SIMON KRISZTINA

TRANSZNACIONÁLIS INFORMATIKAI BŰN(CSELEKMÉNY)ÜLDÖZÉS

Bevezetés

Tanulmányomban szándékomban áll bemutatni az informatikai bűnözés egyik klasszikus, és talán legismertebb formáját, mégpedig a szerzői és szomszédos jogok megsértésével kapcsolatos magatartásokat, egészen egyszerű és – szándékaim szerint – a hétköznapi ember számára is jól érthető módon. Ezt követően vitaindító szándékkal is, vázolnék pár probléma megoldási alternatívát, ahogy mások, és ahogyan mi is harcolunk ellene, végül pedig szeretnék pár javaslattal élni, hogy hogyan lehetne akár hazai, akár nemzetközi szinten felvenni a küzdelmet az informatika világával szemben.

Ismeretlen ismerősök

Először is, szeretném egy fiktív történeten keresztül ismertetni az elkövetői archetípusokat, és magának a cselekménynek az elkövetési módjait. Mindenekelőtt fontos azt leszögeznünk, hogy – mint arra a címben is utalok – ezek a srácok általában nem ismerik egymást személyesen, sosem találkoztak, nincs információjuk a másik koráról, vagy bármilyen személyes adatról, ők egyszerűen – előítéletektől mentesen – valóban a másik tudása alapján vonnak le következtetéseket és osztják elismeréseiket. Az interneten keresztül találkoznak és kötnek barátságokat, ott beszélgetnek, és ott élik mindennapjaikat is.

Tehát a típusok. Először is itt van [dvi] és [jojo],[339] két 15-16 év körüli srác, akik felhasználói szintű informatikai ismeretekkel rendelkeznek, és a plusz, amit tudnak nyújtani, amitől ők fontosak, azaz, hogy rengeteget ülnek a számítógép előtt. Többnyire a késő esti, éjszakai órákban, napi átlag 6-8 órán keresztül elérhetőek az interneten. Több on-line játékot is játszanak párhuzamosan, rendszeres fórumlátogatók, és hozzászólók, tehát mindezek következtében nagyon sok (több száz) ismerősre tesznek szert a legkülönfélébb társadalmi rétegekből.

Következő barátunk [electryc], 17 éves szintén középiskolás. Magának való, nincs sok barátja, a lányoknál nem próbálkozik, kevés emberrel érti meg magát a valós világban, és meg kevesebb érti meg őt. Számára nem jelent csábítást a disco, vagy a biliárd, viszont mindig tud a legújabb játékokról, vagy egyéb szoftverekről, van róla véleménye, már ki is próbálta, sőt sok esetben, a tulajdonában is van egy példány.

[sziti] 20 éves, főiskolás, és tanulmányait támogatandó hamar munka után nézett. Fiatalabb korában azzal hívta fel magára a figyelmet, hogy előkelő helyen végzett pár számítástechnikai játék versenyen, úgyhogy fel is figyelt rá egy szoftverfejlesztő cég, ahol, mint játéktesztelőt foglalkoztatják. Na, nem kell nagy dologra gondolni, a feladata

[339] A zárójelbe tett szó tulajdonképpen egy saját maguk által választott becenév, vagyis szakszóval nick név. Ők az internet világában így nevezik magukat, ez jelenik meg általában az e-mail címükben, aláírásaikban, ha valamilyen fórumon, vagy on-line játékban hozzászólnak, azt is e mögé a név mögé bújva teszik meg.

mindössze annyi, hogy amikor a programfejlesztés egy bizonyos fázisba ért, folyamatosan játsszon vele, minden pályát, minden lehetőséget kipróbálva, és az esetleges programozási hibákra felhívja a figyelmet, illetve egyéb, építő jellegű javaslatot tegyen.

[kos] 23 éves, végzős programozó, ő már saját közegében él, elég antiszociális, nincs egészséges kapcsolata a valós világban élő emberekkel, valahogy nem értik meg egymást. Sajátos – informatikai – szaknyelvet használ a mindennapi érintkezések során is, és ez nem könnyíti meg a kapcsolatteremtést számára. Fordított életet él, vagyis éjszaka fenn van és dolgozik 3-4 óráig, 11-nél hamarabb viszont csak akkor kel fel, ha nagyon muszáj. Valahogy úgy nézhet ki, mint a legelvontabb informatikus a munkahelyünkön, akinek külön lelkülete van, és aki nyugodtan járkál(hatna) az alábbi feliratú pólóban: „Rendszergazda vagyok, ha mosolyogni látsz, kezdhetsz félni..."

Ők a tagjai a mi kis képzeletbeli csapatunknak, sok esetben ők sem ismerik a csapat minden tagját legfeljebb hallomásból, általában egy-két taggal tartanak közvetlen kapcsolatot.

Munkamegosztás

Most pedig, lássuk, hogyan működik ez az olajozott gépezet, hogyan is lesz nekünk, vagy gyermekünknek pár fiatal csínytevéséből a reméltnél korábban, na és persze jóval gazdaságosabban meg az a szuper játék, vagy a legújabb mozi.

A képlet viszonylag egyszerű, mint minden bűnelkövetői csoportnál itt is munkamegosztással dolgoznak, vagyis a cselekménysorból mindenki csak egy bizonyos elemet valósít meg, képességeitől és összeköttetéseitől függően.

[sziti] barátunk épp a legújabb játékot teszteli, már úgy 10 hónapja, amikor végre megcsillan a fény az alagút végén, és úgy néz ki, hiba nélkül fut a program. Még megbizonyosodik egy-két technikai újításról, s amikor már tényleg kiadás közeli állapotba kerül a szoftver, egy óvatlan pillanatban készít róla egy másolatot. Felhelyezi egy – csak a csoport számára elérhető – szerverre, ahonnan [kos] már le is töltötte, és el kezd ismerkedni vele. No, ne a játékleírásra vagy a szabályrendszerre tessék gondolni. Őt ez nemigen érdekli. Az ő szórakozása ebben az újonnan megszerzett játékban a védelem feltörése lesz. Valahogy, még ő sem tudja pontosan mi lesz a megfelelő módszer, de hatástalanítania kell a védelmi megoldást. „Amint" ez sikerül neki, ami teljesen változó, és kiszámíthatatlan időtartam lehet, pár órától egészen a több hetes időintervallumig, már teszi is vissza a csoport szerverére. Az eddigi rekordot a Toca Race Driver 2 nevű játék tartja, amit 4 hónapba telt feltörni, és így is csak annyit értek el, hogy játszható lett a játék, de az igen bonyolult telepítési eljárás miatt valószínűleg senki nem használta, inkább csak a presztízs miatt fejezték be. Jön a következő fázis [electryc] vezényletével, aki még csak le sem tölti a szoftvert a saját winchesterére, hanem ott, a központi szerveren csatol hozzá egy előre magírt infófájlt, amiben két mondatban vázolja, hogy mi módon lehet a programhoz hozzájutni, vagy elhelyezi a kulcsot, és pár szóban mintegy megjegyzi, hogy ezért a játékért melyik csoportnak lehetünk hálásak. Ha ez megvan, tömöríti a játékot és elhelyezi egy másik, igen-igen gyors szerveren, amihez csak egy elit- gondosan szűrt rétegnek van hozzáférése, ilyen például [jojo] és [dvi], akik ezt követően különböző ftp vagy fájlcserélő szerverek útján elterjesztik ezt a sok munkával előállított és aranyáron piacra dobott szoftvert.

Most vegyük szemügyre mindennek a cselekménysornak a büntetőjogi vetületét. [sziti] barátunk önmagában is tényállásszerűen megvalósítja a sikkasztás törvényi

tényállását, hiszen a rá bízott idegen dolgot jogtalanul eltulajdonítja. De mi a helyzet [kos]sal, aki első ránézésre a szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszásáért felelne, ámde itt két dolgot is figyelembe kell vennünk. Az egyik, hogy a műszaki intézkedés hatásos volt-e, hiszen a szerzői jogról szóló törvény szerint, a *műszaki intézkedés minden olyan eszköz, alkatrész vagy technológiai eljárás, illetve módszer, amely arra szolgál, hogy a szerzői jog jogosultja által nem engedélyezett cselekményeket – rendeltetésszerű működése révén – megelőzze, illetve megakadályozza. A műszaki intézkedést akkor kell hatásosnak tekinteni, ha a mű felhasználást a jogosultak a hozzáférést ellenőrző vagy védelmet nyújtó olyan eljárás – különösen kódolás vagy a mű egyéb átalakítása, vagy másolatkészítést ellenőrző mechanizmus – útján ellenőrzik, amely alkalmas a védelem céljának elérésére.*[340] Tehát, ha egy DVD filmet, vagy cd lemezt a kereskedelmi forgalomban kapható programmal törték fel, és tettek másolhatóvá, akkor ki lehet vajon mondani azt, hogy a műszaki intézkedés nem volt hatásos!? Pár éve igen népszerű volt egy DVD decompiler nevezetű program, 30 $-os áron, amely másoláskor különösebb kérdés, vagy választás nélkül törte fel a védelmet, mintegy automatikusan. A RIAA – az amerikai lemezkiadók szövetsége – pert indított, kérve a program betiltását, amely kérésnek a bíróság eleget is tett. Kis idő múlva a kérdéses program más néven újból piacra került.

A másik fontos dolog, amit nagyító alá kell vennünk, az a haszonszerzés, melyet a jogalkotó, mint szükséges célzatot jelöl meg. Ezzel elérkeztünk a probléma egyik kulcskérdéséhez, merthogy – bár tudom, ez első hallásra életszerűtlennek tűnik – de ezeket a fiatalokat nem motiválja a haszonszerzés. Nem törekednek rá és általában nem is származik belőle hasznuk. Modern Robin Hood-ként tűnnek fel a többi felhasználó szemében akik „megszerzik" a „kizsákmányoló" multiktól az áhított programot és eljuttatják az egyszerű néphez. A hírnév az, ami leginkább hajtja ezeket a saját közösségük perifériáján élő srácokat, hogy az újabb és újabb kihívásoknak is eleget tudjanak tenni, az egyre szigorodó biztonsági előírásokat is ki tudják játszani. Sajnos ez az a momentum, ami miatt máris elfelejthetjük a tényállásszerűséget, hiába látszik rögtön, hogy a cselekmény, amit elkövettek bűn, de a Btk. mai állapota szerint mégsem bűncselekmény. [electryc] tevékenységét aztán végkép nem tudom ütköztetni, mivel az ő tulajdonában egyetlen példány sem található, a mindössze pár perces tevékenysége mégis kulcsfontosságú a csoport számára, hiszen mit ér az elvégzett munka, ha nem tudja meg a nagyvilág?! Márpedig ebben a játékban csak az elsőt díjazzák! Az a csapat, aki a leggyorsabban a legjobb törést készíti, annak a programja terjed el világszerte, és aki csak egy órával később rukkol elő a megoldással, arra már senki nem kíváncsi. De térjünk csak vissza megint magához a cselekményhez. Az első számú probléma itt is a haszonszerzés, mint célzat, ami ugye hiányzik, a második gond a vagyoni hátrány okozása, amit szintén meghatároz a jogalkotó, mint eredményt. A kérdés csak az, hogy a vagyoni hátrány meglétére illetve mértékére miből is következtetnek. Hiszen az a tény, hogy egy oldalon ott van egy program, még nem jelenti azt, hogy bárki letöltötte, vagyis birtokba vette. De, még ha ki is lehetne deríteni, hogy hányan töltötték le, akkor is vizsgálni kellene, hogy egyébként ezek a felhasználók a kereskedelmi forgalomban esetleg megvásárolták volna-e ezt a programot vagy csak kíváncsiságból, esetleg státusszimbólumként mutogatják, hogy „bezzeg nekik ez is megvan". Vagy esetleg azt vizsgálják, hogy a forgalmazó bevétele az adott termékből milyen mértékben esett vissza a kérdéses időpontban? Aligha hiszem. A jelenlegi gyakorlat

[340] A szerzői jogról szóló 1999. évi LXXVI. törvény 95. § (3) bek.

szerint az a meghatározó, hogy hány sértettje van egy bűncselekménynek, és mivel a szerzői jogokat általában a kiadók, cégek gyakorolják, hiába derül ki az internetre egy adott kiadó gondozásából minden előadó minden lemeze, ez akkor is csupán egy sértettként szerepel. Az út még meglehetősen göröngyös és kitaposatlan ezen a téren. Rendkívül kevés eljárás folyik, és ezek 1-2%-ában kerül csak sor vádemelésre éppen a nehézkes bizonyításnak köszönhetően.

Ráadásul – ha mindez nem okozott volna már önmagában is épp elég nehézséget számunkra – most utalnék vissza a kezdetekhez, miszerint ezek a fiatalok nem ismerik egymást. Sosem találkoztak. Ennek az oka triviálisan egyszerű. Igen messze laknak egymástól más megyében más országban vagy akár másik földrészen. Sok-sok jogrendszeren átívelve, sok-sok bűnüldözői szervet kijátszva, vagy inkább mindenki csak a sajátját. Míg a nyomozóhatóság az egyik vagy másik országban nem is tud egyik tag cselekményéről, addig más helyen már figyelik, csak épp nem tudják bizonyítani, a harmadik helyen meg lehet, hogy mindez nem is üldözendő. És hogy mi kell mindehhez? A korlátlan, szabad, mindenki számára elérhető internet hálózat, na meg persze egy minimális angol nyelvtudás.

A realitás – Fastlink hadművelet[341]

Mindannak bizonyításául, hogy a fentebb vázolt történet nem csupán egy egyszerű utópikus kitaláció, szeretném röviden ismertetni a 2004. április 21-22-én Fastlink hadművelet néven elhíresült akciót. Az Amerikai Egyesült Államok Igazságügyi Minisztériuma levélben kereste meg az akkori Szervezett Bűnözés Elleni Igazgatóságot – mai nevén Nemzeti Nyomozó Iroda -, melyben tájékoztatták őket, hogy egy „FAIRLIGHT" nevű internetes „warez" csoport után nyomoznak, aki a leggyorsabban és a legsikeresebben a szerzői jogi védelem alatt álló szoftverek, DVD-K, mp3-ak biztonsági rendszerének feltörésében és illegális terjesztésében világszerte, többek között Magyarországon is. A nyomozás 9 hónapig tartott, melynek során fedett nyomozó alkalmazására is sor került. A nyomozás során beszerzett információk alapján a 11 részt vevő ország /USA, Belgium, Dánia, Franciaország, Németország, Magyarország, Izrael, Hollandia, Szingapúr, Svédország, Egyesült Királyság/ helyi idejének megfelelő egyeztetett időben kezdődtek a különböző nyomozati cselekmények, jellemzően házkutatások végrehajtása. Az érintett országokon belül minden esetben több helyszín volt meghatározva, az USA-ban 27 állam, míg Magyarországon 4 helyszín. Az érintett helyszíneket, személyeket és a keresett számítógépek ip címét /minden gép interneten észlelhető, egyedi megjelölésére használt szám/ az FBI munkatársai határozták meg, akik külön kérték, hogy az akció előtt semmilyen nyílt eljárást ne folytasson le a nyomozóhatóság. Az akció teljes időtartama alatt minden helyszínen végig jelen volt egy-egy FBI-os kolléga, aki a további helyszínekkel tartotta a kapcsolatot, illetve szakmai tanácsot adott.

A házkutatás eredményeként sikerült az FBI által keresett két személyt beazonosítani, akiket korábban csak nick névről ismertek, és kihallgatni, egy kivételével minden keresett számítógépet lefoglalni, továbbá számos, a keresett személyek lakásán megtalált winchestert és számítógépes adathordozót lefoglalni, melyek valószínűsíthetően szintén illegális tartalmakat hordoztak. Ez a teljesítmény annál is inkább figyelemreméltó, mivel az egyik helyszínen akadályozták a bejutást a kérdéses terembe, míg a másik

[341] 78/2004. bű.

helyszínen – az internetes információáramlás gyorsaságának köszönhetően – pár óra alatt elvitték az érintett gépeket egy magánlakásba, ahol aztán másnap hajnalban 04.30-kor sikerült megtalálni és lefoglalni.

Ezt követően az FBI jogi attaséja 2 oldalas köszönőlevélben méltatta a kollégák kitartását és erőfeszítését, idézem: *„A munkatársai által tanúsított erőfeszítés rendkívüli volt…A helyettesem, aki részt vett ezen nyomozó csoport munkájában, teljesen le volt nyűgözve munkatársai munkája és erőfeszítése által…Az irodám megtisztelve érzi magát azon lehetőségtől, hogy olyan közel dolgozhattunk munkatársaihoz, és olyan magas szintű támogatást nyújtott számunkra az Igazgatóságuk."*

A hadművelet minden érintett országra kiterjedő mérlege is igen impozáns volt, mindösszesen 120 házkutatást tartottak, 100 személyt azonosítottak be, és hallgattak ki, 200 számítógépet foglaltak le, a lefoglalt illegális tartalom értéke még óvatos becslések szerint is eléri az 50 M dollárt.

Bár az eredmény kárpótol mindenért, azért szeretném felhívni a figyelmet pár apróságra. Kezdetnek arra a 9 hónapra, amit a nyomozásra szántak, aztán a széleskörű, több országra kiterjedő koordinációra, amely igen komoly humánerő bevetését igényelte, továbbá a célországok helyszínein rendelkezésre álló, mind az angol szaknyelvet, mind pedig az informatikát kiválóan ismerő munkatársak bevethetőségére. Mert – ezt sajnos tudomásul kell venni – az ilyen típusú /informatikai/ bűncselekmények ellen kizárólag informatikai beállítottságú, informatikai szaktudással rendelkező kollégák vehetik fel eredményesen a harcot. Az egyéb szakterületen jeleskedő, hibátlan felderítési mutatókkal rendelkező kollégák sajnos sok esetben még egy eredményes házkutatást sem tudnak foganatosítani, a tanúkihallgatás során meg végképp elvesztek, hiszen az eljárás alá vont személy által kimondott szavakat sem értik, vagy félreértelmezik.

A fordulópont

Hazánkba viszonylag későn, 2001-ben érkezett meg a számítástechnikai bűncselekmények üldözésére való hajlandóság, mégpedig az Európa Tanács számítástechnikai bűnözésről szóló egyezményének képében, amelyet 2001. november 23-án, Budapesten nyitottak meg aláírásra, és végül 2004-ben lépett hatályba. Az egyezmény az Európa Tanács történetében az első budapesti egyezmény, egyben a számítástechnikai bűnözés elleni fellépés tárgykörében született első nemzetközi szerződés. A tárgykör fontosságát híven tükrözi, hogy már az aláírásra történt megnyitáskor kiemelkedően magas számú résztvevő, 30 ország, írta alá.[342] A három részből álló egyezmény a részletes büntető anyagi jogi tényállások mellett eljárásjogi rendelkezéseket is tartalmaz, és átfogóan szabályozza a nemzetközi együttműködés jogintézményét is.

Az egyezmény előkészítésével párhuzamosan Magyarországon is megkezdődött a büntető és eljárásjogi normák terén szükséges módosítások kidolgozása. A büntető törvényt módosító 2001. évi CXXI. törvény iktatta be a Btk.-ba az egyezmény rendelkezéseivel összhangban álló új szabályokat, tényállásokat. 2002. április 1-jétől így nálunk is büntetendő a számítástechnikai rendszerbe való jogosulatlan belépés, a számítástechnikai rendszer működésének megakadályozása, vírusok készítése, titkos belépési kódok jogosulatlan előállítása, megszerzése. A büntetőeljárási jog területén a büntetőeljárásról szóló 1998. évi XIX. törvényt átfogóan módosító 2002. évi I. törvény vezetett be az

[342] Dr. Hankó Faragó Miklós OGY 32. ülésnap 196. felszólalás

egyezmény rendelkezéseinek megfelelő szabályokat. Az aláíró államok közül hazánk az elsők között teremtette meg a teljes összhangot a belső jogi szabályozás és az egyezmény rendelkezései között.[343]

A nemzetközi együttműködés kapcsán bevezetett egyik legjelentősebb intézkedés a 24/7 hálózat életre hívása, ami tulajdonképpen egy éjjel-nappal a hét minden napján működő kapcsolattartási pont annak érdekében, hogy lehetővé tegye a számítástechnikai adatokkal és rendszerrel összefüggő bűncselekményre vonatkozó nyomozásokkal, vagy a bűncselekményekre vonatkozó elektronikus bizonyítékok összegyűjtésével kapcsolatos azonnali segítségnyújtást. Így különösen a technikai tanácsok átadását, az adatok megőrzését, bizonyítékok összegyűjtését, jogi jellegű információk átadását és a gyanúsítottak tartózkodási helyének meghatározását.[344] Az egyezmény meghatározza azt is, hogy ha a kapcsolattartási pont független a félnek a nemzetközi jogsegélyért vagy kiadatásért felelős hatóságától, vagy hatóságaitól, akkor képes kell, hogy legyen arra, hogy késedelem nélkül működjön együtt ezekkel a hatóságokkal.[345] Ez a mi esetünkben tökéletesen megvalósul, hiszen hazánkban az ORFK Bűnügyi Főigazgatóság Nemzetközi Bűnügyi Együttműködési Központ látja el ezt a feladatot az i-24/7 Interpol telekommunikációs hálózattal, melynek 186 tagállam részese és éves szinten 60 000 megkeresés érkezik ezen keresztül, amiből mintegy 1000 ügy keletkezik. Ennek ismeretében, továbbá annak tudatában, hogy – mint már korábban taglaltam – milyen szintű speciális ismeret szükséges egy-egy ilyen intézkedés eredményes végrehajtására, kicsit szkeptikus vagyok, vajon milyen színvonalon vagyunk képesek eleget tenni az egyezmény 35. cikk 3. pontjában kikötött megfelelően képzett és felszerelt személyzet követelményének.

Alighanem ez szúrt szemet az Európai Bizottságnak is, amikor 2007. május 22-én közleményt intézett az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának[346], a helyzet értékelése és megoldása végett. A közlemény először is definiálja a számítógépes bűnözés három kategóriáját – csalás, sikkasztás elektronikus hálózaton keresztül, illegális tartalom elektronikus médián keresztül történő közzététele, elektronikus hálózatokkal kapcsolatos bűncselekmények – majd megállapítja, kimondja, a köztudatba ülteti át az tényt, ami ebben a bűncselekménytípusban a legnagyobb probléma számunkra, vagyis, hogy *a cselekmények közös jellemzője, hogy az elkövetés terjedelme, a bűncselekmény és hatásai közötti földrajzi távolság jelentős.* Általános tendenciaként írja le, hogy a számítógépes bűncselekmények száma növekszik, és a bűnözés egyre kifinomultabbá és nemzetközibbé válik, egyértelmű jelek utalnak arra, hogy a számítógépes bűnözésben egyre inkább részt vesznek a szervezett bűnözői csoportok, ennek dacára a határokon átnyúló bűnüldözési együttműködés alapján folytatott európai büntetőeljárások száma nem növekszik. Problémát jelent az információk, szakismeretek és bevált gyakorlatok köz- és a magánszektor közötti cseréjének egyértelmű hiánya. A magánszektor szereplői az üzleti modellek és titkok védelme érdekében gyakran csak nehezen működnek együtt, illetve nem terheli őket egyértelmű jogi kötelezettség arra vonatkozóan, hogy a bűncselekmények miatt feljelentést tegyenek, vagy az azokra vonatkozó információkat megosszák a bűnüldöző hatóságokkal. Ilyen információkra azonban szükség lehet ahhoz, hogy a hatóságok hatékony és megfelelő bűnmegelőzési politikát dolgozhassanak ki. A közlemény konklúziója nem állt meg a

[343] Dr. Hankó Faragó Miklós OGY 32. ülésnap 196. felszólalás
[344] Számítástechnikai bűnözésről szóló egyezmény 35. cikk 1.
[345] Számítástechnikai bűnözésről szóló egyezmény 35. cikk 2. b.
[346] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:HU:HTML

problémafelvetés elméleti szintjén, és a Bizottság találkozót szervez a tagállamok, valamint az Europol, a CEPOL és az EJTN bűnüldözéssel foglalkozó szakértői számára annak megvitatása érdekében, hogy miként lehetne javítani a stratégiai és operatív együttműködést, valamint a számítógépes bűnözéssel kapcsolatos képzést. A 2007-es találkozó lesz a közeljövőben tervezett üléssorozat első ilyen találkozója.

Helyzetkép

Ezek után szeretném felvázolni pusztán érintőlegesen, hogy miként kezelik ezt a problémakört határon innen és túl, hogy valami reális helyzetképünk legyen a jelenlegi gyakorlati viszonyokról, és ezzel összefüggésben a várható eredményekről.

Franciaországban belső pályázókból választják ki az informatikai szakterülettel foglalkozó kollégákat, akik ezt követően 4 hetes képzésen vesznek részt. Ha már kiképzett és bevethető rendőrnek számít, akkor kap egy fém-koffernyi technikát és leküldik vidékre, egyedül, hogy egy komplett adatmentést megcsináljon, anélkül természetesen, hogy az adatállomány sérülne, vagy elveszne. Amennyiben úgy értékeli a helyszínen lévő kolléga, hogy itt valami komolyabb felszereltség kellene, nagyobb volumenű dologba ütközött, akkor betelefonál a központba, ahonnan egy komplett informatikai kisbuszt és további szakembereket küldenek a segítségére. Mindezt a feladatkört a rendőrök és a csendőrök együttvéve 700 fővel felügyelik, és ez nem egy végleges létszám, a tervek szerint rövid időn belül a duplájára emelik. Nem meglepő, hogy ebből a létszámból jut nekik egy csoportra (3-4 fő) akik csak és kizárólag újdonságfigyeléssel foglalkoznak, vagyis új technikai eljárások, szoftverek után kutatnak, amiből egy ingyenes példányt a gyártó cég rendelkezésükre is bocsát, hogy lássák a hibáit, vagy ezzel segítsék elő a munkájukat.

Portugáliában a humánerőt a végzős informatikusokból szerzik be, egyfelől így megspórolják a képzési költséget, másfelől valószínűsíthető, hogy olyan munkaerőt kapnak, aki már találkozott a másik oldallal, esetleg személyes ismerősei is vannak, tisztában van az uralkodó trendekkel. Ebben látom én a módszer hátrányát is, hiszen ilyen esetben nagy kérdés az, hogy az ilyen formán nyert kolléga valójában melyik oldalon is áll.

A Román államigazgatás úgy oldotta meg ennek a speciális szakterületnek a sajátos igényeit, hogy egy épületben helyezte el a területtel foglalkozó rendőröket, ügyészeket és bírákat egyaránt, így a közvetlen napi kapcsolat, továbbá az egy típusú ügyek lehetővé teszik a terminus technikusok készség szintű elsajátítását és az esetleges szaknyelvből adódó, vagy technikai félreértések azonnali tisztázását.

A hazai állapotok ehhez képest elég nyomasztóak. Egyik oldalról érintett az ORFK Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztálya, ahol a rendszeresített állomány 10 fő, ebből 3 fő az informatikai ismeretekkel rendelkező kolléga, és 6 fő a nyomozati tevékenységet végző. Fő profiljuk az informatikai rendszerek elleni támadás kivizsgálása, a tiltott pornográf felvétel terjesztésének kivizsgálása és az interneten elkövetett csalások felderítése. Általánosságban is elmondható, hogy az országos hatáskörű szervezethez képest rendkívül csekély létszámú állomány kifejezetten gyenge műszaki felszereléssel dolgozik mind hardver, mind pedig szoftver téren egyaránt.

A másik alternatíva a BRFK Gazdaságvédelmi Főosztályon a Csúcstechnológia Elleni Bűncselekmények Alosztálya. Ez egy 11 rendszeresített létszámmal idén alakult szervezeti egység, ahol meggyőző – általános – szaktudással rendelkező nyomozók-vizsgálók dolgoznak, fő profiljuk a szerzői és szomszédos jogok védelme. Komoly probléma az egységnél, az informatikai szaktudás hiánya, illetve a sajnálatos – profiljukból

adódó – tény, miszerint a szerzői és jogvédő társulások egyszerűen oly mértékben telepedtek rá a nyomozóhatóságra, hogy önmaguk akadályozzák a munkát a dömpingszerű, minden előzetes kontrollt nélkülöző feljelentésekkel, amire nyilvánvalóan reagálni kell, el kell járni, ugyanakkor épp az ügyek mennyisége megy a minőség rovására, hiszen egyszerűen felőrli az állományt.

Ha már a problémáknál tartunk, minden képen meg kell említeni a területen működő szakértők tevékenységét is. Sajnos több esetben előfordult, hogy személyük nemhogy segítette volna, de egyenesen hátráltatta a nyomozást, és a bizonyítékgyűjtést. A határidőket finoman szólva is rugalmasan kezelik, és mivel a nyomozóhatóságnak konkrét kérdéseket kell feltenniük, amire várják a választ, a szakértők is kizárólag erre fognak válaszolni és nem tárják a nyomozóhatóság elé az adathordozón talált esetleges – a kérdéstől eltérő – tartalmakat, amik elősegítenék a nyomozás előrehaladását. Nem feltétlenül rossz szándékból, sok esetben egyszerűen azért, mert nem értenek hozzá, nem gondolják, hogy fontos lehet. Ugyanakkor csillagászati összegekért dolgoznak. Megfigyelhető sajnos, hogy konkrét bűnügyben eseti szakértőként került kirendelésre olyan személy akinek, noha a szükséges szaktudással rendelkezik, üzleti érdeke fűződött hozzá, hogy a konkurenciát ellehetetlenítse. Vagy egy másik példa, amikor a szakértőt szoros szálak fűzik az ASVA szervezetéhez, ugyanakkor, mint kirendelt szakértő jár el egy konkrét ügyben. Ez is jól illusztrálja a rendőrség kiszolgáltatott helyzetét a szaktudás tekintetében. Hiszen mennyivel egyszerűbb, olcsóbb, na és nem utolsó sorban hatásosabb megoldást jelentene, ha a rendőrség rendelkezne olyan informatikai szaktudással bíró humán erőforrással, ami elsődlegesen – a vádig – tudja vizsgálni az adathordozót, hogy egyáltalán van e bizonyítéka az ügynek, vagy csak a fikció. Amennyiben bírói szakba kerül az ügy akkor a védelemnek természetesen alapvető joga kérni független szakértő kirendelését. De az már nem a bűnügyi – és rendőrségi – költségeket srófolja az egekig. Maga a műszak technológia nem újdonság, ismert hazánkban is, és Európa számos országában elismert a bíróság előtt is.

Jövőkép

Ez után a kissé szomorkás helyzetkép után próbáljunk óvatos optimizmussal a jövőbe tekinteni. Nézzük, mintegy vitaindító szándékkal, mi szükséges ahhoz, hogy ebből a gödörből kimásszunk.

Az első és legfontosabb a saját szakember-szakértő gárda kinevelése, ki- és továbbképzése. Ez évek óta egyáltalán nincs jelen a magyar rendőrségen. Szükség lenne rendszeres alapozó és – típustól függő – továbbképzésre. Igen, különböző – a Bizottság által használt – típusokra kellene bontani az ezen a területen dolgozó kollégákat. Ennek alapvető követelménye, hogy a jelenlegi húszfős országos létszámot legalább háromszorosára emeljük. Szorosabb, napi kapcsolat kiépítése a különböző – területi, helyi – szerveknél dolgozó kollégák között, hogy az egész országban egységesen eljárás alakuljon ki. Kiemelt fontosságúnak tartom, hogy a helyszínen intézkedő kollégák minden esetben nyomon tudják követni az általuk érintett ügy folyamatát a vádemelésen át az ítélethozatalig, hogy ezen a rendkívül fiatal területen egyáltalán beigazolódjon, hogy mi az a bizonyíték, vagy bizonyítási eljárás, ami megáll a Bíróság előtt, vagy mire kell nagyobb hangsúlyt fektetni a következő alkalommal. Készíteni kellene egy országos szakértői listát, amihez minden – a területen dolgozó kolléga – csatolja a saját tapasztalatait, az együttműködés eredményét. Ezzel kiküszöbölhető a szélhámos, nyerészkedő, ellentétes érdeket képviselő alakok.

Figyelembe kellene venni még az eljárás alá vont cégek üzleti titokhoz fűződő jogait és érdekeit, és nem beengedni a színfalak mögé a szakértői ruhába bújtatott konkurens cégvezetőt. Végül az sem biztos, hogy szerencsés megoldás, ha az eljárás ideje alatt a gyanúsítottat kérjük fel, hogy tartson továbbképzést a szervezeti egység számára.

Ha kinőttük saját gyermekbetegségeinket, és már tudunk egységesen, egyforma eljárással az informatikai társadalom bűnözői rétege ellen harcolni, akkor majd talán megérik az idő felvenni a kapcsolatot a külföldi társszervek vezetőivel, majd a végrehajtó állománnyal is, hogy ne legyen problémás, késedelmes a határon átnyúló szerverek, és csoportok felkutatása.

Még egy – egyelőre igencsak utópikus – megoldási javaslat. A NATO 2008. május 14-én írta alá azt a megállapodást, amelynek értelmében az interneten és a számítógépeken tárolt vagy cserélt adatok védelmére hoz létre egy központot Tallinban. Egyelőre hét ország (Észtország, Lettország, Litvánia, Olaszország, Spanyolország, Németország, Szlovákia) nyújt szakembereket és anyagi hozzájárulást a projekt megvalósításához, melynek első számú feladata, hogy megelőzze a számítógépek és a hálózatok elleni internetes behatolási kísérleteket, támadásokat, illetve fellépjen az ilyenek elkövetői ellen. Az egyelőre 30 fővel dolgozó központ a nyáron kezdi meg tevékenységét, a hivatalos avatást azonban csak jövőre tervezik.[347] Ha már ott van egy helyen 7 ország szakember gárdája, csúcstechnikával felszerelve, akkor esetleg nem lehetne még delegálni hozzájuk más országokból is a nyomozóhatóság tagjai közül 3-4 főt, akikhez minden nap megérkeznének a saját országukból a számítástechnikai bűncselekményekhez valamilyen szinten kapcsolható személyek, bűncselekmények adatai, főbb paraméterei, és így számukra valószínűleg – kirajzolódna, mivel több ország jelentését látnák egy asztalon – több típusú bűnelkövetési csoport tevékenysége és földrajzi elhelyezkedése. Amit így egységében látva sokkal egyszerűbb lenne megérteni és felszámolni egyaránt.

De, hagyjuk az utópiát és kezdjük kicsiben, nézzünk szét saját területünkön keressünk informatikai vénával megáldott kollégákat, és merjük „emberszámba" venni őket, elismervén szaktudásukat, és ajánljuk fel munkájukat a társszervek számára, akik bizony nem jutnak tovább nélkülük. Mert, a szerzői jog kérdése csupán egy gumicsont, játék ahhoz képest, ha mondjuk, végiggondoljuk, hogy ugyan ilyen módszerekkel kellene harcolni a tiltott pornográf felvételek kapcsán, ahol gyermekek élete és jövője a tét. Vagy a klasszikus adathalászat, a személyiséglopás ellen, amikor egyik óráról a másikra forgathatnak ki bennünket mindenünkből és nem létező személyekké válunk a szó szoros értelmében, nem is beszélve a központi rendszerek ellen intézett támadásokkal okozott milliárdos károkról. Ezek többségében megelőzhetőek, vagy legalábbis kezelhetőek és figyelemmel követhetőek lehetnének, ha…

[347] http://www.sg.hu/cikkek/60094 (Letöltés ideje: 2008.05.15.)