

Számítástechnikai bűnözés és elkövetők – A bűnelkövetővé válás okainak és jellemzőinek vizsgálata

Készítette: cyber01

Tartalom

1. Problémafelvetés	3
2. A számítástechnikai bűnözés megjelenésének körülményei, fő állomásai	7
2.1. A számítógép megjelenése a bűnözésben.....	7
2.2. A technika és az ember találkozása	8
2.3. Innovatív elkövetési módok a virtuális térben	9
3. A számítástechnikai bűnözés fogalmai, dokumentumai és kriminológiai aspektusai	10
3.1. A számítástechnikai bűnözés nemzetközi dokumentumokban	12
3.2. A „hacker” mint társadalmilag alakított fogalom.....	12
3.3. A számítástechnikai bűnelkövetők jellemzőinek értelmezése	15
<i>Kik a hackerek? – a hackerek demográfiai jellemzőire vonatkozó kutatási előzmények.....</i>	<i>16</i>
<i>A számítástechnikai bűnözés oksági elméletei</i>	<i>18</i>
<i>Létezik-e hacker-társadalom?.....</i>	<i>22</i>
4. Hackerek Magyarországon. Saját empirikus kutatás bemutatása	26
4.1. Demográfia	28
4.2. A kutatás eredményei.....	28
<i>Hogyan válik valaki hackerré? Hogyan lesz valakiből bűnelkövető hacker?</i>	<i>28</i>
<i>A láthatatlan bűnelkövetés.....</i>	<i>30</i>
<i>Felelősségvállalás, önmeghatározás</i>	<i>31</i>
<i>Mi jellemző a magyarországi hacker-társadalomra?</i>	<i>33</i>
4.3. Kutatási lehetőségek	35
5. Javaslatok a bűnmegelőzés, bűnfelderítés és büntetéskiszabás területe számára	36
<i>Bűnmegelőzési javaslatok.....</i>	<i>36</i>
<i>Bűnfelderítési javaslatok</i>	<i>37</i>
<i>Büntetéskiszabási javaslatok.....</i>	<i>37</i>
6. Konklúzió.....	39
Irodalomjegyzék	42

1. Problémafelvetés

A számítástechnika, számítástechnikai bűnözés, hacker, programozás, a vírusírás mind olyan kifejezések, melyek a társadalom számára misztikusak, idegenek és nehezen értelmezhetők, ezért az „egyszerű” felhasználók kevésbé érdekeltek a számítástechnikai ismeretek szélesebb körű megszerzésében.

A számítógépet és internetet használók körében általános jelenség az áldozattá válás lehetőségének figyelmen kívül hagyása. Kevesen nyitják meg úgy elektronikus üzeneteiket, hogy közben a csatolmányban lévő trójai vírus kártékony hatásai miatt aggódnának, vagy megfontolnák, hogy megnyissanak videónak álcázott vírusokat, melyekkel önkéntesen adathalászat áldozataivá válnak, esetleg figyelembe vennék, hogy a közösségi oldalon közzétett írásaik, aktivitásuk egy olyan profil létrehozását teszik lehetővé, melyet nem csak kereskedelmi vállalatok, de lényegében bárki felhasználhat. Kevesen gondolnak arra, hogy bárki ülhet számítógépük „másik” oldalán és figyelheti tevékenységüket.

A számítástechnikai ipar globálissá válása, elpiacosodása és az internet világméretű kiterjedése növelte ugyan az elsajátítható informatikai tudást, ennek megoszlása azonban nagy aránytalanságokat mutat. Az elmúlt 20 év technikai fejlődése során a számítógépek és a hálózatok életünk részévé váltak, de a felhasználók többségében mára sem alakult ki a technika öntudatos használatának gyakorlata.

Az információs hálózatok infrastrukturális szerepükből adódóan a mindennapi élet szervezésének is elengedhetetlen kellékévé váltak. Egy olyan típusú függőség jött létre, mely gyakran önkéntes választásunktól függetlenül befolyásolja társadalmi létünk és ezzel arányosan csökkenti alapjogaink és magánszféránk védelme iránt támasztott igényünket is.

Ugyanakkor ez a nagymértékű dependencia egy másodlagos, látens társadalom kialakulását is magával hozta. A virtuális tér, melyet a számítógépek által összekapcsolt hálózatok rendszere alkot, a felhasználók egy része számára szocializációs közegként kezdett el funkcionálni. Ez a közeg természetéből adódóan a jogalkotó számára kevésbé értelmezhető és szabályozható, többnyire szigorú jogállami keretek nélkül működik. A szabályozatlanság, mely a virtuális térben a jogszabályok alkalmazásának nehézségeit is jelenti, olyan potenciális veszélyforrás, mely folyamatos értelmezésre, kezelésre és figyelemre szorul.

Az információs technológia (IT) mindennapossá, sőt nélkülözhetetlenné válása a bűnözés egy új formájának megjelenését is eredményezte. A számítógépes bűnözés a kriminológia számára sem ismeretlen terület, jelenleg azonban még kevesebb figyelem irányul a hackerek által elkövetett bűncselekményekre, holott a tavalyi évben egyetlen, 50 globális kiterjedésű

szervezet részvételével készült amerikai kutatás 63 437 információs rendszer elleni támadást észlelt.¹ Ha ehhez hozzá tesszük a vállalatok, illetve az információs rendszerek valós számát a számítógépes bűnözés és az azzal okozott kár mértéke megbecsülhetetlen.

E globális szinten is több milliárd dolláros károkat okozó bűnözési forma elkövetőit a közvélemény hackereknek hívja, mely egy olyan gyűjtőfogalom, ami köznyelvi értelemben magában foglal minden egyént, aki számottevő tudással rendelkezik az információs rendszerek és a programozás területén. A hackerek, illetve, közösségeik nem azonosíthatók azonban a kibertér elkövetőivel. A bűncselekményt elkövetők – mint ahogyan az a hagyományos közösségeknél is megfigyelhető – egy szűkebb egységét képezik a vizsgált szférának.

Kutatásom abból a feltevésből indul ki, hogy a hagyományos és a virtuális tér deviáns közösségei jelentős eltéréseket mutatnak. A deviancia kifejezés ebben az esetben a virtuális tér bűnelkövetővé váló közösségeit jelenti, annak ellenére, hogy a társadalmilag megkonstruált fogalom a bűnözéssel össze nem kapcsolható csoportokat is ide tartozónak tekinti. Ez alapján a virtuális teret másodlagos létezőként értelmezőket általánosan nem sorolom a deviánsok körébe.

Különösen foglalkoztat tehát azoknak a csoportoknak a fogalmi elhatárolása a hagyományos bűnelkövetőktől, melyek a kriminológia és a jogtudomány számára jelenleg láthatatlanok. A számítástechnikai bűncselekmények vonatkozásában hagyományosnak tekintem azokat, akik cselekménye valamilyen fizikailag értelmezhető lenyomatot hagy maga után, így ide tartoznak például az erőszakos, a vagyon elleni, a gazdasági bűncselekményt elkövetők, de a számítógépet kizárólag eszközként felhasználók is, akik többek között a gyermekpornográfiával kapcsolatos bűncselekményeket, illetve számítógéppel kapcsolatos csalást elkövetik. A kutatásomban vizsgált bűnözési forma különbözik a hazai szakirodalomban többek között Virág György, Parti Katalin és Szabó Imre által kutatott területektől, mert ezek mind a hagyományos bűnözés új - számítógépes - környezetbe kerülésével, illetve ennek büntetőjogi és kriminológiai aspektusaival foglalkoztak.

A bűnelkövetésre vállalkozó hackerek tevékenységét pont az teszi egyedeivé, hogy ugyan lehet fizikai eredménye cselekményüknek, tehát okozhat vagyoni kárt, fizikai sérülést, sőt közvetetten még halált is, de nem ez magatartásuk legfontosabb eleme. Jellemző, hogy előbb alakul ki az elkövetésre való képesség, melyhez később társul a motiváció. Ez azt jelenti,

¹ Verzion: 2014 Data Breach Investigations Report (Letöltés ideje: 2014.08.15.)
<http://www.verizonenterprise.com/DBIR/2014/>

hogy a bűncselekmény elkövetéséhez szükséges tudás megszerzése nem a bűncselekmény elkövetésének céljával történik, az csak később jelenik meg, vagy egyáltalán nem is alakul ki.

Hipotézisem szerint a számítástechnika globális felhasználása és rohamos terjedése eredményeként létrejövő látens társadalmon belül létezik egy olyan kriminogén csoport, mely számára a virtuális tér másodlagos szocializációs közegként működve befolyásolja a külvilágról, jogszabályokról és bűnelkövetésről alkotott képét. E csoport jellemzője a bűnelkövetés felelősségének teljes tagadása, önálló szabályok alkotása és egy bizonyos szintű felsőbbrendűség érzés a megszerzett tudás egyediségének következtében.

Álláspontom szerint, hasonlóan a fehérgalléros bűnözéshez, létezik a számítástechnikai bűnöző fogalma is, mely önálló kriminológiai kategória, így egyedi bűnmegelőzési és büntetéskiszabási szemléletet tesz szükségessé.

A dolgozat megírását a területtel kapcsolatos szélesebb körű ismeretek hiánya, a társadalom veszélyeztetettségének fokozott mértéke, a bűnözés e formájának magas látenciája és a kriminológia számítógépes bűnözésről alkotott képének szélesítése inspirálta. Feladatommak tartottam a számítástechnikai bűnözés e területén a fogalmi alapok meghatározását, az elméleti keretek feltárását és a későbbi empirikus kutatások megalapozása céljából összefoglalni a kriminológia számára előrelépést jelentő kutatási eredményeket.

Ebben szerepet játszott, hogy Flammich Mariann szociológiai kutatása kivételével a hazai szakirodalomban még nem szolgáltatott adatokat a magyarországi hackerek közösségéről.² Ennek eredményeként valójában több mint egy évtizede semmilyen tényanyag nem áll rendelkezésre a bűnözés e szűk, de annál nagyobb figyelmet érdemlő területének vizsgálatára.

E tudományos igény egy kvalitatív kutatás elkészítését tette szükségessé. Ennek részeként interjúk megkérdezés módszerével tettem kísérletet a magyarországi számítástechnikai bűnelkövetők megismerésére. A megkérdezések alanyait minél szélesebb skáláról kívántam összegyűjteni, így informatikai biztonsági szakértővel, bűncselekményt elkövető hackerrel, etikus hackerrel, illetve a hatóságokkal és áldozatokkal is felvettem a kapcsolatot.

Céлом ezzel összhangban annak feltárása volt, hogy, kik követhetik el ezeket a cselekményeket, kik használják ki a felhasználók tájékoztatatlanságát, vagy találják meg az információs rendszereken lévő biztonsági hibákat és készítenek adatbázisokat az internetet használókról. A megszerzett tudás alkalmazhatósága érdekében pedig szükségesnek láttam a hagyományos bűnelkövetőktől való különbségek ismeretében megfelelő javaslatokat

² Flammich M.: Hackerek: Vázlat a magyar szubkultúráról. 2002.

megfogalmazni a – növekvő problémákat okozó – számítástechnikai bűnözés terjedésének megakadályozásához.

2. A számítástechnikai bűnözés megjelenésének körülményei, fő állomásai

„Nem félek a számítógépektől, a hiányuktól félek.”

Isaac Asimov

Az információs technológia egyike ma a világ legdinamikusabban fejlődő területeinek. A számítástechnika térhódítása együtt jár azonban a számítógépes környezetben elkövetett bűncselekmények növekedésével és az új típusú bűnelkövetési módok megjelenésével is. Ahogyan fejlődik az információs ipar, úgy nő a számítógéppel kapcsolatos bűnözés is.

Ennek története a '60-as évek Amerikájában kezdődik, nem sokkal később terjedésnek indul a világ fejlettebb országaiban, mígnem a '80-as években a magyarországi bűnözéskutatás is felfigyel a problémára.³

2.1. A számítógép megjelenése a bűnözésben

Az információs technológia fejlődésének kezdeti szakaszában a visszaélések két fő jellemzővel bírtak:

- hálózatok hiányában a számítógépek, mint fizikai egységek jelentették a bűnözés tárgyát,
- az elkövetők az esetek többségében megbízhatatlan vagy csalódott alkalmazottak voltak.⁴

A hatvanas évektől a számítástechnikai eszközök szerepe számos szervezet életében jelentősen megnövekedett. A hálózatok és a biztonsági intézkedések hiánya azonban sérülékennyé tette a tárolt információt. A számítógépek védelme ekkor elsősorban fizikai védelmet jelentett. Egy olyan információs rendszer elleni támadás esetén, melynél az informatikai biztonsági intézkedések eredményeként az adott vírus, vagy kémprogram kizárólag fizikai módon juttatható be a kiszemelt hálózatba, az épületbe való bejutás különösen fontos mozzanatát képezi ma is a cselekményeknek.⁵

Az 1970-es évektől a gépek megrongálását célzó bűncselekmények kezdtek egyre elterjedtebbé válni, majd átvette szerepüket az információs rendszereket érintő bűnözés.

³ Az első ezzel foglalkozó írás Dr. Polt Péter „Számítógépes bűnözés” című tanulmánya volt 1983-ban. Ebben fejti ki többek között, hogy a számítógép lehet egyszerre a bűncselekmény tárgya és eszköze.

⁴ Kabay, M.E.: A Brief History of Computer Crime: An Introduction for Students. Norwich, 2008, Norwich University. 4. p.

⁵ 3. sz. interjúalany – etikus hacker

2.2. A technika és az ember találkozása

A számítógépek ellen irányuló szabotázs terjedésével egy időben elkezdődött a legalitás és illegálitás határainak elmosódása. Ekkor a technika iránt érdeklődő, kriminogén jellemzőkkel alig körülírható fiatalok jelentették a modern technológia „deviánsait”. Az 1980-as években - különböző forrásokból megszerzett technikai tudás és a kommunikációs készségek kombinációja révén - elkezdtek feltörni a telefonhálózatokat.⁶

A magyarul pszichológiai manipuláció néven ismert, és minőségileg más magatartást lefedő *social engineering* kifejezés elterjedése és mindennapivá válása az informatika világában a ma is nagy ismeretségnek örvendő Kevin Mitnick nevéhez fűződik.

Mitnick esete azért fontos, mert egy hacker tevékenysége nem ragadható meg egyedül a technikai tudásban és annak magas szintű alkalmazásában. A környezet ismerete és manipulálása az elkészíteni kívánt „hack” hatékonyságát nagymértékben befolyásolja. Az általam elkészített interjúk alapján is az derült ki, hogy az informatikai biztonságtechnika ma is kiemelt figyelmet szentel a fizikai megközelíthetőségnek és az alkalmazottak manipulálhatóságának.

„Lehet milliókat költeni egy rendszerre, de ha az emberi tényező ott van, akkor ez kidobott pénz. Én például megtiltanám azt, hogy munkahelyről facebookozzanak, linkeket nyissanak meg, alkalmazásokat telepítsenek a munkahelyi gépekre.”⁷

A Los Angeles-i Kevin Mitnick az 1980-as években kezdett el az emberek segítőkészségét kihasználva telefonhálózatokat (*phone phreaking*), majd informatikai rendszereket (*cracking*) feltörni.⁸ Legelső – hatóság által megismert – cselekménye miatt a bíróság elrendelte pszichológiai profiljának elkészítését.⁹ Ez azért érdekes különösen, mert bár nem Mitnick volt az első mai értelemben vett hacker, mégis ő tekinthető az első olyan személyiségnek, aki az elkészített kutatás – később olvasható – eredményei szerint elsősorban hacker személyiség és csak másodsorban visszaeső bűnelkövető.

Mitnick példája úgy értelmezhető, mint a technikai forradalom egyik kísérőjelensége. Ahogyan a társadalom fejlődik és új eszközök, ill. gyakorlatok válnak használatossá, úgy jelennek meg azok is, akik képesek kihasználni e technológiák sérülékenységet és jelen esetben kombinálni a szociális készségeket a fejlődés új elemével. Durkheim szerint *„egyetlen jelenség sincs tehát, mely elvitathatatlanabb módon rendelkezne a normalitás összes*

⁶ Kabay: i. m. 7. p.

⁷ 1. sz. interjúalany – büntetett hacker

⁸ Kabay: i. m. 10. p.

⁹ Littman, J.: The Fugitive Game. Online with Kevin Mitnick-The inside story of the great cyberchase. Boston, 1996, Little Brown and Company, 30. p.

*tüneteivel, mint a bűnözés, amely úgy látszik, közvetlen kapcsolatban van mindenféle társadalmi lét feltételeivel.(...) Normális jelenség a bűnözés,(...) mert teljességgel lehetetlen, hogy tőle egyetlen társadalom is mentes legyen.*¹⁰A számítástechnikai bűnözés és bűnelkövető is tehát a társadalmi fejlődés természetes velejárója, mely leképezi az adott közösség viszonyait és fejlettségi szintjét.

2.3. Innovatív elkövetési módok a virtuális térben

Az egyének segítőkészségének kihasználásával párhuzamosan hasonló intenzitással vette kezdetét az új, mára mindennapos elkövetési módszerek terjedése. A számítástechnikai bűnözés megértéséhez kiemelten fontos e nehezen körülhatárolható és a bűnözés kereteit kitágító módok feltárása a teljesség igénye nélkül.

Adathalászat: Ennek lényege a felhasználók személyes adatainak számítógépből „kihalászása”, majd egyéb bűncselekmények elkövetésére való felhasználása. Ez tekinthető napjaink egyik legelterjedtebb „betörési” módszerének.

Vírusterjesztés: A számítógépek számára kártékony vírusok, férgek, kémprogramok már az 1980-as években megjelentek és a mai napig növekvő számot mutatnak. Csak a Kaspersky Lab, mely egyike a vezető IT biztonsági vállalatoknak 28,4 millió finanszírozott malware támadást észlelt 2013-ban.¹¹ Ezek közül a legveszélyesebbek a trójai vírusok, melyek teljes hozzáférést biztosítanak a felhasználók számítógépeire.

„Az az egyik legnagyobb probléma, hogy az emberek mindent letöltenek. Szerintem a torrentezés az egyik legveszélyesebb. Volt már olyan, hogy a srác írta valakinek chat-en, hogy a legújabb vírusirtót telepítette fel és közben én a programmal bejuto trójai segítségével néztem az ő gépét.”¹²

E módszerek közös jellemzője, hogy a programok megtervezése, elkészítése és a részfolyamatok alapjainak megalkotásához egy magas számítástechnikai tudással rendelkező hacker szükségeltetett, a technikai létrehozásának motivációjától függetlenül. Ez alapján az alapvetően innovatív technológiák, nem feltétlenül bűnelkövetési céllal jöttek létre, annak felhasználása és felhasználói köre később változott, megalkotva a hackerekben belüli egyedi bűnözői csoportot.

¹⁰ Durkheim, É.: A bűnözés normális jelenség. In: Gönczöl K., Kerecsi K. (szerk.): A deviancia szociológiája. Szöveggyűjtemény. (Bp., 1996, Hilscher Rezső Szocpol. Egyesület)

¹¹ Kaspersky Lab Report. Financial cyber threats in 2013. 16. p.
<http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-2013-eng-final.pdf>
(Letöltés ideje: 2014.10.15.)

¹² 1.sz. interjúalany – büntetett hacker

3. A számítástechnikai bűnözés fogalmai, dokumentumai és kriminológiai aspektusai

A bűnözés e formájának megjelenésekor a számítógépes bűnözés (computer crime, Computerkriminalitát) fogalmát kezdték el használni. A '90-es években azonban a technika fejlődésének hatására a bűnözés elkezdett differenciálódni és megjelentek egyéb elnevezések is. Ilyen volt többek között a számítógépes környezetben elkövetett bűnözés (computer related crime), mely a dolgozat értelmezésében nem tekinthető a virtuális térhez kötött elkövetésnek, hiszen utóbbiaknál szerzői jogot sértő cselekményekről, vagy az elektronikus félvezetők jogosulatlan kereskedelméről beszélünk.¹³

Jelenleg nem létezik egységes fogalom a bűnözési forma körülhatárolására, ill. annak kriminológiai tipizálása is vitatott. Dolgozatomban így az általam vizsgált területre, - vagyis a hackerekhez köthető bűnözésre - a számítástechnikai bűnözés terminológiát tartom megfelelőnek. A fogalom elfogadása abból a meggyőződésből indul ki, hogy a hackerek által elkövetett cselekmények nem kizárólag a számítógéphez¹⁴ kapcsolódnak, de mindenképp valamilyen technológiai, technikai konnotációval bírnak és ilyen módon a technikai tudás az, ami megragadható a „számítástechnikai” kifejezésben.

Kriminológiai szempontból a számítógépes bűnözésnek mint gyűjtőfogalomnak az elhelyezése is számos problémát vet fel. A Nagy Zoltán András által számítógépes környezetben elkövetett deliktumoknak nevezett cselekményeket¹⁵ a szakirodalom jelentős része a fehér galléros bűnözés fogalmába sorolja. Ennek oka a kriminológus szerint, hogy ezekben az esetekben szintén intellektuális bűnözésről van szó. Meglátása szerint két aspektusból képezhetik az Edwin H. Sutherland¹⁶ által létrehozott fogalom részét a tárgyalt cselekmények. Egyik esetben a foglalkozási, másik esetben a szervezeti bűnözés keretei között.¹⁷

A vizsgált számítástechnikai bűncselekmények tekintetében is beszélhetünk e két elkövetési formáról, azonban a hackerek által elkövetett kriminogén cselekmények mégsem vonhatók a „white collar crime” ernyője alá, hiszen kutatásom szerint az elkövetők olyan demográfiai sokszínű csoportjáról beszélhetünk, ami alapján nem köthető e bűnözés közvetlenül foglalkozáshoz, iskolai végzettséghez, de még társadalmi helyzetéhez sem.

¹³ Nagy Z. A.: Bűncselekmények számítógépes környezetben. Bp., 2009, Ad Librum Kft., 35. p.

¹⁴ Azok kapcsolódhatnak olyan egyéb eszközökhöz is, melyek programozása komoly technikai tudást igényel.

¹⁵ Nagy: i. m.

¹⁶ Sutherland, E. H.: White-Collar Criminality. In: American Sociological Review. 1940. 5. évf. 1. sz. 1-12. p.

¹⁷ Nagy: i. m. 20. p.

Ezek alapján egyetérték Nagy Zoltán András és Balogh Zsolt György következtetésével, mely szerint *„mind a számítógépes, mind a fehérgalléros bűnözés olyan önálló kriminológiai kategória, melyek között van ugyan némi átfedés, de arról még sincs szó, hogy bármelyik kategória egészében tartalmazná a másikat”*.¹⁸

A fehérgalléros bűnözés szempontjainak parttalanná válása eredményezi azt a Korinek László által használt definíciót, mely szerint a számítógépes bűnözés a társadalmi elit és a tömegek bűnözésének összemosódását, relatívvá válását hozhatja magával.¹⁹

Léteznek a kriminológiai meghatározástól különböző büntetőjogi definíciók is. Kunos Imre szerint a *„számítógépes bűnözés azon bűncselekmények összessége, amelyek információ-technológiai eszközök, illetve rendszerelemek ellen irányulnak, vagy információ-technológiai eszközöket, rendszereket használnak bűncselekmény elkövetésének eszközeként”*.²⁰

A külföldi, elsősorban holland és angol - cybercrime területével foglalkozó – kriminológusok kisebb jelentőséget tulajdonítanak a fehérgalléros bűnözéshez való viszony felvázolásának, a fogalmak azonban itt is jelentős eltéréseket mutatnak. Wouter Stol kriminológus szintézise szerint a terminológiák egész arzenálja használatos a folyamatok meghatározására, de vannak olyan sarkalatos pontok, melyek mindegyikben azonosak: vannak bűncselekmények ahol az információs és kommunikációs technológia (IKT) egyszerre célja és eszköze is az elkövetésnek (pl.: hackelés, vírusterjesztés); és vannak bűncselekmények ahol az IKT nélkülözhetetlen a támadás végrehajtásához, de ahol nem az IKT a célpont (pl.: számítógépes csalás, gyermekpornográfia terjesztése).²¹ Ez alapján a „cybercrime” szűk értelemben az első kategóriát foglalja magában, míg tágan értelmezve a másodikat. Ez utóbbi, több kutató számára *„old wine in a new bottle”*, tehát régi bűnözés új keretek között.

A „computer crime” értelmezésének első formájával egyetértve a számítástechnikai bűnözés kriminológiailag egy olyan szűk kategória, melyben a számítógép pusztán használata nem eredményez újabb elkövetési formákat. A számítógép ez alapján leszűkítheti az elkövető és áldozat közötti teret, egyszerűbbé teheti a – hagyományos eszközökkel is lebonyolítható - bűncselekmény végrehajtását, neutralizálhatja az elkövetőt, de mégis csak, mint elkövetési eszközről beszélhetünk.

¹⁸ Balogh Zs. Gy.: Jogi informatika. Bp.-Pécs, 1998, Dialóg Campus, 266. p.

¹⁹ Korinek L.: Bűnözési elméletek. Bp., 2006, Duna Palota és Kiadó, 297. p.

²⁰ Kunos I.: A számítógépes bűnözés a modern információtechnológia felhasználása a bűnözésben. In. Belügyi Szemle, 1999, 11. sz., 28-42. p.

²¹ Leukfeldt, R.; Stol, W.: Cyber Safety: An Introduction. 2012, Eleven International Publishing. 23. p.

Az olyan bűncselekmények esetében, ahol a számítástechnikai program elkészítése, a rendszer feltörése, vagy a programok felhasználói szintet meghaladó kezelése egy másik rendszerben eredményez károkat, már nincs szó pusztán eszközhasználatról. Az intelligencia és a technikai eszközöknek egy olyan kombinációja jön létre, mely kiemeli az elkövetőt a homogén csoportokból.

3.1. A számítástechnikai bűnözés nemzetközi dokumentumokban

A „*Számítástechnikai bűnözésről szóló egyezmény*”,²² a visszaéléseket négy gyűjtőfogalomba sorolja. Ezek közül a *számítástechnikai rendszer és számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények* köre releváns kutatásom szempontjából. Ez a - magyar büntetőjogba már részben átültetett - fogalom sem alkalmazható fenntartások nélkül a kriminológiai vizsgálódáshoz, hiszen ezek nem kizárólag a virtuális tér elkövetőinek cselekményei lehetnek, hanem elkövetők lehetnek azok is, akik a bűnelkövetői csoport által létrehozott infrastruktúrában hozzájutottak a szükséges eszközökhöz, vagy tudáshoz, de nem képezik a közösség részét, nincs erős kapcsolatuk a virtuális térrel, tehát a számítógép jelen esetben is csak instrumentum céljuk eléréséhez.

Hazánkban korábban az 1978. évi IV. tv. „A gazdasági bűncselekmények”, jelenleg pedig a 2012. évi C. tv. „Tiltott adatszerzés és az információs rendszer elleni bűncselekmények” fejezetében foglalt tényállások tartalmazzák a büntetendő cselekményeket, de kriminológiailag ezek sem feleltethetők meg teljesen a hackerek által elkövetett cselekményeknek.²³ E tényállásokat bárki megvalósíthatja, nem szükséges, hogy az elkövető hacker legyen vagy a cselekmény a hackertámadások jellemzőivel bírjon.

3.2. A „hacker” mint társadalmilag alakított fogalom

„A hackerek olyanok, mint a gyerekek, akik egy 10 centest tesznek a vasúti sínre, hogy lássák a vonat képes-e meghajlítani azt, nem realizálva, hogy az egész vonat kisiklását veszélyeztetik.”

Mike Jones, Department of Trade and Industry²⁴

²² Az Európa Tanács Budapesten, 2001. november 23-án kelt, számítástechnikai bűnözésről szóló egyezménye. Convention on Cybercrime, CETS. No. 185 - 23. XI. 2001.

<http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Hungarian.pdf> (Letöltés ideje: 2014.10.02.)

²³ Ezen belül elsősorban a 423.§ és 424§ alkalmazható, de a 421.§ (1) bekezdés d) pont esetében is lehet szó hacker által elkövetett bűncselekményről.

²⁴ Jordan, T.; Taylor, P. (1998). A sociology of hackers. In.: The Editorial Board of The Sociological Review. Oxford, 1998, Blackwell Publishers, 770. p.

A kutatásomban központi szerepet játszó hacker kifejezés értelmezése számos eltérést mutat. A fogalom kezdetekben egy olyan személyt jelentett, „*aki megszállottja a számítógépes rendszerek megismerésének és megértésének*”.²⁵ Erre az időszakra visszatekintve mégis a legmegfelelőbb azt mondani, hogy „*egy pozitív leírása volt valakinek, aki képes elegáns, kreatív és hatékony megoldásokat találni technikai problémákra*”.²⁶

Bruce Schneider neves számítógépes biztonsági szakértő 2000-ben már az írja, hogy „*a hacker olyan személy, aki – intellektuális kíváncsiságból vagy tiszta élvezetből a rendszerek korlátait próbálja felderíteni*”.²⁷

A hackerek számának növekedésével és pluralizálódásával megítélésük és tevékenységük az elmúlt évtizedekben folyamatos változásokon ment keresztül. A kifejezés elkezdett komoly aggodalmakat kelteni az új számítógépes technológiák hatalmával való visszaélés szempontjából.²⁸

Különvált a hacker és a cracker fogalma. Utóbbit Flammich Mariann a médiának tulajdonítja, hiszen „*a cracker terminust a sajtó a rosszindulatú számítógépes behatolások kapcsán kezdte használni, pedig eredetileg a crackernek semmi köze a hackerhez. A cracker csak programozni tud, tudása lényegesen kisebb, mint a hackeré. A szó eredetileg olyan felhasználót jelöl, aki szoftverfeltöréssel foglalkozik*”.²⁹ Ez az értelmezés manapság már kevésbé állja meg a helyét, egyrészt az alkalmazott technikák változásai miatt, másrészt a merev határok összemosódása okán.

A hacker közösségek kutatásának elterjedtebbé válásával újabb és újabb megkülönböztetések kezdtek el terjedni. Ezek közül – a kutatásokban is felhasznált – tipológiát szükséges felvázolni, mely a legmegfelelőbb a legalitás és illegalitás vékony határának körülírására, jelezve, hogy még számos, szintén releváns megközelítés alkalmazható. Ilyen pl. Rogers hacker taxonómiája, a McAfee biztonsági vállalat tipológiája, vagy Goldschmidt bináris elkülönítése.

Az Europol 2003-as jelentése és Dasselaar 2005-ös írása alapján Leukfeldt és de Jong holland kriminológusok a következő tipológiát készítették:³⁰

²⁵ Levy, S.: Hackers: Heroes of the Computer Revolution. Garden City, 1984, Doubleday.

²⁶ Yar, M.: Cybercrime and Society. London, 2006, SAGE Publications Ltd., 22. p.

²⁷ Schneider, B.: Secrets and Urs, Digital Security in a Net.Jerked World. Wiley, 2000, Computer Publishing, John Wiley and Sons, Inc.

²⁸ Hannemyr, G.: Technology and Pleasure: The Art and Craft of Hacking. 1999.

²⁹ Flammich: i. m. <http://hannemyr.com/en/sj98.html> (Letöltést ideje: 2014.08.22.)

³⁰ Leukfeldt et. al.: i. m. 104. p. http://www.mediakutato.hu/cikk/2002_03_osz/01_hackerek/#03 (Letöltés ideje: 2014.08.15.)

- *White hat vagy fehér kalapos hackerek*: jóhiszemű, gyakran hivatásos, magas technikai tudással rendelkező személyek.
- *Black hat vagy fekete kalapos hackerek*: a szintén magas technikai tudásukat destruktív céllal felhasználó bűnelkövetők
- *Gray hat vagy szürke kalapos hackerek*: az előző két csoport között álló hackerek, akik ugyan bűncselekményeket követnek el, de annak célzata a rendszerek biztonságának tesztelése
- *Hacktivisták*: olyan politikai vagy társadalmi aktivisták, akik az informatikát használják fel céljaik elérése érdekében
- *Script Kiddiek*: csekélyebb technikai tudással rendelkező – gyakran fiatalok – bűnelkövetők
- *Politikai vagy vallási szélsőségesek*: az informatikai rendszereket felhasználó terroristák

E tipológia a kezelési/bűnmegelőzési módok miatt különösen fontos a kriminológia számára. Valójában nem léteznek ennyire merev határok a kategóriák között, ugyanakkor a tudományos vizsgálat érdekében fontos az elkülönítés, mert segít megérteni a motivációban rejlő – bűnmegelőzési szempontból fontos – különbségeket.

Tim Jordan és Paul Taylor angol szociológusok 6 fő motivációs tényezőt különítenek el. Ezek valójában a *hacktivisták* és *politikai vagy vallási szélsőségesek* kivételével minden kategóriánál integráns részét képezik cselekedeteiknek, attól függetlenül, hogy az milyen károkat okoz végül.

Az első, hogy a hackerek gyakran bevallottan addiktak a számítógépek és/vagy számítógépes rendszerek, de még inkább a „hack” véghezvitele iránt. Második a kíváncsiság az iránt, hogy mi található a számítógépes hálózatokon belül. Harmadik, hogy a hackerek gyakran azt állítják, az „offline” élet unalmas az „online” világ izgalmaéhoz és tilosságához hasonlítva. Negyedik a hatalom, mely esetükben a számítógépes rendszerek feletti hatalomszerzést jelenti. Ötödik a pillanatnyi elismerés más hackerektől vagy barátoktól, ami egy olyan jutalom és cél sokuknál, mely a közösség elfogadását vagy a képzetesebb hackerek hierarchiájába betagozódást jelenti. Végül a hatodik, a jövőbeni számítógépes felhasználók és a társadalom figyelmeztetése a számítógépes hálózatokban található hibákról.³¹

A két kutató a különbséget legalitás és illegalitás szempontjából abban látja, hogy az adott hacker tudását a számítógépes alvilágban vagy a számítógépes biztonsági iparban hasznosítja.

³¹ Jordan, Taylor: i. m. 768. p.

Ezzel kapcsolatban a legfontosabb – ma is érvényes - kijelentés szerint a cselekmények etikai és erkölcsi oldalát kell figyelembe venni. Analógiát vonva a való életben történő betöréssel nagy különbségek láthatók az okozott kár, illetve érdeksérelem szempontjából. Egy betörés alkalmával nem hallani olyanról, hogy az elkövető nem vitt el semmit, csak bement a nyitott ajtón, körülnézett, majd kijött és felhívta a tulajdonost, hogy zárja be azt.

A számítástechnikai betörések világában ez azt jelenti, hogy a „jó” és „rossz” hacker között ott található – jogtudattól függetlenül – különbség, hogy a büntetőjogi tényállásszerűség megvalósítása csak a figyelemfelkeltésig terjedt, vagy megjelennek másodlagos motivációk, mint például a számítástechnikai rendszert felhasználók adatainak, levelezésének stb. lementése.

A felvázolt szakirodalom és e példa alapján fehér kalapos hacker az, aki hivatását gyakorolva, engedéllyel tehát biztonságtechnikai szakértőként lép be rendszerekbe. Szürke kalapos hacker az, aki egyébként megvalósítja a bűncselekményt, de céljait a fent említett hat motiváció vezérli, és nem jelenik meg másodlagos bűnelkövetési szándék, míg fekete kalapos az, akinek lehetnek hasonló motivációi, mint az előzőnek, de ezeken túllépve más – általában – büntetőjogilag is értékelhető tényállást is megvalósít.

A script kiddiek esete annyiban más, hogy ők magukon viselhetik a szürke és fekete kalapos hackerek cselekményének jellemzőit, de nem rendelkeznek azzal a tudással, mely valóban hackerré teszi őket, így a bűnelkövetői karrier kisebb súlyú cselekmények elkövetésében nyilvánul csak meg.

A felvázolt általános „hacker motivációkon” kívül meghatározhatók konkrét „offender” motívumok is, melyek az elsődleges motivációkat egészítik ki, de már túlmutatnak a számítástechnikai bűnelkövetésen. Ezek két fő csoportot foglalnak magukban: a bosszút, és a vagyonszerzést. Rogers szerint az első elkövetője az egyénekre, szervezetekre, országokra vagy kontinensekre koncentrálhat, addig a második a kapzsiságra és pénzszerzésre.³²

Kombinálva ezt a hackerek általános tipológiájával egy olyan fekete kalapos elkövetőt kapunk, akinek vannak általános, közösségre jellemző és elkövetői motivációi is, melyek már nem a hacker identitáshoz kötettek, hanem mint az később látszani fog szocializációs és szociális tényezők által befolyásoltak. Bemutatandó kutatásomban e fekete kalapos hacker értelmezés képezi a számítástechnikai bűnelkövető fogalmának alapját is.

3.3. A számítástechnikai bűnelkövetők jellemzőinek értelmezése

³² Rogers, E. M.: A two-dimensional circumplex approach to the development of a hacker taxonomy. In: Digital Investigation, 2006, 3. évf., 2. sz., 97-102. p.

Kik a hackerek? – a hackerek demográfiai jellemzőire vonatkozó kutatási előzmények

Az általam vizsgált kutatások közül Goldschmidt tevékenységét szükséges kiemelni, aki a „jó” és „rossz” hacker dichotómia létjogosultságát és jellemzőit vizsgálta egy olyan közegben, ahol a hacker-társadalom jelentős szerepet vállal, mind politikai, mind bűnelkövetési oldalról.³³

Összesen 54 önmagát hackerként definiáló személlyel készített interjút, melyből 51 volt férfi. Csupán 5 rendelkezett számítógéppel kapcsolatos bűnelkövetői előélettel, mégis mindenki beszámolt büntetendő cselekmények elkövetéséről. Ahogyan írja: „*az interjúalanyok fiatalok, egyedülállók, tanultak, átlag feletti keresettel bírnak, európai vagy amerikai gyökerekkel rendelkeznek és nagyobb részt ateisták*”.³⁴

Korábban Hollinger is hasonló eredményre jutott, mint írja: „*a legtöbb számítógépes bűnöző fehér, nem erőszakos személyiségű, közép vagy felsőosztályba tartozó és büntetlen előéletű.*” Hollinger a hackereket „*elektronikai útonállóknak*”, olyan innovatív deviánsoknak kezelte, akik az úttörő kommunikációs csatornáknak és információs vállalatokban lévő sérülékenységekre leselkednek.

Flammich Mariann szociológus 2002-ben magyar hackerekkel végzett interjúkutatása részben igazolja, de több tekintetben ki is egészíti a külföldi kutatások eredményeit. Az általa megkérdezettek 15 és 24 év közöttiek voltak, jellemzően tanultak (mindenki műszaki, informatikai tudományokat folytatott, vagy éppen az irányban kívánt továbbtanulni). Többségük értelmiségi szülők gyereke és budapesti volt, de szerinte a lakhely nem befolyásolja szükségyszerűen a hackerek közösségéhez tartozást. A lányok alacsony számáról tudósít, amit a megkérdezettek öt főre becsültek országosan.

A hackerek magyarországi megjelenéséről két állítást említ a tanulmány szerzője. „*Az egyik vélemény szerint Magyarországon nyolc-tíz ember nevezhető igazi hackernek, és legfeljebb százan vannak azok, akik alacsonyabb szinten művelik a hackelést. A másik becslés nagyvonalúbb, 25-30 főt tart számon a komolyak, kétszázat pedig a szélesebb értelemben vett magyar hacker társadalom tagjai között.*”³⁵

A hacker társadalom tagjainak számszerűsítése nemzetközi szinten is problematikus, de több kísérlet is történt a meghatározása érdekében a kriminológiai és szociológiai vizsgálódások során. Sterling az 1990-es évek elején az aktív hackerek számát 5000-re, míg

³³ Goldschmidt, O.-T.: Identity Construction Among Hackers. In: K. Jaishankar (szerk.): Cyber Criminology Exploring Internet Crimes and Criminal Behavior. (London, 2011, CRC Press) 34. p.

³⁴ Goldschmidt: i. m. 35. p.

³⁵ Flammich: i. m.

az elit, tehát azok számát „*akik elég képzettek ahhoz, hogy szofisztikáltabb rendszerekbe is behatoljanak*” mindössze 100 főre értékelte globálisan.³⁶ Egy másik kutatás szerint ennél több, tehát 2000 valódi hacker és 10000 kezdő volt csak az Egyesült Államokban.³⁷

A számítógépes alvilágról a már említett, Jordan és Taylor szolgáltatnak kvantitatív adatokat. Kutatásukban azt a következtetést vonták le, hogy a támadások, illetve a támadók elsősorban az USA-hoz köthetők, azonban nem határozhatók meg e felmérések alapján az ún. „*hacker underground*” gócpontjai, hiszen egy olyan nemzetközi jelenségről van szó, ahol a nemzetállami határok jelentősége számottevően csökken, illetve nem szükséges fizikai kontaktus az elkövető és az áldozat között.³⁸ A magas látencia miatt az adatok véleményem szerint azonban igencsak pontatlanok lehetnek.

A kutatás jelez bizonyos szintű növekedést a támadások számában, amelyet kettős hatás eredményezhet. Ez egyrészt a bűnelkövetők számának növekedése, másrészt pedig a feljelentési hajlandóság javulása, azonban – ahogyan a kutatást vezető Taylor kifejti – egyik álláspont sem támasztható alá teljes egészében.

Az ezredforduló után az elkövetők számának és demográfiai adatainak mérése a kezdeti kihívások után még nehezebbé vált. A globalizált bűnözés és a magas fokú anonimitás biztosíthatósága a kvantitatív mérés lehetőségét is a minimumra csökkentette.

Ezzel kapcsolatos átfogóbb kutatást Bachmann végzett 2008-ban. A területet vizsgáló kriminológusokhoz hasonlóan ő is kifejti, hogy a hivatalos statisztikai adatok megbízhatósága alacsony, melyben legfontosabb probléma az elkövetőkre vonatkozó, valamint a trendvizsgálatokhoz szükséges adatok hiánya. Hangsúlyozza továbbá a viktimológiai felmérések szükségességét a bűncselekmények alacsony feljelentési hajlandóságának és a felderítésbe vetett alacsony bizalom okainak vizsgálatához.³⁹

Bachmann a kutatás részeként népszerű számítástechnikai konferenciákon gyűjtött adatokat kérdőív felhasználásával. A kérdőívek kitöltésének feltétele volt egy olyan információs rendszerbe történő behatolás elkövetése, melyre a tulajdonos nem adott engedélyt. A kérdőívet 124 résztvevő töltötte ki, melyből 3 volt nő. Uralkodó vélemény a

³⁶ Sterling, B.: *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. London, 1992, Viking. 76-77. p.

³⁷ Clough, B.; Mungo, P.: *Approaching Zero: Data Crime & the Computer Underworld*. London, 1992, Faber & Faber. 218. p.

³⁸ Jordan, Taylor: i. m. 761-762. p.

³⁹ Bachmann, M.: *Deciphering the Hacker Underground: First Quantitative Insights*. In: Holt, T. J.; Schell, B. H. (szerk.): *Corporate Hacking and Technology-Driven Crime. Social Dynamics and Implications*. (New York, 2011, Information Science Reference) 107. p.

szakirodalomban, hogy e közösségek működtetésében kiemelt a férfiak szerepe.⁴⁰ Van olyan, aki ezt a környezetet egy „maszkulin öltözőhöz”⁴¹ hasonlítja, de olyan is akad, aki a „férfiasság vadnyugati védjegye”⁴² kifejezéssel írja le e társadalmat.

Az előző kutatások fiatalkorú többségét megcáfolva Bachmann a számítástechnikában profi, biztonsági szakértők nagyobb számáról tudósított. A hacker közösségek professzionalizálódását támasztja alá az egyetemet végzett hallgatók 90%-os aránya, illetve a 18 és 19 év közötti fiatalok aktív hallgatói státusza is. A vizsgált szféra több mint 90%-a rendelkezett munkahellyel. Kiderült az is, hogy a megkérdezettek több mint fele soha nem volt házas.⁴³

Összefoglalva a fejezetben foglaltakat a hacker-társadalom és részben a „*hacker underground*” demográfiai jellemzőit adó nemzetközi és magyar kutatások is számos hasonlóságot fogalmaznak meg. A felmérések alapján – és részben kutatásom eredményeivel összhangban – kijelenthető, hogy a hackerek a technikai fejlődés egy korábbi szintjén inkább a fiatalkorúak és fiatal felnőttek körébe tartoztak. Az ezredforduló után azonban, ahogy a hackerek „hőskorának” fiatalkorúi egyre idősebbek lettek, illetve a technikai eszközök egyre szélesebb körökben váltak elérhetővé egyre egyenletesebbé vált az életkori megoszlásuk.

Látható vált az is, hogy a közösségek legalább háromnegyedét olyan férfiak alkotják, akik legalább középiskolai végzettséggel rendelkeznek, vagy aktív tanulmányokat folytatnak, valamint családi állapotukat tekintve egyedülállók.

A számítástechnikai bűnözés oksági elméletei

Számos kutatás a számítástechnikai bűnelkövetők személyiségének szociológiai értelmezésével foglalkozik, míg mások a pszichológiai tényezőkkel. A motiváció jelen dolgozatban a fehér, szürke és fekete kalapos hackerek elkülönítéséhez szolgálat elengedhetetlen alapot, azonban az egyéni személyiségminták kialakításában is fontos szerepet játszik. A fentiek alapján elemzem és értékelem az elkövetésre vonatkozó releváns oksági elméleteket, melyek a *motivációt*, illetve a *racionális választást* tartják a bűnelkövetői viselkedés alapjának, ill. azokat, melyek pszichológiai és szociológiai alapon konstruálják meg az elkövető profilját.

A motiváció szempontjából beszélhetünk olyan faktorokról, melyek „pozitívan” befolyásolják a bűnelkövetővé válást. Majid Yar a következőképp foglalja össze az ide tartozó

⁴⁰ Bachmann: i. m. 110.p.

⁴¹ Taylor, P. A.: Hackers: Crime in the digital sublime. New York, 1999, Routledge, 32. p.

⁴² Bachmann: i. m. 112. p.

⁴³ Bachmann: i. m. 112. p.

elméletek eredményeit: „Több motivációval foglalkozó kutató ténylegesen úgy látja a hackereket, mint racionális aktorok, akik tudatosan választják a tilalmazott cselekményeik iránti elköteleződést valamilyen féle jutalom, vagy kielégülés reményében.”⁴⁴

A Yar által példaként hozott elméletek a bűnelkövető személyiségének sarkalatos pontjaként azt a motivációs hálót határozzák meg, mely az adott személyt a számítástechnika jogkövető gyakorlatától a tilalmazott szféra felé irányítja.

A hatóságok általános szemlélethez közelítve leegyszerűbb az elkövetést mindössze a rosszindulat, vandalizmus és az indokolatlan rombolási szándék általános jelenségével magyarázni. A jogérvényesítők és számítástechnikai biztonsági vállalatok világszerte ezt a megközelítést alkalmazzák, mondván az információs rendszerek feltörése mögött nincsenek társadalmi legitimációs tényezők, így azok mind az öncélú rombolás archetípusaként értelmezhetők.

Az elméletek második csoportja még szintén valamilyen önös szándékot határoz meg, azonban ezek már túllépnek a „céltalan” cselekmények halmazán és a cél elérésének kielégítő hatásait helyezik a középpontba. Dowland és társai a személyiség magjának így többek között a kíváncsiságot, az izgalmat, az erőfitogtatást, a rendszerek feletti győzelem érzésének hajszolását tartják. Az információs rendszerekbe behatoló, rendszerelemeket romboló, onnan adatokat kivonó elkövetőket e belső legitimációs tényezők továbbá semlegesítik is a bűncselekmény elkövetésének értelmezésétől, melynek eredményeként a tudatban pozitív tevékenységként interpretálódik az adott behatolás.⁴⁵

A motivációt személyiség-meghatározó tényezőként értelmező elméletek harmadik csoportja a „hackelést” csupán instrumentumnak tekinti a hagyományos bűnözésben megfogalmazódó célok elérése érdekében. Itt valójában a kitűzött célnak megfelelő elkövetői személyiségről beszélhetünk. Cél lehet többek között a vagyonszerzés, a bosszú, vagy akár a vágyakozás, tehát a társadalommal egyidős motivációs háló ugyanúgy alkalmazható a hackerek identitás-struktúrája esetében is.⁴⁶

A motivációközpontú elméletek nézőpontjával kapcsolatban végül szükséges megemlíteni a Sykes és Matza által megfogalmazott neutralizációs technikákat.⁴⁷ A két kutató 1957-ben megfogalmazott elméletét már hatással volt több hackerekkel végzett kutatásra. A kvalitatív

⁴⁴ Yar: i. m. 33. p.

⁴⁵ Dowland, P.; Furnell, S.; Illingworth, H.; Reynolds, P.: Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. In: Computers and Security, 1999, 18. évf., 6. sz., 715–726. p.

⁴⁶ Grabosky, P.; Smith, R.: Telecommunication Fraud in the Digital Age: The Convergence of Technologies. In: David Wall (szerk.): Crime and the Internet. (London, 2001, Routledge) 29-44. p.

⁴⁷ Sykes, G. M.; Matza, D.: Techniques of Neutralization: A Theory of Delinquency. In: American Sociological Review, (1957, American Sociological Association) 22. évf., 6. sz., 664–670. p.

felmérések eredményei azt mutatják, hogy a bűncselekményeket elkövető hackerek önmeghatározásában fontos szerepet játszik a bűnelkövetői stigmától való elhatárolódás.⁴⁸ Azok a kutatások, melyekben elsősorban az „insider” definiálja saját személyiségét, elsősorban a befektetett munka bonyolultságát, a behatoláshoz szükséges intellektus felhasználását határozza meg a cselekmények középpontjának, illetve megnyilvánulásai alapján személyiségét is ez az általam „intellektuális felsőbbrendűségnek” nevezett önkép határozza meg alapjaiban.

A számítástechnikai elkövetőkkel foglalkozó másik nagy területet a pszichológiai és szociális faktorokat egyesítő megközelítések jelentik. Ellentétben a racionális választáson alapuló megközelítésekkel, itt a külső és belső tényezők általi befolyásoltság kerül a középpontba.

A pszichológusok egy része a számítástechnikai addikció oldaláról közelít. A hackelést, illetve az „online” világba való becsatornázást e kutatók az „*Internet Addiction Disorder*”⁴⁹ kifejezéssel illetik. Itt egy olyan rendellenességről beszélnek, mely hasonlóan a nikotin-, kábítószer- és alkoholfüggőséghez csökkent önuralmat eredményez, így alacsonyabb lesz az ebben szenvedő ellenállási képessége vágyaival szemben.⁵⁰

Az elméletek másik csoportja már a belső és külső tényezők eredményezte bűnelkövetői profil vizsgálatával foglalkozik. A szintén interjú vizsgálatok során felhasználható elméleti keretet jelen esetben Costa és McCrea amerikai pszichológusok „*Five Factor Theory of personality*”(FFT) elmélete biztosítja. Az 1992-ben publikált elmélet a számítástechnikai bűnelkövetők esetében a nyomozás során felhasználható pszichológiai profil elkészítéséhez szolgáltató kiváló alapot.

Az ötfaktoros modell öt endogén, tehát biológiai alapú tényezőt tartalmaz, melyek az extroverzió, a barátságosság, a lelkiismeretesség, az emocionalitás, és az intellektus. Ezekhez kapcsolódnak hozzá különböző exogén vagy más néven szociológiai tényezők, melyek kulturálisan determinált jelenségeket, személyes vágyakat és attitűdöket foglalnak magukba.⁵¹

A biológiai determinánsok között elsősorban olyan hagyományos bűncselekményeket elkövetésre is ható tényezőket találunk, mint a trauma, genetikai elváltozások, korábbi

⁴⁸ Yar: i. m. 34. p.

⁴⁹ Young, K.; Pistner, M.; O'Mara, J.:Cyber Disorders: The Mental Health Concern for the New Millennium. In: CyberPsychology and Behavior, 1999, 2. évf., 5. sz., 475–479. p.

⁵⁰ Érdekesség, hogy Kevin Mitnick amerikai és Paul Bedworth angol hackerek ítéletének részét is képezte a függőséget gyógyító kezeléseken való részvétel.

⁵¹ Costa Jr., P. T. ; McCrae, R. R.: (1992). Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual. Odessa: Florida, 1992, Psychological Assessment Resources Inc.

sérülések, betegségek, illetve minden olyan belső tényező, mely hatással van az intellektuális és személyiségfejlődésre.⁵² A hackerek közötti vizsgálatok némelyike diszlexiáról, diszkalkuliáról, sőt Asperger szindrómáról is tudósít.⁵³

A szociológiai determinánsok tekintetében szintén általánosabb tényezőket találunk. Ilyen a családi és társas kapcsolatok szerepe, a felmenőkkel és testvérekkel való viszony, az iskolai, illetve később a munkahelyi teljesítmény. Hackerekkel kapcsolatos kutatások e területen a szülői válaszokról, iskolai nehézségekről, iskolakerülésről vagy kábítószer-függőségről számolnak be.⁵⁴

Az öt centrális faktor esetében beszélhetünk egyedi elkövetői jellemzőkről. Ilyen a magas szintű analitikus és logikai gondolkodás, mely a behatolások végrehajtásának fontos eleme. Második tényező az introvertált, vagy épp extrovertált személyiség attól függően, hogy az elkövető milyen mértékben képes alkalmazkodni a virtuális tér új elemeihez, a változó elkövetési módokhoz. Emellett gyakori személyiségjellemző az alkalmazottak körében az elégedetlenség, mely a munkahelyi információs rendszerek elleni támadásoknál fontos motivációs tényező. Az elmélet harmadik eleme a szociális képességek alacsony foka, mely tartalmazza a kollégákkal és családdal kialakított bensőséges viszony hiányát, ill. az interperszonális kapcsolatok kiépítésére való képesség alulfejlettségét. Negyedik függő változóként a technikai képességek jelennek meg, mely az operációs rendszerek, programozási nyelvek, elkövetéshez használt programok és rendszer-sérülékenységek magas szintű ismeretét jelentik. Végül itt is fontos elem az internetfüggőség, mely hatással van az előző tényezőkre, abból a feltételezésből kiindulva, hogy a számítógép előtt töltött idő befolyásolja más személyiségelemek dominanciáját.⁵⁵

Az e fejezetben röviden, a teljesség igénye nélkül felvázolt irányzatok megfelelően példázzák a bűnelkövető hackerek személyiségének többszempontú értelmezését, melyek inkább mesterséges elválasztást tesznek lehetővé. Minden nagy elméleti csoport alkalmas a vizsgált szféra bizonyos személyiségjegyeinek kiemelésére és annak körülírására.

Vizsgálatom elkészítésében így a motiváció, ill. az exogén és endogén tényezők érvényességét hangsúlyozó faktorok egyaránt felhasználásra kerültek. Meglátásom szerint ezek a külön is tanulságos megközelítések csak egymással párbeszédben és együttműködve

⁵² Lickiewicz, J.: Cyber Crime Psychology – Proposal of an Offender Psychological Profile. In: Problems of Forensic Sciences 2011, LXXXVII. sz., 242. p.

⁵³ Zieger, W.; Föttinger, C. S.: Understanding the hackers mind – a psychological insight into the hijacking of identities. Krems, 2004, Danube University.

⁵⁴ Chiesa, R.; Ducci, S.; Ciappi, S.: Profiling Hackers: The Science of Criminal as Applied to the World of Hacking. New York, 2008, CRC Press.

⁵⁵ Lickiewicz: i. m. 242-243. p.

képesek meghatározni komplex személyiségstruktúrákat és egyben feltárni a bűnelkövetővé válás sarkalatos pontjait, melyek – a hagyományos bűnözéshez hasonlóan – a külső és belső tényezők által kialakított személyiség motivációiban ragadhatók meg igazán.

Létezik-e hacker-társadalom?

Az egyéni szinten túl, a közösségek fejlődésében és működésében is jelentős változásokat hoztak az elmúlt évtizedek. Már az 1990-es évekre is láthatóvá vált a hackerek látens társadalmának pluralizálódása. Meyer és Thomas kutatásai szerint voltak a számítástechnikát üzleti keretek között használók, a hackelési technikákat fegyverként kezelők, valamint azok a csoportok, akik szerint a hacking az egyetlen lehetőség a számítógépes tudás terjesztésére.⁵⁶ E megkülönböztetést a mai közösségekre alkalmazva mindinkább a biztonságtechnikai iparban dolgozó hackerek közösségére, a bűnelkövetői csoportokra, illetve az etikus hackereket tömörítő fórumokra gondolhatunk. A közösségek nagy kiterjedését jelzi, hogy a két kutató már a technikai fejlettség egy korábbi szakaszában is a számítógépes alvilág világméretű társadalmáról beszélt.

A hacker-társadalmak általános jellemzőivel később már a szociológiai kutatások is foglalkoztak. Taylor és Jordan szerint az *„az elképzelt közösség, amelyet a hackerek kreálnak és fenntartanak a következő elemekkel körvonalazható: technológia, titkosság, anonimitás, a tagság változékonysága, férfidominancia és motivációk. A közösség itt úgy értendő, mint egy társadalmi csoportkonstrukció kollektív identitása, vagy ezzel összefüggően, mint egy társadalmi csoport »kollektív képzelete«.*”⁵⁷

A közösség tagjainak elsődleges és legelemibb része a technológia, illetve a technológiával való kapcsolat. Ez annak a közös hite, hogy a technológia olyan új, váratlan célok felé irányulhat, ami alátámasztja a hackerek kollektív képzeletét. Minden közösség alapját a számítástechnika iránti érdeklődés határozza meg attól függetlenül, hogy tudásukat célzottan bűnelkövetésre, vagy a jog keretei között használják fel. Véltetően a rendelkezésre álló tudásuk és technika iránti érdeklődésük nélkül a közösség működésképtelenné válna és elveszítené minden funkcióját.

A titkosság azonban ambivalens szerepet játszik a közösségek működésében. Egyrészt cselekedeteik titkosságot igényelnek, másrészt viszont az információ megosztása és az elismerés megszerzése publicitást von maga után. A hacker-közösségek és online fórumok tagjainál általában az elismerés utáni vágy erősebb, mely a közösségen belüli elfogadást,

⁵⁶ Meyer, Thomas: i. m. 31-67. p.

⁵⁷ Jordan, Taylor: i. m. 762-763. p.

nagyobb tiszteletet és több tudást eredményezhet. *„Sok hacker trófeákat gyűjt lemásolt dokumentumok, vagy programok formájában, mert ez bizonyítja a közösségnek, hogy a hacker »ott járt«.*”⁵⁸

Az anonimitás egy titkossághoz hasonló fogalom, mely szintén a közösség látens jellegét erősíti, azzal a különbséggel, hogy itt a hacker „offline” személyazonosságának védelméről beszélhetünk és nem a cselekmény titkosságáról. Ennek fenntartására szolgálnak a valós adatokat elrejtő szoftverek, a kizárólag álnéven történő virtuális kommunikáció, illetve a tagok közötti fizikai érintkezés hiánya.⁵⁹

A tagság állandó változása laza szerveződést eredményez, melyből a kilépés a szubkultúrákkal ellentétben kevésbé problematikus. A közösségek saját szabályaik szerint működnek és többségében nincs vezetőjük. Jellemzője, hogy a közösségben való bennmaradás gyakran nehezebb, mint az abból való kilépés. *„Ha megállsz, ha nem csinálod egy hétig, a dolgok változnak, a hálózat mindig változik. Nagyon gyorsan változik és minden trükköt fejből kell megtanulnod, az alapértelmezett jelszavakat, a kiaknázható hibákat.*”⁶⁰ Másik lehetőség viszont – a tanulmány írói szerint – az élethosszig tartó tagság, melyet a bűnügyi nyilvántartásba vétel és a gyanú jelent.

A demográfiai adatokból is látható a férfi dominancia, melynek okai lehetnek szocializációs folyamatok, mely során a fiúkat tanítják meg gyakrabban a technológia felhasználására, valamint a közösségek hegemon maszkulinitása is befolyással van a nemi megoszlásra.⁶¹ A bűnözői közösségek esetében ez a jellegzetesség hatványozottan igaz lehet, abból kiindulva, hogy általánosságban a nők szerepe a hagyományos bűnözésben is alacsonyabb a férfiakénál.⁶²

Azokban az esetekben, amikor nem egyéni elkövetésről van szó, a csoport megvitatja a cselekmény mögötti célokat is, mely a kollektív identitás erősítésén keresztül a bennfentesség érzését kelti a tagokban. A csoport egységes működése továbbá általános motivációs törekvéseket is tartalmaz, melyek közvetlen együttműködés nélkül is megteremtik a – külső szemlélők számára idegennek tűnő - elvi alapokat.

A virtuális bűnökkel foglalkozó kriminológusok egy része már a számítógépes közösségek megjelenése óta foglalkozik a devianciával, a deviáns címkével, ill. annak elfogadásával. E

⁵⁸ Jordan, Taylor: i. m. 765. p.

⁵⁹ uo.

⁶⁰ Jordan, Taylor: i. m. 766. p.

⁶¹ Jordan, Taylor: i. m. 767. p.

⁶² Lásd: Messerschmidt.

kriminológusok elsősorban Howard S. Becker 1963-ban publikált „Kívülállók”⁶³ című művén keresztül igyekeznek megérteni a számítástechnika deviánsnak titulált közösségeit.

A „hacker” kifejezés mediatisált fogalmából kiindulva itt egy olyan társadalmi konstrukcióról beszélhetünk, mely képlékennyé teszi a szó valódi jelentést, így változtatva meg az eredetileg semleges gyűjtőfogalom alkalmazását. Mindez koherens Becker azon feltevésével, hogy a társadalom általános konformitásával szemben automatizmussá vált minden „szabályszegő” csoport deviáns címkével ellátása.

Annak ellenére, hogy egy teljesen más társadalmi-gazdasági környezetben fogalmazódott meg Becker címkézéselmélete, a hacker közösségek megítélésében fontos szerepet játszik e mesterséges címke felvétele és elfogadása. Általánosan jellemző, hogy a társadalom és a hatóság azokat a magatartásmintákat, melyeket nem ért, vagy nem tud az általánosan elfogadott normák alapján megmagyarázni, deviánsnak tételez. Ez a hacker közösségekkel kapcsolatosan hatványozottan igaz, hiszen egy olyan távolságtartással, félelemmel és egyben kíváncsisággal kezelt csoportról beszélhetünk, melyet különösen nehéz megérteni és átlátni valódi működését.

Ez a szekvenciális modell a marihuána-fogyasztóvá válást és a deviáns karriert vizsgálva kiemeli, hogy különbséget kell tenni azon elkövetők között, akik csak fiatalkorban követnek el bűncselekményt, tehát nem válnak felnőtt elkövetővé, illetve a szekvenciákat végigjárók között.⁶⁴ Ez utóbbi esetben a deviáns közösségekbe bevonódás és más deviánsokkal történő érintkezés, tehát a becsatornázódás fázisa különösen fontos. A hackerek közösségében ez egészen fiatalkorban kezdődik és vagy véget ér az első felelősségre vonásnál, vagy folytatódik és átlép az akkor már felnőtté váló, közösségbe egyre inkább bevonódó egyén a tényleges megbélyegzés fázisába.

E fázisban a bűnügyi nyilvántartásba vételt követően már az egyén legfontosabb jellemzője a „hacker” kifejezés mögötti társadalmilag konstruált negatív jelző lesz. A számítástechnikai elkövetők körében ez lehet olyan cselekmény is, melynek társadalmi veszélyessége elenyésző ugyan, de az elkövetés bonyolultságából eredő misztikum mégis súlyosbítja megítélését.

A társadalom hozzáállása és bizalmatlansága a bűnelkövetői csoportok felé tolva az egyént a címke elfogadását és az érvényesülés egyetlen lehetőségét eredményezi.⁶⁵

Látható, hogy a másodlagos deviancia, a bűncselekményt elkövető hackert az egyetlen olyan közösségbe kényszeríti, melyben gyakorolhatja tevékenységét, így a pozitív

⁶³ Becker, Howard S.: Outsiders. Glencoe, 1963, IL: Free Press.

⁶⁴ Becker: i. m. 19-25. p.

⁶⁵ Becker: i. m. 19-25. p.

visszacsatolás kiegészülve a fentebb említett „közös identitással” megalapozza a bűnelkövetői karriert.

Mindazonáltal szükséges kiemelni Becker –kutatásom eredményei tekintetében egyik legfontosabb - álláspontját, mely szerint, ha a rajtakapás jó időben történik és választási lehetőséget ad, akkor elkerülhető a deviancia fokozódása, melynek egyébként végső lépése a szervezett deviáns csoportba való belépés lenne. Feltételezésem szerint a számítástechnikai bűnelkövetőknél ez két esetben igaz. Egyrészt, ha fiatal korban egy nagyobb horderejű bűncselekmény elkövetéséért megfelelően történik a felelősségre vonás, illetve másrészt, ha az adott illető – bármilyen korcsoportba is tartozzon – nem semlegesíti magát a bűnelkövetés ténye alól.

Az itt példaként felvázolt, közvetlenül számítástechnikai bűnelkövetők közösségére kondicionált elmélet és az attól független címkézésemélet segítségével válik értelmezhetővé a hacker közösségek vizsgálatának célja. Láthatóan egy nehezen körülírható, és definiálható közegről beszélhetünk, melynek számos egyedi jellemzője van, ugyanakkor az egyén közösségben betöltött szerepének és a társadalmi folyamatok hatásainak szempontjából hasonló jellegzetességeket is megfigyelhetünk. A közösségekbe történő bevonódást hasonló tényezők befolyásolják, mint a konvencionális elkövetők esetében, azonban a közösségek szervezettsége és működése jelentős eltéréseket mutat.

4. Hackerek Magyarországon. Saját empirikus kutatás bemutatása

„Én mindig azt mondom, hogy az internet olyan, mint egy kút. Ha beledobsz valamit, azt onnan soha nem szedi ki senki.”⁶⁶

Az előző fejezetekben tárgyalt nemzetközi kriminológiai elméletek és hipotézisem vizsgálata egy empirikus kutatás elkészítését tette szükségessé. Kutatásomban a számítástechnikai bűnelkövető létének alátámasztása mellett célom volt a bűnözővé válás kritikus pontjainak meghatározása. Emellett pedig, a magyarországi hacker közösségek vizsgálatainak hiányában körül kellett határolnom azokat a csoportokat is, melyek az - általam megalkotni kívánt - számítástechnikai bűnelkövető fogalmába tartozókat tömörítik. Elsősorban a már összefoglalt kutatások alapján meggyőződésemm volt az is, hogy a bűnelkövetővé váló hackerek döntéseit, virtuális térhez való viszonyát jelentősen befolyásolja a hálózatokon szerveződő, „computer underground” néven ismert közösség.

Bachmann kvantitatív módszerrel elkészült kutatásával szemben a terület vizsgálatához szélesebb körben alkalmazott kvalitatív metodológiát választottam. Ennek részeként tematikus interjúk elkészítésével és egy fókuszcsoport vizsgálattal vált lehetővé a magyarországi hackerek és közösségek esszenciális jellemzőinek definiálása.

Feltáró jellegű vizsgálódásom Budapest területére korlátoztam az IT biztonsági vállalatok és a számítástechnikai tudományterületen végzetek nagy koncentrációja miatt. Szempont volt emellett a város kiemelkedő népességszáma is, mely fizikailag is közelebb hozza egymáshoz a tapasztalatot és tudást szerezni kívánó etikus és bűnelkövető hackereket egyaránt.

A kutatásomban vizsgált bűncselekményt elkövetők jellemzőinek, motivációinak, és társadalmi státuszuk széles skálája, ill. a magas látenciája az ún. hólabda módszer alkalmazását tette szükségessé. A módszer lényege, hogy a már elért mintába került személyekkel kiépített kapcsolatokon keresztül jutottam el olyan személyekhez, akik kutatásom szempontjából releváns információval rendelkeztek.

Az interjúk beszélgetések segítségével teszteltem hipotézisem egyéni bűnelkövetésre vonatkozó részét, ill. meghatároztam a hackerek és számítástechnikai bűnelkövetők közötti különbségeket és hasonlóságokat. A fókuszcsoport vizsgálattal az egyes személyek közösségben való tevékenységét, világképük egymásra hatását és bűnözésről alkotott szemléletüket tártam fel.

⁶⁶ 3. sz. interjúalany – etikus hacker

Az interjú vizsgálat során IT biztonsági szakértőkkel, etikus és bűncselekményt elkövető hackerekkel vettem fel a kapcsolatot, míg a fókuszcsoport beszélgetést egy heterogén összetételű hacker közösséggel készítettem el. Feltéve, hogy a csoportba tartozók kontrollált fókuszcsoporthoz hasonló beszélgetés közben, egymásra reagálva egymás véleményére hatva egy sor olyan információt szolgáltathatnak, amelyet egy interjú során nem.

A hackerek megtalálásának nehézségei miatt több pontból indult ki a megkérdezettek felkeresése. Kezdetben felvettem a kapcsolatot több IT biztonsági vállalattal, így ebből pontból kiindulva értem el interjúalanyaim háromnegyed részét. A megkeresések másik fázisában számítástechnikai fórumokon keresztül a kutatás célját feltárva kértem a fórumokat használok segítségét. Ennek eredményeként egy akkor házi őrizetben lévő hackerrel, majd rajta keresztül a közösségbe tartozó másik hackerrel is felvettem a kapcsolatot. A fókuszcsoporthoz hasonló beszélgetést egy IT biztonsági szakértő segítségével szerveztem meg.

Megkeresést intéztem egyes hatóságoknál dolgozó szakértők felé is, ezek azonban nem jártak eredménnyel. A Legfőbb Ügyészséget, a Fővárosi Főügyészséget, a Nemzeti Nyomozóirodát, illetve ezen belül a Csúcstechnológiai Bűnözés Elleni Osztályt kerestem fel sikertelenül. Az áldozatok vizsgálatához a Szellemi Tulajdon Nemzeti Hivatalával próbáltam felvenni a kapcsolatot, melynek számítógépes adatbázisát 2013. szeptember 16-án érte támadás. A hatóság elutasítása miatt nem kerülhetett sor ennek, a hackerek körében sok vitát kiváltó ügy részleteinek vizsgálatára.

Az elkészült beszélgetések anonim, az interjúalanyok személyének azonosítására alkalmatlan módon rögzítettem és dolgoztam fel. A legrövidebb beszélgetés 45, míg a leghosszabb 2 óra 10 percet vett igénybe, míg a fókuszcsoporthoz hasonló beszélgetés 2 óra 30 perc időtartamban zajlott.

1. táblázat: A kutatás során megkérdezettek száma

	Interjú	Fókuszcsoporthoz	Összesen
IT biztonsági szakértő	4		4
Etikus hacker	4	5	9
Büntetett hacker	2		2
Összesen:	10	5	15

A táblázatban látható csoportosítás az interjúkban elhangzottak alapján történt. E csoportok között vannak bizonyos átfedések, melyek elsősorban az IT biztonsági szakértők és etikus hackerek esetében jelentősebbek, azonban ha büntetőjogi tényállások megvalósítása szerint

próbálnánk differenciálni, mind a három kategóriában lennének átfedések. Ez utóbbi azt jelenti, hogy a legtöbb esetben hangzottak el példák büntetőjogi tényállást megvalósító cselekményekről. Fontos kiemelni, hogy két interjúalanyál elítélés is történt információs rendszer és adatok elleni bűncselekmény elkövetése miatt, míg egy személy számolt be felmentő ítéletről.

4.1. Demográfia

A kutatás során megkérdezettek életkorukat tekintve 19 és 39 év közöttiek voltak. Az interjú és fókuszcsoport beszélgetésben összesen résztvevő 15 személyből 13 volt férfi és 2 nő. A legmagasabb iskolai végzettség 9 esetben egyetem, 2 esetben szakképesítés, 4 esetben érettségi volt. Ez utóbbinál 3 esetben folyamatban lévő egyetemi képzésről, míg 1 esetben pályakezdői munkanélküliségről beszélhetünk.

4.2. A kutatás eredményei

Hogyan válik valaki hackerré? Hogyan lesz valakiből bűnelkövető hacker?

Kérdéseim első modulja a megkérdezettek életútjára vonatkozott a bűnelkövetővé válás kritikus pontjainak és a hacker-közösségekbe bevonódás folyamatának megértése céljából. Az itt elhangzottak alapján három fontos megállapítás tehető.

- a technológia iránti érdeklődés életútyszerű, a vizsgált alanyok közösségekbe való bevonódása független a későbbi foglalkozástól,
- az információs rendszer és adatok elleni bűncselekmények elkövetése integráns részét képezi a tanulási folyamatoknak,
 - a fiatalkorban a szociológiai és szocializációs faktorok jelentősen befolyásolják a legalitás és illegalitás közötti választást.

A fiatalkor vizsgálatának eredményei azt mutatják, hogy az információs technológia iránti érdeklődés már gyermekként elkezdődik. Az adatok alapján úgy tűnik, hogy 7-8 éves korban megfigyelhető bizonyos szintű érdeklődés kialakulása, mely a középiskolai, gimnáziumi oktatási szint elérésére már programozási szintű tudást eredményez. Az informatikai rendszereket érintő bűncselekmények elkövetése szempontjából kritikusnak a 14 és 20 év közötti, tehát a serdülő- és fiatal felnőttkor időszaka tekinthető.

Mind a fiatalabbak, mind az idősebbek számoltak be tanulási folyamataik során elkövetett különböző rendszerfeltörésekről, web sérülékenységek kihasználásáról, melyek száma a felnőtté válás során folyamatos csökkenést mutatott. Ezek között iskolai információs rendszer

feltörése, fájlmegosztó oldalak üzemeltetése, de legnagyobb számban a weboldalak hibáinak kihasználása szerepelt. Tetteiket szinte kivétel nélkül a tanulási vágy, a kíváncsiság, a közösségek elfogadása motiválta.

„Ezt nem lehet könyvekből megtanulni (...) szerintem valójában mindenki gray hat. A white hat inkább csak egy nagyon jó rendszergazdának a leírása. A tanulás során szerintem mindenki tör fel rendszereket.”⁶⁷

Ezzel kapcsolatban két megállapítás tehető. Egyrészt, fiatal korban látható az általános társadalmi normák, így részben a jogszabályok figyelmen kívül hagyása a legtöbb tanulásban lévő hackernél. Ez a későbbiekben enyhülni kezd, de az információs rendszerek feltörésének gyakorlata felnőtt korban is egy sajátos, közösségi morál alapján kerül megítélésre.

Másrészt, a fiatalkori forrófejűségen és esetleges tettvágyon kívül semmi jele nincs bűnelkövetői szándéknak. Egészen a felnőtté válásig a bűnelkövetővé, etikus hackerré vagy IT szakemberré válók között nem fedezhetők fel nagy különbségek a rendszerfeltörés megítélésének és végrehajtásának szempontjából.

Az elkövetett cselekmények azonos tényállása ellenére azonban úgy tűnik, vannak olyan motivációs eltérések, melyek az egyéni és családi szocializációból, szociális helyzetből eredhetnek. Előbbi – a pszichológiai elméletek tanulságaira gondolva – lehet többek között a személyiségi jogok tiszteletben tartásának hiánya, a felelősség ignorálása, a tulajdon tiszteletének alacsony foka („virtuális vandalizmus”), míg utóbbi a szülők alacsony keresete, tanulási lehetőség hiánya vagy a teljesítmény értékelésének elmulasztása a család részéről.

Összefoglalva e tényezők egy olyan erkölcsi gát hiányát eredményezik, melyek a későbbiekben visszatartják a felnőtté váló személyt a súlyosabb bűncselekmények elkövetésétől. A bűnelkövetővé válás vizsgálatának szempontjából egyik legfontosabb interjú során, melynek alanya egy 19 éves már büntetett hacker volt, az derült ki, hogy egy információs rendszer feltörésénél elsődleges szándéka a rendszerek hibáira való figyelmeztetés és az érvényesülés vágya volt, de ennek ellenére minden behatolás után adatbázisokat készített az ott található személyes adatokból. Valahol itt található meg a rendszerek feltörésének az a kissé homályos határa, mely láthatóvá teszi, ki sodródik később további bűnelkövetés felé és ki áll meg a hibákra való figyelemfelkeltés szintjén.

Véleményem szerint ez kardinális pontja a későbbi számítástechnikai bűnelkövetésnek, annak ellenére, hogy jogilag mindkét cselekmény egy kategóriába tartozik. Az egyéni morál és értékítélet, mely a hackerek közösségében általánosan felülírja a büntetőjogi szabályokat

⁶⁷ 3. sz. interjúalany – etikus hacker

így választási helyzetet teremt. A fiatalkorban általában szürkezónában lévő cselekmények pontos elemzése így rávilágíthat a későbbi bűnelkövetői karrier lehetőségére és segíthet megelőzni más, gyakrabban már vagyoni motivációk kialakulását.

A megkérdezettek a Magyarországon megjelenő információs rendszer elleni bűncselekményeknél úgy tartják, hogy e tanulási időszak esetei a legnagyobb számban ismertek a hatóság számára. Itt még nagy szerepet játszik a feltűnési és érvényesülési vágy, mely kortól függetlenül a tanuló - általuk inkább script kiddienek, mint igazi hackernek tekintett - egyénekre jellemző. A megkérdezettek elmondása és saját tapasztalataim azt mutatják, hogy a felderített, illetve a médiában megjelenő információs rendszer elleni bűnelkövetés hazánkban nagyobb részt e cselekményeket jelenti.

A láthatatlan bűnelkövetés

A technika iránti érdeklődés, a tudás megszerzése, a hackerré válás és a fiatalkor együttes hatásaként teremtnének meg a valódi bűnelkövetővé válás tényezői. Az interjúk alapján látható, hogy a hackerek közössége a professzionalizálódás egy bizonyos szintjén kettéválik. A hagyományos bűnelkövetést befolyásoló tényezők alapján érvényessé válik a fekete kalapos hacker kifejezés, melynél már a vagyoni vagy információszerzési motiváció felülírja az általános hacker mentalitással magyarázható univerzális célokat. Így a bűnelkövetők egy olyan csoportja jön létre, mely számára már nem a hírnévszerzés, vagy a feltűnési vágy lesz az elsődleges, hanem inkább a Jordan és Taylor kutatásban látható titkosság és anonimitás feltételeinek szigorú betartásával, a látenciában maradás.

Ez alapján, Magyarországon is vannak olyan bűnelkövetői csoportok, melyek információs rendszerek feltörésével foglalkoznak, de ezekről szinte semmit sem tudunk. Ezen a szinten már olyan tudatos bűnelkövetésről van szó, melyben minimális lebukási lehetőséggel óriási haszonszerzés lehetséges, kiegészülve azzal, hogy nincsenek országhatárok, így jóval nagyobb a támadási felület.

Az IT biztonsági szakértők tapasztalatai alapján a célzott, vállalatok érintő, illetve az államellenes támadások esetében is úgy tűnik, hogy kiemelkedően magas a látencia. A sérülékenységeket hivatalosan vizsgáló szakértők számos olyan esetről számoltak be, melynél történt bűncselekmény észlelés, de a megtámadott intézmény nem kívánt feljelentést tenni. Ezek között voltak olyanok, ahol ismert volt az elkövető személye is. Ennek egyik oka lehet a cselekmény alacsony tárgyi súlya, másik a biztonsági hibák titokban tartása, míg harmadik a hatósági tevékenységbe vetett alacsony bizalom.

A bűncselekményt elkövető csoportok működésének fontos jellemzője a rejtettség mellett az alacsony innovációs szükséglet. A biztonsági szakértők arról tudósítanak, hogy a technika folyamatos fejlődésével, új programok megjelenésével nincs szükség olyan mértékű innovációra a bűnözés területén, mint másfél évtizede volt. Ez azt jelenti, hogy egy bizonyos szintű tudás lehetővé teszi a vagyoni célzatú bűncselekmények elkövetését anélkül, hogy folyamatos önfejlesztésre lenne szükség. Az információszerzési - vállalatokat érintő - támadásoknál viszont egyre nagyobb szervezettség és tudás figyelhető meg.

„Olyan alacsonyan van a léci védelmi oldalon, hogy bejutni egy rendszerbe sokszor annyi, mint egy gyerektől elvenni a cukorkát.”⁶⁸

Egy megkérdezett IT biztonsági szakértő emellett kritikus pontnak tartja a hackerek szervezett bűnözésbe való belépését, illetve eszközzemélyként való felhasználását. Itt arról van szó, hogy vagyoni motivációval rendelkező hackerek könnyebben bevonódhatnak bűnszövetségekbe, illetve szervezett bűnelkövetési formákba, melyben szerepük az információs rendszerek elleni támadások végrehajtásáig terjed.

Felelősségvállalás, önmeghatározás

A bűnelkövetés jellegzetességeinek meghatározásának következő lépéseként a bűncselekmény elkövetéséért érzett felelősségvállalást vizsgáltam. Ennek elsődleges célja a bűnismétlés okainak feltárásán keresztül bűnmegelőzési lehetőségeket ajánlani az igazságszolgáltatás számára.

Az eleméleti alapvetések közül az interjúk felvétele során e szempontból Sykes és Matza öt tényezőből álló neutralizációs teóriájának érvényessége vált hangsúlyossá.⁶⁹ A kriminológusok által meghatározott öt technika a következő: a felelősség tagadása, a kár okozásának tagadása, az áldozat létének tagadása, az elítélők elítélése, és a magasabb értékekre hivatkozás.

Az interjúk beszélgetésekre visszatekintve a számítástechnikai bűncselekményt elkövető két hackernél mind az öt technika érvényre jutott, míg az etikus hackereknél a magasabb hatalomnak való megfelelés, illetve a kár okozásának tagadása volt jelen néhány esetben. Az IT biztonsági szakértőknél már egyik technikát sem véltem felfedezni, ők minden cselekménytípustnak átlátták a következményeit és a felmerülő aggályokat.

⁶⁸ 7. sz. interjúalany – szakértő

⁶⁹ Sykes; Matza: i. m. 664–70. p.

A bűncselekményt elkövetőknél a felelősség tagadása szinte minden cselekmény elkövetésénél fellelhető volt, a vagyoni motivációjú bűnözés esetében a szociális helyzetre hivatkoztak, míg az információs rendszerek feltörésénél a rendszerek hibái „jogosították” fel őket azok kihasználására. Többször is elhangzott a beszélgetések során, hogy egy olyan rendszert feltörni, melyet rosszul védenek, nem bűncselekmény. Analógiát vonva itt egy olyan szemlélet látható, melyben egy alacsony kerítésen átlépni nem jelent birtokháborítást.

A kár okozásának tagadása magában a virtuális tér egyediségében ragadható meg. A fizikai megjelenés hiánya olyan érzést kelt a rendszert feltörőben, mintha nem is lennének hatásai cselekedeteinek. Legfontosabb semlegesítő tényező annak érzése, hogy amit a virtuális térben lemásol az adott személy, az nem tűnik el, hanem duplikálódik, tehát kettő lesz belőle, így ez valójában nem is lopás. Másik tényező ezzel kapcsolatban a hatások tovagyrűzésének figyelmen kívül hagyása.

„Az a különbség a kettő között pszichológiailag, hogy amikor szétörsz egy kukát akkor az a kuka volt-nincs, de egy informatikai rendszernél mindent működőképesen hagysz, csak készítesz belőle egy másolatot. Ez valószínűleg sokkal kisebb korlátot jelent mindenkinek fejben. (...) átirok itt egy számot, de nem szakad le a plafon, nem gyullad rám a ház, hanem a világ túlsó végén történik egyszer valami.”⁷⁰

Az áldozat létének tagadása szorosan összefügg a hatások tovagyrűzésének figyelmen kívül hagyásával. Az ezzel kapcsolatos kérdésnél gyakran jelent meg a bankszámlák feltörésének esete. A különböző pénzintézeteket, biztosítótársaságokat, pártokat, vállalatokat nem tekintik áldozatnak, mondván azok biztosítva vannak, így valódi károkozás nem történik, vagy ha igen, azt akkor sem érzik meg.

„Banknál szerintem nincs áldozat (...) ők egy milliárdot sem éreznének meg. /Kérdező: Azért ez megjelenik valahol, nem?/ Elképzelhető, de nem tartom valószínűnek.”⁷¹

Az etikus hackerek esetében mindössze az adathalászattal össze nem kapcsolható rendszerfeltörés esetleges kárainak tagadása látható. A fókuszcsoporthoz tartozók beszélgetés során az derült ki, hogy közösségi szinten csak a vagyoni kárt tekintik valódinak, az információvesztés, vagy bizalomvesztés nem aggályos.

Mások elítélése annyiban figyelhető meg, hogy a tudás pozitív visszacsatolásának hiánya egy rendszerszintű ellenszenvet eredményez az elkövetők egy részénél. Itt legfontosabb a hatóságokkal szembeni ellenszenv, de politikai-gazdasági szereplőkkel való szembehelyezkedés is tapasztalható.

⁷⁰ 7. sz. interjúalany – IT biztonsági szakértő

⁷¹ 6. sz. interjúalany – büntetett hacker

Végül a magasabb értékekre hivatkozás mind a két csoport esetében a feltárt hibákra való figyelemfelkeltés. Ez azt jelenti, hogy a büntetőjogi tényállásszerűség ellenére pozitív cselekedetről beszélnek, mely felülírja a konvencionális szabályok betartását. Több példán keresztül láthatóvá vált, hogy ezt a tevékenységet reakciótól függetlenül mindenki pozitívnak tartja, annak ellenére is, ha az esetek egy részében feljelentés, vagy fenyegetés lesz a vége.

„Igazából komolyabb kárt nem is akartam okozni, csak amikor úgy volt, hogy muszáj. Mikor tudom, hogy az adott weboldal használóinak kára származhat belőle”⁷²

Az öt neutralizációs technika segítségével látható, hogy a bűnelkövető hackerek és nagyon ritkán más hackerek sem látják a cselekmények mögötti problémákat. Ez nem a sérülékenységek jóindulatú bejelentésénél okoz valójában aggályokat, hanem a bűnelkövetővé válás megelőzhetősége szempontjából. Míg az adott személy a cselekményét nem látja bűncselekménynek, vagy nem akarja érte vállalni semmilyen formában sem a felelősséget, addig a későbbi súlyosabb bűnelkövetés veszélye is fokozottan fennáll. Ennek következtében a fiatalkorú, még képlékeny értékítéllettel rendelkező fiatal hackerek esetében már az első hatósági érintkezés alkalmával különösen fontos lenne a cselekménnyel okozott kár tudatosítása. A 6. sz. interjúalany esetében először kiszabott megrovás például hatástalannak bizonyult, de nem az elszánt bűnelkövetői célok miatt, hanem mert további 4 nyomozás mellett sem érti, hogy miért vonják felelősségre a rendszerek hibáinak jelentése okán.

Mi jellemző a magyarországi hacker-társadalomra?

Magyarország hacker-társadalmát a megkérdezettek egy egyre kiterjedtebb és képzettebb szakmai közösségként írják le, mely különböző konferenciákon, képzések keretében mind virtuálisan, mind fizikailag kapcsolatban van egymással. E közösségek egyre kevésbé tekinthetők rejtettnek, hiszen a mára iparágga fejlődött informatikai biztonság területén számos vállalat és több tucat szakértő tevékenykedik. E közösségekben is megfigyelhető a szenvedélyszerű, élethosszig tartó bevonódás, a tudás alapvető kritériumának szükségessége, azonban mára inkább csak laza szakmai szerveződésről beszélhetünk.

A biztonságtechnikai ipartól független hackerek, illetve a bűnelkövetők tekintetében azonban még fellelhetők egyediséget jelző elemek. A kutatás során kiderült, hogy az iparágba be nem tagozódó csoportoknak – a tudás minimumkövetelményén kívül - két összetartó

⁷² 6. sz. interjúalany – büntetett hacker

tényezője van. Az etikus hackereknél ez a Levy által meghatározott hacker etika,⁷³ melyben a decentralizációs szemlélet és az egyedi értékítélet még szilárdan él, míg a bűnelkövető hackereknél ez a véghezvitt cselekményekből származó tekintély.

A bűnelkövetők közösségére fókuszálva további különlegességek is láthatók. Ellentétben a szubkultúrákkal, itt megfigyelhető az államhatárokon átívelő csoporttagság, mely a zárt fórumokon való információszerzést jelenti. Fizikai érintettség a csoportok tagságában kevésbé van jelen és valódi bizalmi közösségekről sem beszélhetünk. A bűnelkövető hackerek között bizonyos szintű lojalitás megfigyelhető, mely kiterjed egymás bűncselekményeinek titokban tartására, de a - hallottak alapján - mindenki magáért felel.

„Mindenkinek van egy nick neve, csak ezek ismerik egymást. Hogy valós személyként ki az az illető általában nem tudjuk. Vannak akiket személyesen is ismerek, de ez nem átlagos. Nem fogod mindenkinek híresztelni, hogy te ki vagy. Kialakulnak barátságok, de ha az ember óvatos, akkor ez mindig nevek barátsága.”

Az elméleti okfejtésben látható virtuális identitás ez alapján fontos részét képezi azoknak a csoportoknak, melyek cselekményei hatásági reakciókat váltanak ki. A közösség szerveződésének így van egy kollektív identitása, melyet a tudás vagy valamilyen aktuális cél tart össze, de amint a közös érdekek megszűnnek a közösség működése is diszfunkcionálissá válik.

E közösségek megközelíthetősége a kívülállók számára problematikus, csak olyanok kerülhetnek be, akik a közösség értékítélete alapján valamit fel tudnak mutatni, illetve a megfelelő szakmai kérdéseket teszik fel. Kívülállóként a csoportok működését így problematikus pontosan körülírni, hiszen több ezer hozzászólás, rendszerfeltörések, azonos világnézet szükséges ahhoz, hogy teljesen megbízható információkat lehessen kinyerni.

Az ideológiai színezet és a hatalomellenesség a bűnelkövetői csoportoknál inkább csak a neutralizáció részét képezi, míg az általánosabb, de nem hivatásos hackerek közösségénél egy rendszerszintű bizalmatlanság, hatalomellenesség és konspiratív szemléletmód is látható csíráiban, mely azonban racionális alapokból táplálkozik. A közösség tagjai az informatikai biztonság államigazgatási, gazdasági és jogszabályi problémáira fordítanak kiemelt figyelmet, melynek integráns része az információbiztonság alacsony szintjének kritikája is.

A bűnelkövetéssel érintett hackerek számának tekintetében 100 és 200 fő közötti becsléseket kaptam, mely más bűncselekmények elkövetőihez képest jóval alacsonyabb szám.

⁷³ Levy: i. m.

Ennek ellenére az áldozatok elérhetősége, a bűnözés nemzetközi jellege és a magas fokú neutralizáció felhajtó ereje lehet a következő generációk új típusú bűnözésének.

4.3. Kutatási lehetőségek

A jövőben a felvázolt eredmények árnyalása érdekében szükség lenne egy hatósági megkérdezésre, mely elősegítheti az előző fejezetekben a következőkben javasolt bűnmegelőzési tevékenység előmozdítását, ill. nagyobb rálátást adhat az ügyészségek, bíróságok e területen végzett munkájára és a felderítés hatékonyságát növelő lehetőségekre.

A hackerbűncselekményekkel érintettek vizsgálatában nagy előrelépést jelentene a célzott támadások kriminológiai elemzése, mely már a nemzetközi számítástechnikai bűnözés aspektusaira is rávilágítana. Ennek részeként külön figyelmet igényel a számítástechnikai eszközökkel elkövetett szervezeti bűnözés, mely központjában a gazdasági, kormányzati szféra ellen irányuló látenciában maradó cselekmények feltárása áll.

5. Javaslatok a bűnmegelőzés, bűnfelderítés és büntetéskiszabás területe számára

Mind a rendelkezésre álló szakmai tényanyag, mind az elkészült interjúk fontos tanulságokat hordoztak magukban a számítástechnikai bűncselekmények magyarországi kezelésével kapcsolatban.

A kissé egyoldalú kép, melyet a hatósági megkérdezés elutasítása és a témával kapcsolatos magyar nyelvű szakirodalom hiánya okozott, nehezzé teszi a kész javaslatok megfogalmazását, így inkább irányelvek felvetésére szorítkozom.

A számítástechnikai bűnözés informatikai rendszereket érintő részterületével kapcsolatban számos bűnmegelőzési, felderítési és büntetéskiszabási feladat kínálkozik. A legnagyobb probléma, hogy egy olyan összetett társadalmi jelenséggel állunk szemben, melyben minden államnak, minden társadalmi rétegnek, és minden információs rendszert használó egyénnek szerepe van. Akár az elkövetőkre, akár az áldozatokra gondolunk, a virtuális tér mobilitásából következően az érintettek száma nem korlátozható és a károk is felbecsülhetetlenek lehetnek. Az információs rendszerek támadásának tovaryűrűző hatása lényegében bárkit áldozattá tehet.

Bűnmegelőzési javaslatok

E szempontból a legtöbb teendő az oktatás területére hárul. Egyrészt, mivel az internet használatának tanulási folyamatában vagyunk, a tudatos információbiztonsági felkészítés elengedhetetlen a megfelelő szocializáció biztosításához. Az informatikai eszközök és hálózatok használatának terjedésével nem járt együtt a használatra való felkészítés, így az internet megfelelő táptalaját képezi egy új bűnelkövetői típus megjelenésének.

Hosszabb távon általános oktatási szintű felkészítés szükséges, mely segít megszüntetni az informatika használata és a biztonságtudat között fellelhető aránytalanságokat.⁷⁴ Magyarország kiberbiztonsági stratégiája⁷⁵ ugyan említi a tudatossággal és az oktatással kapcsolatos feladatokat, azonban ezek mind elvi szinten fogalmazódtak meg. Az infrastrukturális támadásokon kívül, az egyéneket érintő biztonság területe számára is csak a szituációs védekezés tudatosítását hangsúlyozza.

A bűnözés szempontjából a társadalmi szintű bűnmegelőzés hangsúlyozására lenne igény. Mind az áldozatok, mind az elkövetők esetében társadalmi szemléletváltásra van szükség, az

⁷⁴ Itt már látható bizonyos szintű előrelépés, mely Nemzetközi Gyermekmentő Szolgálat, oktatási tevékenységében ragadható meg.

⁷⁵ 139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról <http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf> (Letöltés ideje: 2014.09.16)

okozott kár tudatosításának érdekében. E téren bűnmegelőzési stratégiánk mindössze egy bekezdésében található információk, melyek a televízió és a számítógépes játékok erőszak-közvetítő hatásán kívül szintén csak az áldozattá válás lehetőségének elkerülését hangsúlyozzák.⁷⁶

Bűnfelderítési javaslatok

Kutatásom alapján látható, hogy egy reaktív szemlélet vált uralkodóvá e cselekmények felderítésében. Ez a már bekövetkezett információs rendszer elleni támadásokat követő „tűzoltást”, eseménykezelést jelenti.⁷⁷ Az információs rendszert érintő bűnfelderítés területén vizsgálódásaim arra mutattak rá, hogy a feljelentések igen kis részét teszik ki a bűnözés társadalmi jelenségének, illetve ezek is inkább a fiatalkori, kevésbé jelentős cselekményeket érintik. A valóban nagy aggodalomra okot adó támadások az esetek többségében nem jutnak a hatóságok tudomására, vagy a nyomozás megszüntetésével zárulnak. Az elkövetett számítástechnikai bűncselekmények felderítésében a kutatásomban leírt jellemzőkkel bíró közösségek ismerete, motivációik meghatározása elősegítheti a bűncselekményt elkövetők elérését és az esetleges bűnözői csoportok feltérképezését.

A bűnözés területi mobilitásának kezelésére több nyugat-európai példából látható, hogy egy háromszintű szervezetre lenne szükség.⁷⁸ Ez a gyakorlatban azt jelentené, hogy helyi, területi és országos szinten a hagyományos rendőri tevékenység kiegészítésével specializált egységek támogató munkáján keresztül lehetne hatékonyabbá tenni elsősorban az információs rendszerek elleni, de akár egyéb számítógépes környezetben elkövetett bűncselekmények nyomozását is. Továbbá e téren a biztonságtechnikai iparral történő együttműködés is növelné a felderítés esélyét, valamint elősegíthetné a bűnmegelőzés fejlődését.

Büntetéskiszabási javaslatok

Pozitív szerepe lehet e téren a közérdekű munkának, illetve a jóvátételnek, hiszen mindkét joghátrány segítheti az okozott kár tudatosítását. Ez akkor érheti el hatását, ha olyan befogadó intézményről vagy személyről van szó, ahol az adott bűncselekménnyel okozott kár realizálódott.

⁷⁶ 1744/2013. (X. 17.) Korm. határozat a Nemzeti Bűnmegelőzési Stratégiáról (2013–2023)

<http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13172.pdf> (Letöltés ideje: 2014.09.16)

⁷⁷ Ezzel foglalkozó szerv a Kormányzati Eseménykezelő Központ, mely azonban csak állami és önkormányzati intézményekkel kapcsolatos védelmet lát el.

⁷⁸ Leukfeldt et. al.: i. m. 256-257. p.

Olyan területeken ahol tudatosítható az információbiztonság szerepe és elősegíthető az elkövetéshez használt tudás jogi keretek közötti felhasználása még inkább csökkenthető a bűnismétlés esélye. Az alternatív szankciók segíthetnek felismerni az okozott kár valós megjelenésének tényét és megszüntetni a fizikai távolságból származó neutralizációt is.

Ez mind fontos a bűncselekmények számának csökkentése szempontjából is, hiszen a jelenleg felnövő generáció számára a technika fejlődésével exponenciálisan nő a számítástechnikai tudással rendelkező fiatalok száma, így akár a bűnelkövetői karrier kezdetét is jelenthetik a fiatalkori cselekmények.

Összefoglalva: társadalmi szintű figyelem szükséges a területre, annak érdekében, hogy a bűnelkövetés új formájaként a virtuális tér ne termeljen ki újabb bűnözői csoportokat és, hogy azon fiatalok, akik eddig a fizikai társadalom kontrolljai miatt nem követtek el bűncselekményt később se használják az informatikát, illetve az informatikai tudásukat figyelemfelkeltésre, vandalizmusra, vagy akár vagyoni célzatú bűnelkövetésre.

6. Konklúzió

A számítógépes bűnözés e speciális területének kriminológiai vizsgálata több szempontból is nehéz feladatnak bizonyult. A legnagyobb problémát a fogalmak meghatározása, a terület büntetőjogi szemlélettől elhatárolása és a bűnözéssel érintett csoportok vizsgálata jelentette. További kérdéseket vetett fel a bűncselekmény egyediségének bizonyítása, illetve a hacker-társadalom jellemzőinek pontos körülírása is.

A számítástechnikai bűnözés elméleti alapvetésinek és a nemzetközi szakirodalom tanulságainak az áttekintése eredményeként egy olyan kriminológiai elkövetői kép rajzolódott ki számomra, mely bűnelkövetése nem magyarázható önmagában egyetlen oksági elmélettel sem. A biológiai, pszichológiai, szociológiai, valamint részben a racionális választás tényezői egy olyan komplex elkövetői halmazra mutatnak, mely talán az eddigi legheterogénebb jellemzőkkel rendelkező bűnelkövetői csoportot foglalja magában. E csoportnak egyetlen szilárd központja a tudás, és a tudás felhasználásának minden jogszabályi keretet felülíró vágya, melyet az egyéb, bűnelkövetést magyarázó tényezők eltérő mértékben, de együttesen tesznek árnyaltabbá.

A kriminológia oksági elméleteinek számítástechnikai bűnözésre konvertált tanulságai és kutatásom eredményei egymást kiegészítve mégis lehetővé tették a számítástechnikai bűnöző fogalmának meghatározását.

A kriminológiai alapokon elvégzett vizsgálatom azt mutatja, hogy megalkotható a számítástechnikai bűnelkövető kriminológia kategóriája. A fekete kalapos, vagyis bűnelkövető hacker nemzetközi fogalma, - mely a hackerekre jellemző kíváncsiságon, tudásvágyon kívül az információs adatbázisok építését, a virtuális vandalizmust, vagy akár a vagyonszerzést emelte ki többlettényezőként – segítette elő a magyar hackerek vizsgálata révén e kriminológiai számára értelmezhető fogalom létrehozását.

Ennek értelmében számomra e bűnelkövető az informatika világát másodlagos élettereként értelmező olyan személy, aki számítástechnikai tudásának felhasználásával információs rendszer elleni bűncselekményeket úgy követ el, hogy abban információszerzési, vagy károkozási motívum is megjelenik. Bűncselekményének legfontosabb mozzanata magába a rendszerbe történő behatolás, illetve az ezt megkönnyítő program létrehozása. Tevékenysége egyediségét erősíti, hogy az adott rendszer feltörésével szerzett haszon a fizikai valóságban csak részben, vagy egyáltalán nem realizálódik.

Hipotézisem bűnelkövetői egyediséget hangsúlyozó része egy szempontból azonban árnyaltabb lett. Az elkészített interjúk arra világítottak rá, hogy a bevonódásnak csak egy bizonyos pontjáig beszélhetünk vegytiszta számítástechnikai bűnözésről. A szociális helyzet, a társadalmi-gazdasági körülmények és bizonyos szinten a pszichológiai jellemzők átveszik a virtuális identitás szerepét, így a Magyarországra inkább jellemző vagyoni célzatú bűnelkövetésnél már túlsúlyba kerülnek a hagyományos bűnözői csoportokra vonatkozó jellegzetességek. Ebből következik, hogy az e cselekményeket elkövetők már inkább bűnelkövetők, mintsem hackerek.

A számítástechnikai bűnözésre vonatkozó elméletek másik tanulsága a hacker közösségek sajátos jellemzőinek körülírása volt. Az ezzel foglalkozó kutatások a titkosság, anonimitás, férfidominancia, az egyedi motivációk, és a tagság változékonyságának bemutatásán keresztül lehetővé tették a bűnelkövetői csoportokba betagozódás jellemzőinek feltárását. Az intézményelméleti alap pedig, értelmezhetővé tette a csoporthoz tartozás stigmatizáló szerepét és a társadalmi reakciók bűnismétlésre gyakorolt hatásait.

A magyarországi hacker közösségek vizsgálatának eredményeként és az elméleti alapok segítségével sikerült rávilágítanom a magyar közösségek egyedi jellemzőire is, melyek közül legfontosabb a nagy fizikai kiterjedtség, a személyazonosság védelme, illetve - a fizikai valóságban működő mikro-társadalmakkal ellentétben - a nagyfokú bizalmatlanság. A tagság szempontjából különösen fontosnak bizonyult a külföldi hackerekkel való kapcsolattartás is, mely az új vírusok, behatolási módszerek átvételében, ill. kollektív célok megfogalmazódásában jelenik meg.

A deviáns közösségek kiterjedtségéről azonban, már jóval kevesebb információt kaptam. Egy lazábban szerveződő közösség tagjainak elérésén keresztül elsősorban a számítástechnikai bűnözők csoportjának – fentebb említett - jellemzőiről tudósíthatok, de a mélyebben gyökerező, esetleg bünszövetségben, bűnszervezetben működő, vagy hírszerzési tevékenységet végző hackerekről konkrét tényeket nem állíthatok.

A magyarországi IT biztonsági szakértőkkel, valamint hackerekkel elvégzett önálló empirikus kutatásom számos hatósági, oktatási tevékenység szükségességére is rávilágított, melyben kitüntetett szerepe van a fiatalkori bűnmegelőzésnek, figyelembe véve, hogy a fiatalkor a későbbi bűnelkövetésben nemcsak a számítástechnikai, hanem a hagyományos bűnelkövetés megelőzésének is kiemelt terepe. A kriminológia számára ezért fontos továbbra is hangsúlyozni a maximális figyelmet igénylő nevelési feladatokat, mely az áldozattá és az elkövetővé válás elkerülése miatt egyaránt prioritás.

A súlyosabb fiatalkori bűncselekmények tekintetében ezért kiemelt figyelmet kell fordítani az egyes cselekmények morfológiájának, a mögöttük lévő motivációk és az okozott kár mértékének vizsgálatára. A konkrét ügyek feltárása így segíthet meghatározni a későbbi bűnismétlés valós esélyeit és megtalálni az adott ügyben alkalmazandó megfelelő eszközöket.

E kriminológia számára még kevésbé átlátható terület társadalmi szintű figyelmet igényel a potenciális áldozatok és elkövetők heterogenitása következtében. Az bizonyossággal állítható a kutatásban elhangzott interjúk alapján is, hogy a szituációs bűnmegelőzés mellett a biztonságtechnikai ipartól és az kibervédelemtől teljesen eltérő megoldások szükségesek az információs technológiában rejlő veszélyek elkerülése végett.

Ahogy arról már korábban írtam, kriminológiai szempontból is születtek a számítógépes bűnözés szinte minden területeivel kapcsolatban nagyobb volumenű értekezések, azonban ezek egyike sem tért ki az általam számítástechnikai bűnelkövetőknek hívott egység mélyebb, empirikus vizsgálatára. A további tudományos munkák elengedhetetlenek a terület valós veszélyeinek, kriminálstatisztikai adatainak és a bűnözés tendenciáinak meghatározása érdekében.

A dolgozat által képviselt szemlélet is arra utal, de a vizsgált szféra egyediségéből is következik, hogy a kriminológia, szociológia és pszichológia területének egyaránt szerepet kell vállalnia a társadalmi szintű megoldások kialakításában.

Lezárás dátuma: 2014.11.04.

Irodalomjegyzék

Monográfiák

Balogh Zs. Gy.: Jogi informatika. Bp.-Pécs, 1998, Dialóg Campus.

Beck, U.: A kockázat-társadalom - Út egy másik modernitásba. Bp., 2003, Századvég Kiadó.

Becker, H. S.: Outsiders. Glencoe, 1963, IL: Free Press.

Chiesa, R.; Ducci, S.; Ciappi, S.: Profiling Hackers: The Science of Criminal as Applied to the World of Hacking. New York, 2008, CRC Press.

Clough, B.; Mungo, P.: Approaching Zero: Data Crime & the Computer Underworld. London, 1992, Faber & Faber.

Costa Jr., P. T.; McCrae, R. R.: Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual. Odessa: Florida, 1992, Psychological Assessment Resources Inc.

Holt, T. J.; Schell, B. H. (szerk.): Corporate Hacking and Technology-Driven Crime. Social Dynamics and Implications. New York, 2011, Information Science Reference.

Jaishankar, K. (szerk.): Cyber Criminology. Exploring Internet Crimes and Criminal Behavior. London, 2001, CRC Press.

Kabay, M.E.: A Brief History of Computer Crime: An Introduction for Students. Norwich, 2008, Norwich University.

Korinek L.: Bűnözési elméletek. Bp., 2006, Duna Palota és Kiadó.

Leukfeldt, R.; Stol, W.: Cyber Safety: An Introduction. 2012, Eleven International Publishing.

Levy, S.: Hackers: Heroes of the Computer Revolution. Garden City, 1984, Doubleday.

Littman, J.: The Fugitive Game. Online with Kevin Mitnick-The inside story of the great cyberchase. Boston, 1996, Little Brown and Company.

Mitnick, K. D.; Simon W. L.: A legendás hacker – A megtévesztés művészete. Bp., 2003, Perfect-Pro Kft.

Nagy Z. A.: Bűncselekmények számítógépes környezetben. Bp., 2009, Ad Librum Kft.

Parti K.: Az eladók már rég hazamentek. A büntetőjog mint az online pornográfia szabályozásának eszköze. Doktori értekezés. Pécs, 2013.

Rogers, E. M.: Diffusion of Innovations. New York, 1983, Free Press.

Schneider, B.: Secrets and Urs, Digital Security in a Net.Jerked World. Wiley, 2000, Computer Publishing, John Wiley and Sons, Inc.

Sterling, B.: The Hacker Crackdown: Law and Disorder on the Electronic Frontier. London, 1992, Viking.

Stoll, C.: The Cuckoo's Egg: tracking a spy through the maze of counter-espionage. New York, 1989, Simon and Schuster.

Taylor, P. A.: Hackers: Crime in the Digital Sublime. New York, 1999, Routledge.

Wall, D. (szerk.): Crime and the Internet. London, 2001, Routledge.

Yar, M.: Cybercrime and Society. London, 2006, SAGE Publications Ltd.

Zieger, W.; Föttinger, C. S.: Understanding the hackers mind – a psychological insight into the hijacking of identities. Krems, 2004, Danube University.

Tanulmányok

Bachmann, M.: Deciphering the Hacker Underground: First Quantitative Insights. In: Holt, T. J., Schell, B. H. (szerk.): Corporate Hacking and Technology-Driven Crime. Social Dynamics and Implications. (New York, 2011, Information Science Reference) 105-127. p.

Dowland, P., Furnell, S., Illingworth, H.; Reynolds, P.: Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. In: Computers and Security, 1999, 18. évf., 6. sz., 715–726. p.

Durkheim, É.: A bűnözés normális jelenség. In: Gönczöl K., Kerecsi K. (szerk.): A deviancia szociológiája. Szöveggyűjtemény. (Bp., 1996, Hilscher Rezső Szocpol. Egyesület) 9-15. p.

Flammich M.: Hackerek: Vázlat a magyar szubkultúráról. 2002.
http://www.mediakutato.hu/cikk/2002_03_osz/01_hackerek/#03

Goldschmidt, O.-T.: Identity Construction Among Hackers. In: Jaishankar, K. (szerk.): Cyber Criminology Exploring Internet Crimes and Criminal Behavior. (London, 2011, CRC Press) 31-53. p.

Grabosky, P.; Smith, R.: Telecommunication Fraud in the Digital Age: The Convergence of Technologies. In: Wall, D. (szerk.); Crime and the Internet. (London, 2001, Routledge) 29-44. p.

Hannemyr, G.: Technology and Pleasure: The Art and Craft of Hacking. 1999.
<http://hannemyr.com/en/sj98.html>

Jordan, T.; Taylor, P. (1998): A sociology of hackers. In.: The Sociological Review. Oxford, 1998, Blackwell Publishers, 757-780. p.

Kaspersky Lab Report. Financial cyber threats in 2013
<http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-2013-eng-final.pdf>

Kincsei A. (2007): Technológia és társadalom az információ korában. In: Pintér R. (szerk.): Az információs társadalom (Bp., 2007, Gondolat - Új Mandátum) 47-64. p.

Kunos I.: A számítógépes bűnözés a modern információtechnológia felhasználása a bűnözésben. In. Belügyi Szemle, 1999, 11. sz., 28-42. p.

Lickiewicz, J.: Cyber Crime Psychology – Proposal of an Offender Psychological Profile. In: Problems of Forensic Sciences 2011, LXXXVII. sz., 239-252. p.

Meyer, G.; Thomas, J.: The bawdy world of the bythe bandit: A postmodernist interpretation of the computer underground. In: Schmallegger, F. (szerk.): Computers in criminal justice. (Bristol (Indiana): Wyndham Hall, 1990, Wyndham Hall Press, Inc.) 31-67. p.

Parti K. (2013): Harc az online illegális tartalom ellen. In: Vókó Gy. (szerk.): Kriminológiai Tanulmányok 49.(Budapest, 2012, OKRI) 49-68. p.

Rogers, E. M.: A two-dimensional circumplex approach to the development of a hacker taxonomy. In: Digital Investigation, 2006, 3. évf., 2. sz., 97-102. p.

Sutherland, E. H.: White-Collar Criminality. In: American Sociological Review. 1940. 5. évf. 1. sz. 1-12. p.

Sykes, G. M.; Matza, D.: Techniques of Neutralization: A Theory of Delinquency. In: American Sociological Review, (1957, American Sociological Association) 22. évf., 6. sz., 664–670. p.

Young, K.; Pistner, M.; O'Mara, J.: Cyber Disorders: The Mental Health Concern for the New Millennium. In: CyberPsychology and Behavior, 1999, 2. évf., 5. sz., 475–479. p.

<http://www.verizonenterprise.com/DBIR/2014/>

Egyezmények, stratégiák

Az Európa Tanács Budapesten, 2001. november 23-án kelt, számítástechnikai bűnözésről szóló egyezménye. Convention on Cybercrime, CETS. No. 185 - 23. XI. 2001.

<http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20Hungarian.pdf>

139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

<http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf>

1744/2013. (X. 17.) Korm. határozat a Nemzeti Bűnmegelőzési Stratégiáról (2013–2023)

<http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13172.pdf>