, fővárosi főkapitányság, helyi szintként 154 városi, 22 kerületi kapitányság és 21 határrendészeti kirendeltség áll. A körzeti megbízotti irodák kistelepülésen és a fővárosban is jelen vannak. Központi szinten ennek megfelelően hozzávetőleg 1.050 fő, területi szinten 5.150 fő és helyi szinten 27.250 fő teljesít szolgálatot. Amint azt a bűnügyi fertőzöttségi adatok[9] is szükségessé teszik az országos átlagot jelentősen meghaladó rendőri jelenlét szükséges Budapesten.

A szolgálatellátás helyére vonatkozó kérdés volt: Jelenlegi munkahelyének mi a településtípusa?



Forrás: saját felmérés

A kiberbűncselekmények kezelésének intézményesített formája a rendőri alapképzésben nem értékelhető.[10] A rendőri felsőfokú oktatásban (BA képzés) az elmúlt évek során jelentős fejlesztések valósultak meg:

- az egyes jogi és kriminalisztikai tárgyakban a kiberbűncselekmények felderítése, nyomozása, bizonyítása során szükséges ismeretek megemelt időkeretben jelennek meg a képzésben
- célzottan e terület elsajátítását szolgáló szabadon választható és kötelező kurzusok kerültek bele a képzési programba.

[9] Bővebben: http://www.police.hu/hu/bunugyiterkep (2018. 01. 05.)
[10] GENVAL ország értékelő jelentés 174. o. http://data.consilium.europa.eu/doc/document/ST-14583-2016-REV-1-DCL-1/en/pdf (2018. 01. 05.)

— kialakítás alatt van egy kibernyomozó (nappali munkarendben) és egy informatikai nyomozó (levelező munkarendben) szakirány létesítése, amely az eredményes akkreditációt követően specialisták képzését hivatott megvalósítani

A mesterképzési szakokon folyamatban van a kiberbűnözéssel kapcsolatos kurzusok fejlesztése és a Rendészettudományi Doktori Iskola keretein belül is növekszik az e témával kapcsolatos témakiírások száma.

Mindezekkel együtt kijelenthető, hogy a rendőrség aktív állományában szolgálatot teljesítő személyek jellemzően nem a rendőri képzési rendszerből szerezték be a kiberbűncselekmények elleni fellépéshez szükséges ismereteiket.

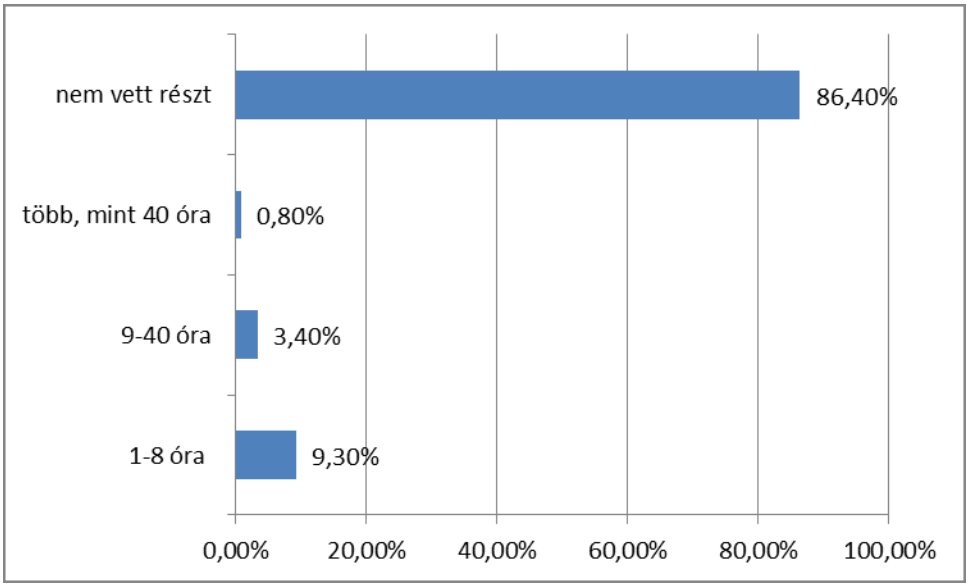
Ez a tudás tipikusan 3 forrásból származik:

— már ilyen tárgyú ismeretekkel, képzettséggel jelennek meg a rendőri egységekhez. Ekkor a képzettségi szint jellemzően nem felsőfokú, mivel a rendvédelmi szervekhez képest az informatikai terület jobb anyagi kilátásokat kínál.
— az informatikához, számítástechnikához érdeklődéssel forduló rendőrök önképzés keretében sajátítják el
— a rendőrségen szolgálatot teljesítő személyek különféle nemzetközi képzéseken vesznek részt. Erre elsődlegesen a specializált szervek munkatársai (Budapesti Rendőr-főkapitányság – BRFK Korrupciós és Gazdasági Bűnözés Elleni Főosztály - Pénzhamisítás és Csúcstechnológiai Bűnözés elleni Osztály - Csúcstechnológiai Bűnözés Elleni Alosztály, valamint a Nemzeti Nyomozóiroda Kiberbűnözés Elleni Főosztály) kapnak arra lehetőséget, hogy az ILEA (International Law Enforcement Academy – Nemzetközi Rendészeti Akadémia), Amerikai Egyesült Államok Titkosszolgálatának (U.S. Secret Service) és a Szövetségi Nyomozó Iroda (FBI), valamit a Közép-európai Rendőrakadémia, ECTEG (European Cybercrime Training And Education Group- Európai Kiberbűnözési Tréning és Oktatási Csoport), EUROPOL(Európai Rendőrségi Hivatal), CEPOL (European Union Agency for Law Enforcement Training), OLAF (Európai Csalásellenes Hivatal) képzésein részt vegyenek .

Magyarországon a továbbképzési lehetőségek nem kellően fejlettek a kiberbűnözés elleni fellépést illetően. A Belügyminisztérium Vezetőképzési, Továbbképzési és Tudományszervezési Főosztály akkreditált képzései szűk kör részére nyújtanak ismereteket. Jellemzően ad hoc jellegű, nem rendszeres és nem tervezett képzések állnak rendelkezésre[11].

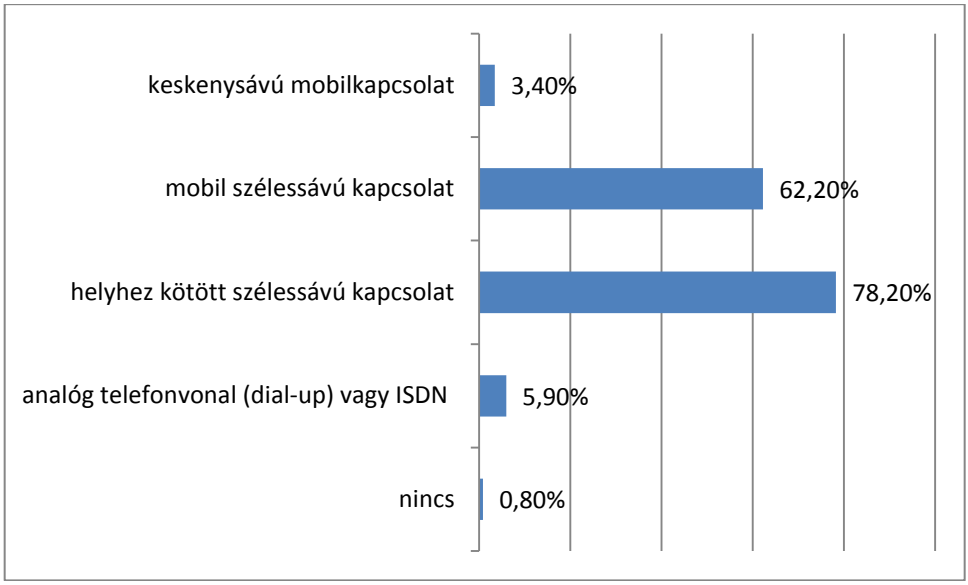
A képzési lehetőségek figyelembevételével a kérdőívben az szerepelt, hogy: „Vett már részt kiber-bűncselekmények nyomozásával, kezelésével kapcsolatos képzésben?” A válaszadó 118 főből 102 fő semmilyen képzésben nem vett részt e tárgykörben.

[11] Bővebben: Simon Béla: Rendészettudományi Kar – Kiberbűnözés elleni kapacitásfejlesztési koncepciója – munkaanyag, 2016.



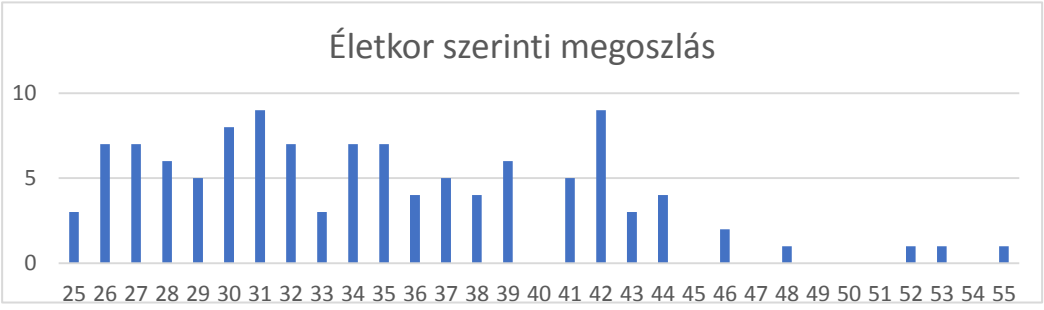
Forrás: saját felmérés

Annak vizsgálatára, hogy a megkérdezettek mennyiben alapozhatnak munkájuk során az infokommunikációs eszközökről, internet használatáról magánemberként megszerzett tudásukra – indokoltnak láttuk e vonatkozásban is felmérni ismereteiket, lehetőségeiket. Kérdésként tettük fel, hogy A háztartásában milyen internet hozzáférés áll rendelkezésre? Jeleztük, hogy több válasz is lehetséges. A válaszadó 119 főből mindössze egy személy nyilatkozta, hogy nem rendelkezik internettel. Ez abból a szempontból is lényeges, hogy a későbbi e-learning anyagok kidolgozása és az életen át tartó tanulás elve mentén van lehetőség arra, hogy a szükséges ismereteket a célzott állomány otthonában, illetve otthonában is feldolgozza, elmélyítse.



Forrás: saját felmérés

Összehasonlításként a KSH adatai szerint a rendszeres internet használók aránya a 16-74 éves személyek arányában Magyarországon 2017 évben 76% volt[12]. A jelen kutatásban megkérdezettek életkor szerinti besorolását az alábbi diagram mutatja:



Forrás: saját felmérés

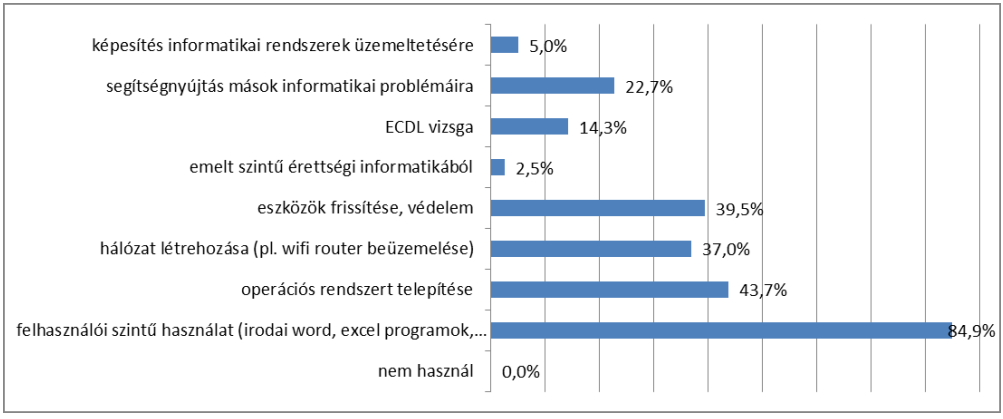
Az eredmények hasonlóak a szélesebb életkori sávot vizsgáló országos felmérés eredményeihez. Ez vélhetően abból is adódik, hogy a megkérdezettek csupán 5,2%-a volt 45 év feletti, és a legidősebb megkérdezett személy 55 éves volt. Így tehát nem szerepeltek a

[12] https://www.ksh.hu/docs/hun/eurostat_tablak/tabl/tin00091.html (2018. 01. 08.)

vizsgált sokaságban az idősebb korosztály tagjai, akik ezt az arányt rontották volna és nem szerepeltek a 16-24 év közötti személyek sem, akik ezt az arányt vélelmezhetően javították volna.

Érdekes adat az is, hogy a megkérdezettek majdnem kétharmadának fontos a folyamatos internet elérés és ezért mobiltelefon előfizetéseikben internetes csomag is szerepel. Ez olyan fejlesztések lehetőségét nyitja meg, amely az állomány azonnali elérésének (pl riadóztatás) megvalósítási lehetőségét bővíti. Ezen túlmenően lehetőséget biztosít lokálisan egy adott környezetben található rendőrök szolgálatba léptetésének megvalósítására.[13]

A következő kérdés arra irányult, hogy a megkérdezett milyen szinten ért az informatikához? Több válaszadásának lehetősége mellett a válaszadók közül senki sem volt, aki ne használna számítógépet.



Forrás: saját felmérés

Bár ECDL vizsgával csak a megkérdezettek 14,3%-a, illetve emelt szintű informatika érettségivel 2,5% rendelkezik, de ezek az alacsony számok jelentős részben visszavezethetők arra, hogy a megkérdezettek többsége koránál fogva akkor végezete középiskolai tanulmányait, amikor e számonkérési formák jóval kevésbé voltak elterjedtek.

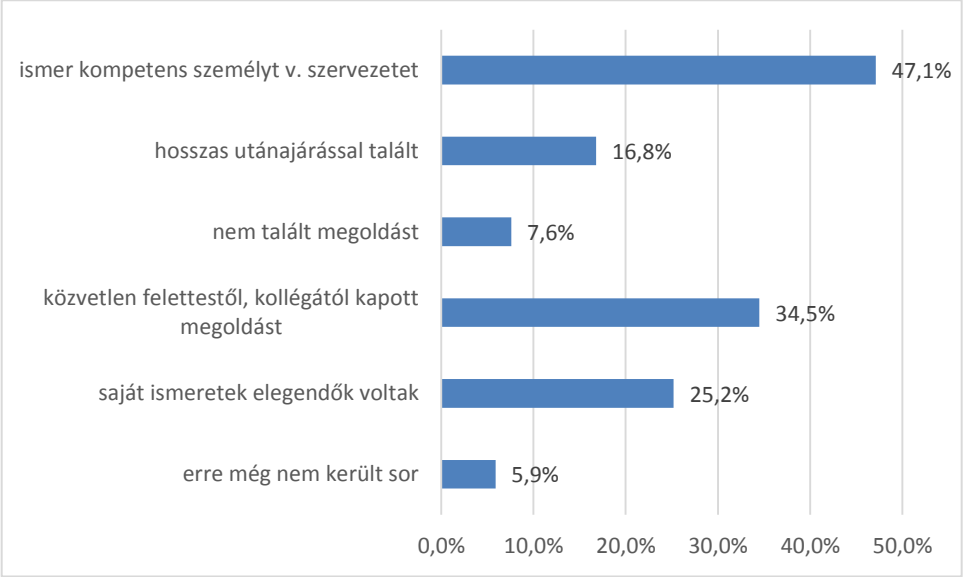
A kutatás érdekes eredménye volt, hogy a megkérdezettek közül 6 fő úgy nyilatkozott, hogy van informatikai rendszerek üzemeltetésére képesítése. Mivel a kérdőív anonim volt, így nincs lehetőség az érintettek közvetlen megkérdezésére, de az aránytalanul magas szám azt jelentené, hogy a rendőrség állományából több, mint 2100 fő tulajdonképpen rendszergazdai képesítéssel bír. Vélhetően olyan személyek is jelölték ezt a választ, akik az ECDL vizsga birtokában az informatikai rendszer és a Büntető Törvénykönyvben sze-

[13] Például olyan rendőri alkalmazás kifejlesztése által, amivel a rendőr szolgálati pihenőjét, akár pihenőnapját töltve is kaphat értesítést egy azonnali intézkedést és jelentős számú élő erőt igénylő eseményben való intézkedésre. Ekkor túlmunka elrendelése mellet önként szolgálatba léphet.

replő információs rendszer[14] fogalmakat egymás szinonimájaként értelmezve a számítógép üzemeltetési képzettséget kívánták jelölni.

Az informatikai infrastruktúra és képzettség feltárását követően a kiberbűncselekményekkel kapcsolatos tevékenységre fókuszált a kérdőív:

Ha szolgálati feladati ellátása során informatikával kapcsolatos kérdés merül fel, akkor tud segítséget kérni? (több válasz is lehetséges)



Forrás: saját felmérés

A kérdésre adott válaszok azért kiemelten fontosak, mert a kiberbűncselekmények jelenlegi volumenéről sem áll rendelkezésre pontos statisztikai adatsor, illetve arra sem állnak rendelkezésre szűrések, hogy a büntetőeljárások során milyen arányban van szükség informatikai szakértők bevonására. Az informatikai szakkérdés határa folyamatosan változik, illetve jelentős mozgást mutat azon esetek száma, amikor nem külső szakértő igénybevételével kerül eldöntésre egy informatikával kapcsolatos speciális kérdés, hanem a rendőrség belső állományából kiképzett személyek rendőri jelentésben adnak választ a felmerülő problémákra.[15]

[14] Büntető törvénykönyvről szóló 2012. évi C. törvény 459.§ (1) bekezdés 15. pont értelmében információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

[15] Simon Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle, 2017/7–8. 87–105. o.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám

A kiberbűncselekmények nyomozása és az informatika egy olyan szakterület, ahol az ismeretek folyamatos karbantartása szükséges. A fejlődő technikai megoldások, az egyre szofisztikáltabb elkövetési magatartások szükségessé teszik a továbbképzések tartását. Amíg jellemzően például az élet elleni bűncselekmények nyomozására megszerzett ismeretek lassú idő alatt avulnak el, addig tárgyalt szakterületünkön ez rövid időn belül megtörténik. Természetesen nem lehetséges, hogy minden kiberbűncselekménnyel esetlegesen foglalkozó munkatárs folyamatosan minden területen naprakész információkkal rendelkezzen. A helyes arány kidolgozása szükséges ahhoz, hogy a bűncselekmények összetettsége, elszaporodottsága által befolyásoltan álljon rendelkezésre a kiképzett állomány[16].

Országos szinten még nem alakult ki olyan rendszer, amelyben a területi és helyi szervek munkatársai a hatáskörükbe tartozó bűncselekmények vonatkozásában (legalább) egy olyan mentor/multiplikátor elérhetőségét ismerik, akitől a digitális bizonyítékok rögzítésére, elemzésére, valamint a nyomozások lefolytatásához szükséges információkat beszerezhetik, de a tervek ezt célozzák az ORFK Bűnügyi Főosztály Korrupció és Gazdasági Bűnözés Elleni Osztály, mint szakirányító szerv részéről is. A képzésekben a Nemzeti Nyomozóiroda Kiberbűnözés Elleni Főosztály, valamint A BM Nemzetközi Oktatási Központ aktív részvétele válik szükségessé.

A 47,1% os arány – akik tudják azon személyek, szervezetek elérhetőségét, akiktől segítséget kérhetnek – nagyon alacsony. Nem várható el, hogy e területen a Tevékenységirányítási Központok adjanak iránymutatást. E szám emelése kiemelten fontos a gyors és hatékony intézkedések végrehajtásához.

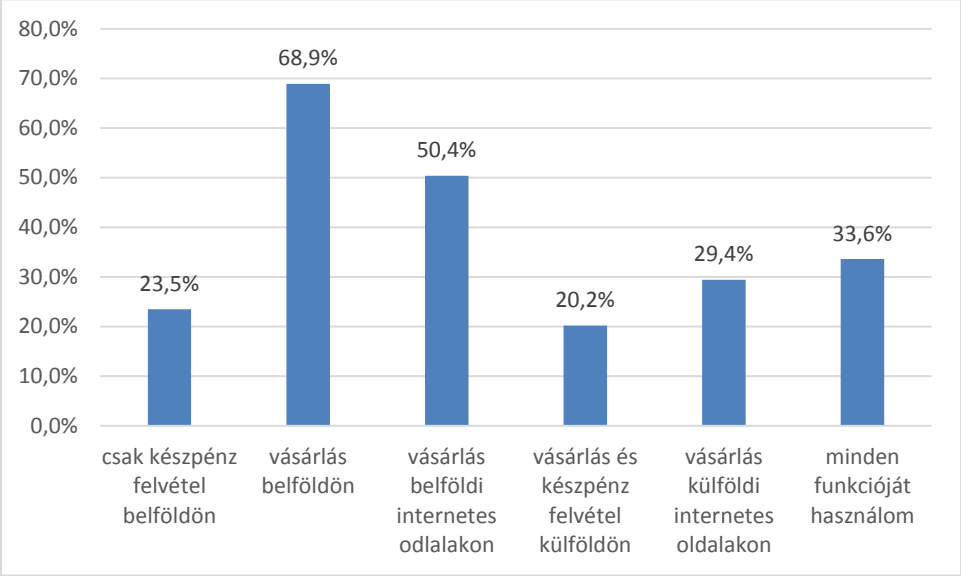
A kérdőív nem tudta feltárni azt a problémát sem, hogy a felettesektől, kollégáktól, hosszas telefonálás után elért személyektől beszerzett információ mennyire volt szakszerű. Ennek feltárása további kutatás célja lehet.

A kiberbűncselekmények következő fontos területe a készpénz - helyettesítő fizetési eszközökhöz kapcsolódó visszaélések. Bár 2017 harmadik negyedévében ismét jelentősen bővült a magyarországi fizetési kártya elfogadói hálózat. Részben ennek is köszönhetően ismét több mint 25 százalékkal nőtt a kártyás vásárlási forgalom, amelynek már 69 százaléka bonyolódott a gyors és korszerű érintéses technológia használatával. 2017 év végére a hazai kibocsátású fizetési kártyák száma több mint 9 millió darab volt. A 2017-es év alatt folytatódott az internetes vásárlási forgalom jelentős bővülése is, mind darabszámban, mind értékben 37 százalékos volt az emelkedés ezen a téren, azonban a teljes kártyás vásárlási forgalom kis része (6, ill. 10 százalék darabszámot, ill. értéket tekintve) bonyolódik csak ilyen módon. 2017 második negyedévében a kibocsátói oldalon elkövetett fizetési kártyás visszaélések száma (9949 darab) a forgalom növekedési üteménél kisebb mértékben, 9 százalékkal nőtt, míg az okozott kár értéke (256 millió forint) 20 százalékos csökkenést mutatott az előző év azonos időszakához képest. Továbbra is jellemző, hogy a visszaélések főként internetes vásárlási tranzakciókat érintik, mind darabszámban, mind ér-

[16] Simon Béla: Rendészeti szervek együttműködése a kiberbűnözés ellen. Megjelenés alatt a Nemzetbiztonsági Szemlében.

tékben körülbelül a visszaélések 80 százaléka köthető ehhez a forgalomhoz. Az elfogadói oldalon szintén a forgalom bővülésénél kisebb mértékben emelkedett a visszaélések száma (1179 darab) és az okozott kár értéke (50 millió forint), ami 10, ill. 4 százalékos növekedést jelentett a tranzakciószámot és az értéket tekintve az előző év azonos időszakához képest. Kijelenthető, hogy csökkent a fizetési kártyákkal elkövetett visszaélések forgalomhoz viszonyított aránya, azaz még biztonságosabbá vált a kártyahasználat a fogyasztók számára[17]. Mindezek mellett is a kiberbűncselekmények egyik fontos kategóriája maradt a bankkártyákkal kapcsolatos bűnelkövetés[18] E körben is indokolt volt felmérni az állomány ismereteit a készpénz helyettesítő fizetési eszközök használatáról.

A megkérdezettek bankkártyahasználati szokásaira vonatkozóan az alábbi válaszok születtek:



Forrás: saját felmérés

A kapott adatokból a csak készpénzfelvételt jelző válaszadók magas száma adhat okot további vizsgálatok folytatására, mivel az meglehetősen magas még ha figyelembe vesszük a 150.000Ft-ig terjedő ingyenes felvétel lehetőségét, akkor is jelentős az aránya azoknak, akik ezt a pénzügyi rendszernek és ügyfélnek is költséges megoldást választják.

[17] http://www.mnb.hu/letoltes/penzforgalmi-tablakeszlet-tajekoztato-20171215.pdf (2018. 01. 07.)
[18] Amint azonban bevezetésre kerül az 5mp-en belüli átutalás (2019.07.01-től), és a bankkártyáktól független fizetési módok terjednek el (kriptovaluták, különféle telefonos alkalmazások stb.) úgy e visszaélés típus egyre jobban összemosódik várhatóan az információs rendszerek elleni támadásokkal.

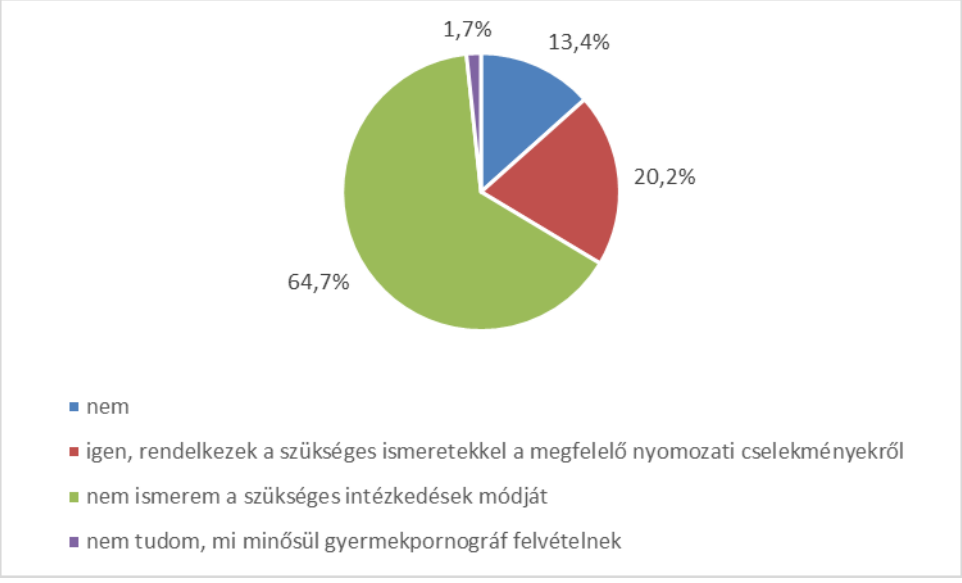
A következő kérdés a Btk. 375. §(5) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás elkövetése esetén ajánlott sértetti magatartás ismeretére kérdezett rá: Ha Önhöz állampolgári jelzés érkezik, hogy az érintett személy értesítést kapott SMS-ben, hogy a bankkártyájával illetéktelenek éppen vásároltak, akkor Ön mit javasol számára?

A válaszadók 88,2%-a választotta a „Tiltsa le és tegyen azonnal feljelentést" választ, míg a fennmaradó 11,8% a „Vegye fel az összes pénzt a számláról, amit a bankkártyával el lehet érni, tiltsa le kártyáját, majd tegyen feljelentést" választ jelölte meg.

A „Nem tudom" és a „Felesleges feljelentést tenni, csak tiltsa le a kártyát és vegye fel az összes pénzt" választ senki sem jelölte meg.

A kiválasztott lehetőségek mindegyike lehet a követendő legjobb magatartás, de ennek megválaszolásához jellemzően nem szükséges rendészeti képzés, hiszen ez a bankkártya használathoz kapcsolódó általános ismeret.

A következő kérdés a gyermekpornográfiával kapcsolatos ismereteket vizsgálta, vajon tisztában van-e a válaszadó, milyen elsődleges intézkedések megtétele szükséges, amennyiben gyermekpornográfiával kapcsolatok internetes tartalomról kap bejelentést.



Forrás: saját felmérés

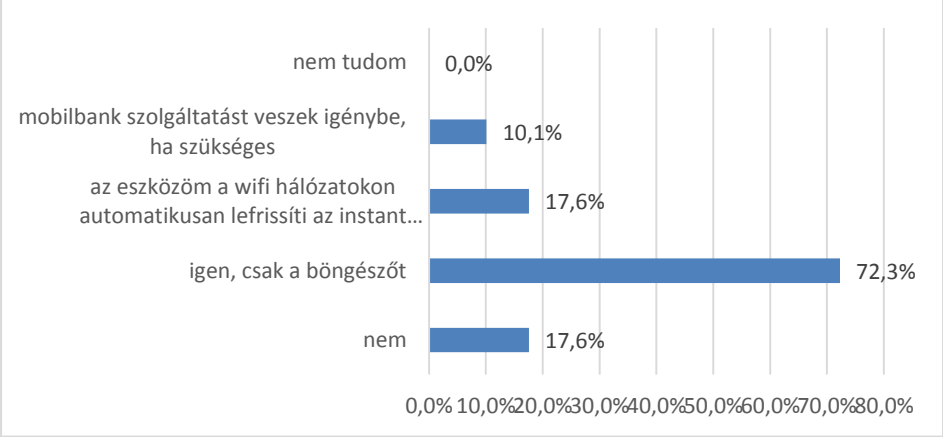
Látható, hogy a válaszadók közül majdnem minden hatodik személy ismeretei teljes mértékben hiányoznak. Mindössze a megkérdezettek 20%-a gondolja úgy, hogy egy ilyen bűncselekmény nyomozásához szükséges ismeretekkel rendelkezik. 64,7%-a a válasz-

adóknak szinte csak olyan szinten áll, hogy felismeri a cselekmény társadalomra veszélyességét, de az ellene való fellépésre nincsenek részletes információi. Egy olyan bűncselekmény esetében, ahol:

- rendkívül nagy a látencia
- az elkövetők egy jelentős része intellektuális elkövető, és a konspirációra nagy figyelmet fordít
- a bűncselekményekkel okozott kár, azaz a sértettekre gyakorolt hatása sok esetben egész életre kiható
- e bűncselekmény típus sokszor csak titkos információgyűjtés segítségével deríthető fel, amihez további speciális gyakorlati ismeret szükséges

A gyermekpornográfia bűncselekmény bűnügyi statisztikában történő megjelenése[19] rendkívül nagy kilengésekkel, de nyilvánvalóan hatalmas látenciával[20] mutatja a fertőzöttséget. Ez a terület, ahol jelentős erőforrásokkal és a stratégiához kapcsolódó bűnüldözői, bűnmegelőzési akciótervet indokolt kidolgozni.[21]

A következő kérdés az információbiztonságra vonatkozó attitűdök felmérését célozta: Szokott-e nyilvános wi-fi hálózatokhoz kapcsolódni? (étteremben, vonaton, áruházban, közterületen, ha igen, akkor milyen műveleteket hajt végre?)(több válasz is lehetséges)



Forrás: saját felmérés

A nyilvánosan és ingyenesen elérhető vezeték nélküli internet kapcsolatok a nyugateurópai országokhoz viszonyítva Magyarországon nagy forgalmú környezetben, illetve különféle

[19] Bővebben: https://bsr.bm.hu (2018. 01. 08.)
[20] Bővebben: https://pedo.help/statistics/ (2018. 01. 08.)
[21] A Digitális Gyermekvédelmi stratégia mellett ágazati akciótervekre volna szükség. Lásd: http://www.kormany.hu/download/6/0e/c0000/Magyarorsz%C3%A1g%20Digit%C3%A1lis%20Gyermekv%C3%A9delmi%20Strat%C3%A9gi%C3%A1ja.pdf

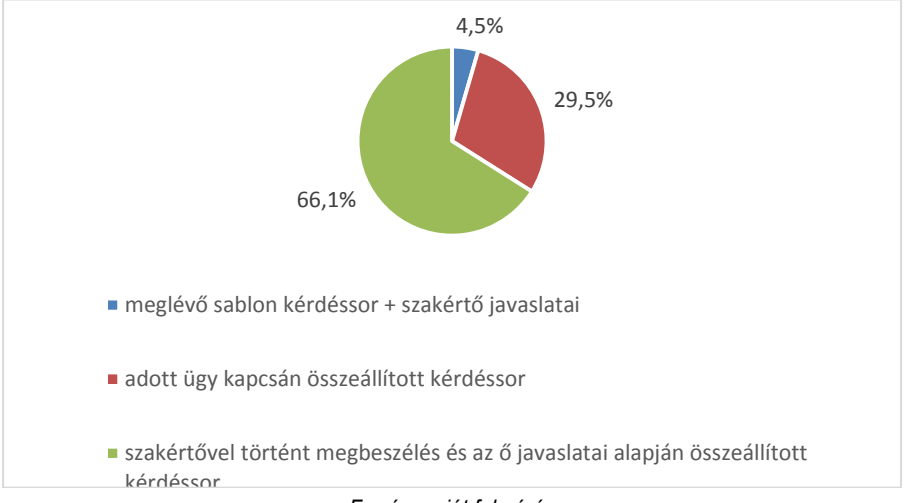
szolgáltatásokat nyújtó üzlethelyiségek (fodrász, étterem, bolt, autószalon, stb) környezetében sokkal nagyobb gyakorisággal fordulnak elő. Ennek egyik fő oka, hogy a mobil internet ára a vásárlóerő paritáshoz viszonyítva magas, így az emberek vagy nem fizetnek elő arra, vagy alacsony adatcsomag mellett lehetőleg WIFI kapcsolatra váltanak.

Azt is fontos azonban megjegyezni, hogy az átlagos felhasználók nem állítják be telefonjukat, úgy, hogy az egy kapcsolt – és nem feltétlen biztonságos – vezeték nélküli internet kapcsolódás esetén ne szinkronizálja le az e-mailjeit, instant üzenetküldő és más futó applikációkat. Úgyszintén nem jellemző, hogy a felhasználók azonnal egy virtuális magánhálózati kapcsolaton keresztül kapcsolódnak egy megbízható internetes szerverhez.

Ezekkel együtt tehát a jelentős különbség a kizárólag böngészőt használó felhasználók és az eszközöket azonnal frissítő felhasználók között vélhetően sokkal kisebb, mivel valószínűleg a böngészés közben futó alkalmazások lefrissülnek a háttérben a felhasználók tudta és szándéka nélkül.

Talán a legnagyobb közvetlen kár bekövetkezése a mobiltelefonokon a banki alkalmazások kompromittálásán keresztül valósulhat meg. Éppen ezért nevezhető minden 10 megkérdezett felhasználó felelőtlennek, amikor nem megbízható helyen mobilbankol. A GSM rendszeren keresztül történő kommunikáció sokkal nehezebben támadható, így az állomány – és egyébként minden felhasználó – figyelmének felhívása indokolt arra, hogy a banki alkalmazásokat lehetőség szerint a mobilszolgáltató adatkapcsolatán keresztül végezze.

A következő kérdések az informatikai szakértéshez kapcsolódó viszonyt voltak hivatottak vizsgálni. A vizsgálat során arra voltunk kíváncsiak, hogy amennyiben szakértő kirendelésére van szükség a kibernyomozás területén, a megkérdezettek tudják-e, hogy a kirendelő határozatban milyen alapvető kérdéseket kell feltenni?

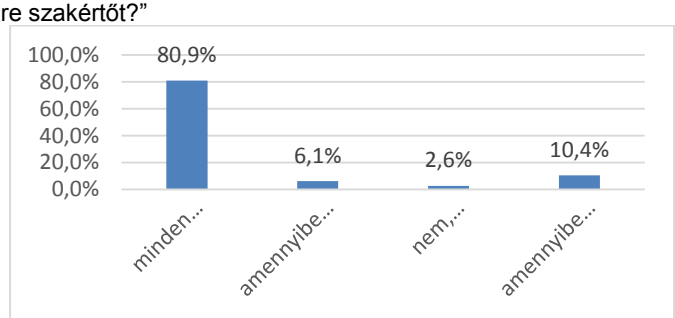


Forrás: saját felmérés

A jogtudomány művelői számára sem egyértelmű a szakértő kirendelésével összefüggésben, hogy a kirendelő hatóság mennyiben kommunikálhat a kirendelt szakértővel. A pártatlan szakértői vizsgálatot mindenképpen az biztosítaná a leginkább, ha a kirendelő hatóság csak a kirendelő határozatban adna felhatalmazást a vizsgálat lefolytatására, a szakértő pedig csak szakvéleményében adna tájékoztatást az elvégzett vizsgálatról. Minden olyan esetben, amikor a szakértő az eljárás és a bizonyítás aktuális helyzetéről a szakvélemény elkészítéséhez szükségeshez képest többlet információkat kap a kirendelő hatóságtól, az alkalmas lehet a szakértő befolyásolására. Mindezek mellett azonban az informatikai szakértők az eredményes együttműködés érdekében kiemelten fontosnak tartják az előzetes egyeztetést a kirendelést megelőzően.[22] E vita eldöntése érdekében indokolt lehet módszertani utasítás kiadása a nyomozóhatóság tagjai irányába, hogy a fegyveregyenlőség elve a vád és védelem közt ne csorbuljon.

Az informatikai szakkérdések sok esetben jóval összetettebbek, mint a többi szakértői terület. Az informatika területén az ügyben eljáró nyomozó gyakran nem is gondol olyan bizonyítékokra, melyek elérhetőek a szakértői vizsgálat tárgyául szolgáló infokommunikációs eszközből[23]. Fontos kérdéseket vet fel a szakértők és szaktanácsadók közti határvonal abban az esetben, amikor az informatikai eszközök vizsgálata már a házkutatás, lefoglalás során indokolt. Úgyszintén a jogi rendelkezéseknek és gyakorlatnak kell kimunkálnia, hogy meddig terjedhet a nyomozóhatóságok digitális nyomrögzítői tevékenysége[24] és mikortól szakkérdés egy vizsgálat lefolytatása.

E probléma megkérdezettek általi értelmezését célozta a következő kérdés: „Amennyiben a nyomozás során bármilyen informatikai eszköz kerül lefoglalásra (okos telefon, táblagép, laptop, PC.) milyen esetben rendelne ki az eszköz által tárolt adatok tartalmának megismerésére szakértőt?”



Forrás: saját felmérés

[22] Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD értekezés, Pécsi Tudományegyetem Állam és Jogtudományi Kar Doktori Iskola, Pécs, 2017. 119. o.
[23] Például egy lefoglalt mobiltelefonról csak a hívások, üzenetek kinyerése és vizsgálata csak apró töredéke annak, amilyen információkat rejt egy készülék és a hozzá kapcsolt felhő alapú tárhely.
[24] Máté I. Zs.: i. m. 67. o.

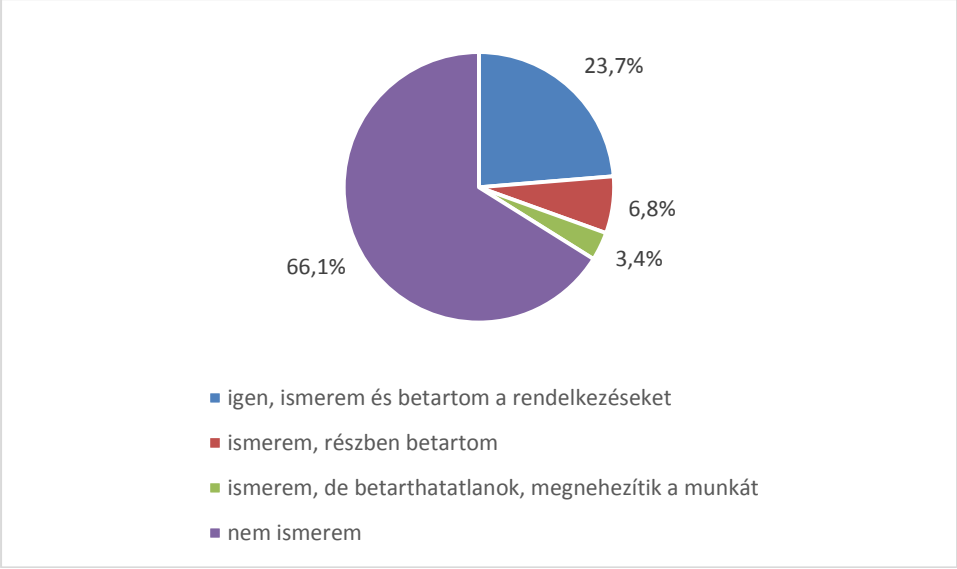
HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám

A kapott eredményből is látható, hogy a megkérdezettek számára sem elérhetőek azok a rendőri szolgálatok, melyeket az angolszász terminológia a digitális bizonyítékok helyszíni vizsgálója (Digital Evidence First Responder, DEFR) [i] elnevezéssel jelöl. Jelenleg a rendőrségen belül a BRFK Számítógépes Bűnözés Elleni Alosztálya, valamint az NNI Kiberbűnözés Elleni Főosztály munkatársai nyújtanak segítséget a digitális bizonyítékok rögzítéséhez és kinyeréséhez. Ez a tevékenység az alanyi körre tekintettel[25] szakértői véleményt nem adhat, de sok esetben szükségtelenné teszi informatikai szakértő kirendelését. Az még a közeljövő fejlesztési feladatai közé tartozik, hogy minden területi és helyi szerv számára ésszerű földrajzi távolságon belül elérhetővé váljanak az e tevékenységet végző, digitális forenzikus eszközökkel felszerelt egységek vagy személyek.

Mint minden jelentős adatvagyont, különleges adatot kezelő szervezetnél, így a rendőrségen belül is kiemelt figyelmet kell fordítani az információbiztonságra, adatbiztonságra. Jellemzően az adatszivárgások elhárításának két fő iránya vetődik fel az egyik a különféle biztonsági, behatolás detektáló, tevékenységfigyelő és egyéb szoftverek iránya, míg a másik a humán tőke tudatossága fejlesztésének iránya. A megoldás természetesen az egyenszilárdságú rendszerek táján található. Annak eldöntése, hogy melyik irány támogatására milyen erőforrásokat delegálnak: rendkívül összetett kérdés. Az azonban mindenképpen költséghatékony megoldás, ha a meglévő biztonsági eszközök megfelelő alkalmazására bírja rá a munkáltató a személyi állományt. Ennek egyik formája egy közérthető, használható, aktualizált informatikai szabályzat, melynek fontosságát a személyi állomány is ismeri és belátja és ennek következtében betartja azt. A megkérdezettek attitűdjét az informatikai szabályzathoz kívánta az alábbi kérdés felmérni: „A 60/2008. (OT 32.) ORFK utasítás a Rendőrség Ideiglenes Informatikai Biztonsági Szabályzatáról és a 45/2013. (XI. 15.) ORFK utasítás az intranethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer rendőrségi igénybevételének szabályairól szóló jogszabályokat ismeri és betartja?”

[25] Nyilvántartásba vett igazságügyi szakértők száma elenyésző e szerveken belül.



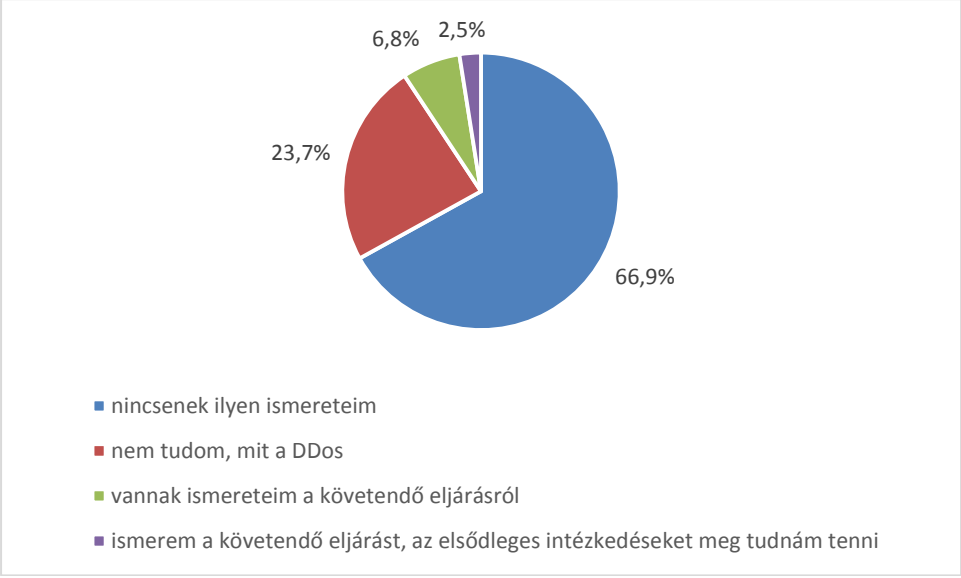
Forrás: saját felmérés

Kijelenthető, hogy a megkérdezett állomány kevesebb mint negyede tartozik a megfelelő tudással rendelkezők közé. Egy ilyen összetett szabályozóról (mely terjedelmében messze meghaladja e tanulmány karakterszámát) felelősen kijelenteni, hogy azt ismeri valaki: nehéz és talán merész kijelentés. A pontos eredmények ismerete információ biztonsági tesztek, sérülékenységvizsgálatok útján tárható fel alaposan.

A kibertérben elkövetett vagyoni jogokat sértő bűncselekmények után az egyik leginkább elszaporodott jogsértő cselekmény csoport az informatikai rendszerek elleni támadások. Ehhez kapcsolódó ismeretszintet volt hívatni feltárni az alábbi kérdés: „Ha egy állampolgári bejelentés érkezik Önhöz, hogy egy vállalkozás internetes oldala elérhetetlen DDoS támadás miatt, akkor vannak ismeretei a lehetséges teendőkről?”

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám



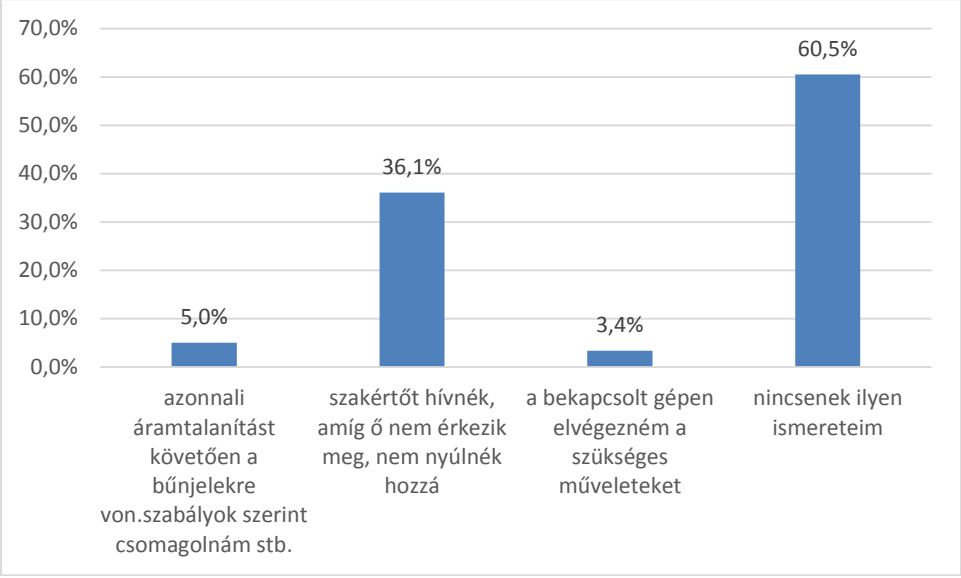
Forrás: saját felmérés

Amint látható a válaszadó 118 főből mindösszesen 3 fő jelezte, hogy egy összetett rendszer elleni támadás esetén ismeri a követendő eljárást és képes az elsődleges intézkedések megtételére. Az arány emelése oktatásokkal, továbbképzésekkel, módszertani utasításokkal, illetve vonalvezetői rendszer[26] kiépítésével orvosolható volna.

A tényleges rendőri munka során számos bűncselekmény típusnál válik szükségessé működésben lévő PC, laptop lefoglalása. Kb. 5 évvel ezelőttig az európai nyomozóhatóságok általánosan bevett gyakorlata az un. „freeze" eljárás volt az eszközök azonnali áramtalanításával. Korunkban azonban az eszközök titkosítása és felhő alapú tárhelyek ezt az eljárásrendet felülírták, sokkal összetettebbé tették.

A vizsgálat következő kérdése: „Egy házkutatás során kell intézkednie bekapcsolt személyi számítógép adattartalmának rögzítésére. Ismeri a helyes eljárásrendet? (több válasz is lehetséges)"

[26] Minden szervezeti egységnél van legalább egy olyan személy, akinek a hatáskörbe tartozó esetekre vonatkozóan vannak ismeretei és ezeket az ismereteket továbbképzéseken folyamatosan szinten is tartja.



Forrás: saját felmérés

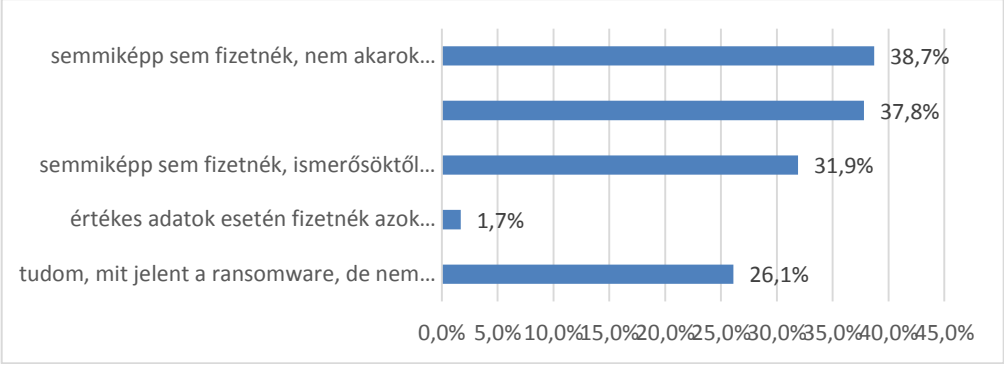
A megkérdezettek mindössze 3,4%- érzi magában a szükséges szakértelmet egy ilyen intézkedés foganatosításához a szükséges eljárási cselekmények lefolytatásához, ami rémisztően alacsony arány, ha figyelembe vesszük, hogy milyen gyakorisággal kerül/kerülhet rá sor.

Bár egy IT eszközön mindig lesznek olyan eljárások, (titkosítás, speciális rendszerbeéállítások, stb) amelyek következtében a lehetségesen kinyerhető bizonyítékoknak csak egy része válik megismerhetővé, de szükséges kidolgozni olyan módszertani utasítást, amelynek követése minimalizálja az adat- és információvesztés veszélyét. Természetesen ehhez a célhardverek biztosítása is szükséges.

A legutolsó kérdés az utóbbi évek egyik legnagyobb információbiztonsági kihívásának a zsarolóvirusokak megítélését kívánta felmérni: „Ha a tulajdonában álló informatikai eszközöket (személyi számítógép/laptop/okostelefon) ransomware (zsarolóvírus) támadás éri, akkor mit tesz? (több válasz is lehet)”

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám



Forrás: saját felmérés

Bár az átfogó megoldást e probléma orvoslására az ellene küzdő nagy nemzetközi szervezetek sem találják, így jelen kérdésre sem adható tökéletes válasz. Az mindenképp hasznos, hogy a megkérdezettek 38,7%-a felkészült egy esetleges ransomware támadásra, de ennek a számnak további emelése szükséges, hiszen egyre nagyobb azon értékeink aránya, melyeket digitálisan tárolunk.

Összességében tehát szükséges átvilágítani, hogy a rendőri alapképzésben milyen módon lehet fejleszteni a kiberbűnözéssel szembeni fellépést hatékonnyá tevő alapismereteket, hiszen a közterületi rendőri tevékenység ellátása során is ezek az ismeretek az állampolgárok tájékoztatása, helyszínbiztosítás, bizonyítékok megőrzése, elsődleges intézkedések megtétele során jelentőséghez jutnak.

Amint azt a tanulmány első soraiban is érintettük: a bűnüldözői, kriminalisztikai tevékenység napról napra nagyobb arányban veszi igénybe a különféle digitális forrásból, adatbázisból, stb származó bizonyítékokat. Korunk technikai fejlettsége (mindenhol jelen lévő szenzorok, mesterséges intelligencia, big data, stb) sokszor lehetővé teszi, hogy számítógép mögül oldjon meg a nyomozóhatóság reménytelennek tűnő bűneseteket. Természetesen az analóg és a digitális forrásból származó információkat nem kizárólagosan, hanem egymást segítve kell felhasználni a bűncselekmények nyomozásában. Azt is látnunk kell, hogy az Orwell-i „Nagy Testvér” technológiai oldalról már megvalósult, csupán az a kérdés, hogy ki működteti és ki hasznosítja az összegyűjtött információkat. Ennek meghatározása jogalkotói kérdés, de a nyomozóhatóságok tagjainak mindenképp készen kell állni, hogy törvényes keretek között minden olyan információt összegyűjtsenek a digitális forrásokból is, melyek a rendészeti szervek alkotmányos céljainak elérést segítik.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 1. szám

FELHASZNÁLT IRODALOM

1. Bányász Péter: Kiberbűnözés és közösségi media. Nemzetbiztonsági Szemle, 2017/4. 55–74. o.
2. GENVAL ország értékelő jelentés http://data.consilium.europa.eu/doc/document/ST-14583-2016-REV-1-DCL-1/en/pdf (2018. 01. 05.)
3. Gyaraki Réka: Számítógépes bűncselekmények és az ellenük való védekezés. In: Christián László (szerk.): Információvédelem. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, Budapest, 2015. 175–189. o.
4. Kiss Tibor – Parti Katalin: A mém vajon mi? Mémekért való felelősség megállapíthatóságának kérdései és lehetőségei. Infokommunikáció és Jog, 2016/2:(66–67) (2017) 3–-47. o.
5. Kiss Tibor – Parti Katalin: Informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer, Budapest, 2016. 491–517. o.
6. Kiss Tibor: Az internet és a társadalmi egyenlőtlenségek Információs Társadalom: Társadalomtudományi folyóirat, 13. (2013/3-4). 97–99. o.
7. Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD értekezés, Pécsi Tudományegyetem Állam és Jogtudományi Kar Doktori Iskola, Pécs, 2017.
8. Nyeste Péter: A bűnügyi hírszerzés. Magyar Rendészet, 2012/4.
9. Simon Béla: Az igazságügyi szakértés egyes kérdései a büntetőeljárásban, különös tekintettel az informatikai szakterületre. Belügyi Szemle, 2017/7–8. 87–105. o.
10. Simon Béla: Rendészeti szervek együttműködése a kiberbűnözés ellen. Megjelenés alatt a Nemzetbiztonsági Szemlében
11. Simon Béla: Rendészettudományi Kar – Kiberbűnözés elleni kapacitásfejlesztési koncepciója. Munkaanyag, 2016.