MÁTÉ ISTVÁN ZSOLT

A DIGITÁLIS BŰNFELDERÍTÉS GYAKORLATA, AVAGY AZ IGAZSÁGÜGYI INFORMATIKAI SZAKÉRTŐ A BÜNTETŐELJÁRÁSBAN

1. Az informatika, a kommunikáció- és a jogtudomány interdiszciplináris tere

A tudományágak és tudományterületek a kezdetektől a közelmúltig bezárólag a szétválás és osztályokra tagolódás útját járta: tudományágak, részdiszciplínák, aldiszciplínák jöttek létre. Az utóbbi száz esztendőben a tudományterületek közötti átfedések, egybemosódások tapasztalhatók, melynek legérzékletesebb bizonyítéka az, hogy a legjelentősebb tudományos eredmények a „tudományok, tudományágak spontán vagy tudatosan szervezett együttműködéséből születnek."[592] Ez a megközelítés arra hívja fel a figyelmet, hogy a tudományágakat és területeket nem egymástól élesen elhatárolt közegekként (akár a vízen úszó olaj), hanem inkább egymásban többé-kevésbé oldott, egymást átjáró matériaként tekinthetjük. Nincs ez másként abban a dimenzióban sem, ahol a fiatal és dinamikusan fejlődő informatika, a konzervatív jogtudomány és a közelmúltban önállósodott kommunikáció tudomány találkozik. Jelen írás e találkozási térnek egy kis darabkáját vizsgálja: nevezetesen a büntetőeljárásban működő igazságügyi informatikai szakértő munkáját és annak beágyazottságát az informatika, a kommunikáció- és a jogtudomány interdiszciplináris terébe.

2. Az igazságügyi informatikai szakértő feladatai

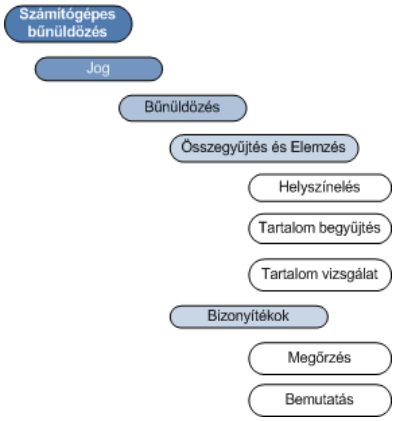
2.1. A számítógépes bűnözés

A számítógépes bűnözés csaknem egyidős jelen sorok szerzőjével. Az egyik kronológia szerint 1966-ban Mineapolisban történt az első feljegyzett eset, melynek során egy számítógépes programot használtak fel egy gazdasági bűncselekményhez. Hét évvel később, 1973-ban már 2 milliárd USD kárt okoztak a számítógépet elkövetési eszközként felhasználó bűnözők.[593] Az eltelt csaknem fél évszázad alatt még az informatikai területen vezető szerepet betöltő észak-amerikai térség szereplői sem válaszoltak meg minden alapvető kérdést a digital forensic science, vagy magyarul a bűnügyi informatika tudományterületén.

Számos osztályozási mód próbálja feltérképezni és azonosítani a bűnügyi informatika ható- és hatáskörét. Az észak-amerikai szakirodalomban a law enforcement officer-ként (bűnüldözési tisztviselők) említett szakértők helye bizonyítékok összegyűjtése

[592] Nagy József: Hierarchikus multidiszciplinák? Magyar Tudomány 1999/2. sz. Forrás: http://epa.oszk.hu/00700/00775/00002/1999_02_ 16.html (letöltés ideje: 2013.06.25.)
[593] Thomas A. Johnson (szerk.): Forensic Computer Crime Investigation. CRC Press.Boca Raton. USA 2005. 26. o.

elemzése, valamint azok megőrzése és bemutatása területén azonosítható,[594] amint azt a következő ábrán.



1. sz. ábra: szakértő helye az észak-amerikai Cyber Crime osztályozásban (Brinson és társai nyomán)

Ez a megközelítés a helyszíni és laboratóriumi vizsgálatok elkülönítésére, elkülönülésére utal, mely megfelelő létszámú szakértő, vagy bűnüldözési szaktisztviselő rendelkezésre állása esetén megvalósítható. A magyarországi helyzet ugyanakkor jelentősen eltér az észak-atlanti példától. Ezt a különbséget legmarkánsabban a jogszabályi környezetből olvashatjuk ki, mely híven tükrözi az eltérő jogrendszerből (common law, case law versus civil law) is adódó hangsúly és nézőpont különbségeket.

2.2. Az igazságügyi szakértő Magyarországon

Magyarországon – a büntetőeljárásban – a szakértő szerepét a büntetőeljárásról szóló 1998. évi XIX. törvény 99.§ (1) tisztázza: „*Ha a bizonyítandó tény megállapításához vagy megítéléséhez különleges szakértelem szükséges, szakértőt kell alkalmazni*". Ezt az igazságügyi szakértői tevékenységről szóló 2005. évi XLVII. törvény 1.§ (1) teszi kézzelfoghatóvá: „*…a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel segítse a tényállás megállapítását, a szakkérdés eldöntését*". Az igazságügyi informatikai szakértői szakterületeket a 9/2006. (II.27) IM rendelet 6. számú melléklete határozza meg:

1. informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver)
2. informatikai biztonság
3. informatikai rendszerek tervezése, szervezése
4. stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység
5. számítástechnikai adatbázis, adatstruktúrák
6. szoftverek

A szakterületen jelenleg dolgozó mintegy százötven szakértő e keretek (jogtudományi dimenzió) között vizsgálja a különféle eszközöket és adatokat (informatikai

[594] Ashley Brinson – Abigail Robinson – Marcus Rogers: A cyber forensics ontology: Creating a new approach to studying cyber forensics. in digital investigation 3S (2006), Elsevier B.V. Amsterdam, 2006. 37. o.

dimenzió), majd interpretálja (kommunikáció-tudományi dimenzió) megállapításait. A büntetőeljárás, mint ennek az interdiszciplináris térnek a kerete, vagy határa akkor lehet sikeres – az egyes tudományterületek adott pillanatban elfogadott, magas szintű és szakszerű alkalmazását értve ezen – ha mindhárom kiemelt komponens kellő mértékben érvényesül, illetve más megközelítésből a komponensek közötti diszharmónia megszűnik. Mivel a magas szintű és szakszerű alkalmazást meglehetősen nehéz definiálni, a továbbiakban a három diszciplína közötti zavar kiküszöbölésének egyik módját tárgyalom.

2.3. Az igazságügyi informatikai szakértő kommunikációja a büntetőeljárásban

Álláspontom szerint a büntetőeljárásban – a tárgyalt területen – megjelenő legjelentősebb problémája az a kommunikációs konfliktus, zavar mely az eljárás egyes szereplőit (szakértő, nyomozó, ügyész, ügyvéd, bíró) akadályozza a saját szakterületükön a korábban tárgyalt magas szintű és szakszerű alkalmazásban. Ahogy azt Shannon a Kommunikáció matematikai elmélete című írásában (később Shannon-Weaver modell) megfogalmazta a hatékony és gyors információ átvitel fontos összetevője az átviteli csatorna és az alkalmazott információ kódolás595.

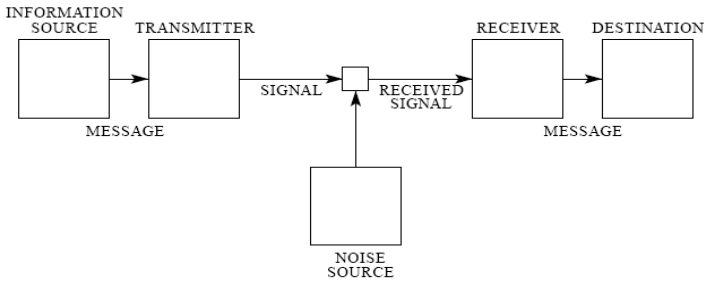


Fig. 1 — Schematic diagram of a general communication system.

2. ábra - Információátvitel (Shannon, 1949)

A tárgyalt területre alkalmazva a modellt a nyomozó, a nyomozást felügyelő és az ítélkezésben résztvevő szereplők jogi-társadalomtudományi beszédmódjának (kódolásának) és a szakértő műszaki – informatikai - természettudományos alapú beszédmódjának (kódolásának) konfliktusára figyelhetünk fel. Ez a konfliktus abból a felismerésből eredeztethető, melyre a számítógépes bűnözés szülőhazájában (USA) jöttek rá a bűnüldöző szervek: a specializálódott bűnözés felderítéséhez, szakértőkre, specialistákra van szükség, mert az élet más területein bevált kriminalisztikai módszerek itt jórészt hatástalanok. A számítógépes bűncselekmények felderítésében alkalmazott szakértők saját nyelvüket (kódrendszerüket) használván nem alakult ki (gyakorlati tapasztalataim alapján, Magyarországon semmiképpen) olyan közvetítő nyelv, kommunikációs csatorna, mely a büntetőeljárás szereplői részére lehetővé tenné egymás pontos megértését. Ez a tény annak tükrében leginkább sajnálatos, hogy a XXI. század második évtizedében a mindennapi életet már jelentős mértékben áthatja az informatika, a számítástechnika alkalmazása.

595 Shannon, C. E.: A Mathematical Theory of Communication in The Bell System Technical Journal. Vol. 27. 379-423. o. és 623-656. o. July. October. Bell Laboratories. Berkeley Heights. New Jersey. USA. 1948. 2. o.

A jelzett problémának az nyomozati munka hatékonyságának alacsony szintje (elektronikus bizonyítékok kezelése, értelmezése) mellett az ítélkezés pontossága (bizonyítékok súlyának fel nem ismerése) és gazdasági szempontok (növekvő bűnügyi költségek a többszörös szakértő kirendelés által) is felmerülhetnek, mint következmény. Nem nehéz elképzelni a felsoroltak következményeit, ugyanúgy, mint ahogy megoldás is viszonylag egyszerű.

3. Képzési megoldások a kommunikáció hatékonyabbá tételére

A kommunikációs zavar feloldásának módja magából a Shannon-Weaver modellből adódóik: ha a küldő kódolását (beszédmódját, szóhasználatát és jelentéstartalmait stb.) nem ismeri a vevő, akkor azt meg kell tanítani erre, a szükséges mértékben. Erre a felismerésre elsőként az IRS (Internal Revenue Service – Adóhivatal) vezetősége ébredt rá az Amerikai Egyesült Államokban, amikor Michael Anderson és Robert Kelso vezetésével létrehozták a az első számítógépes bűnözés felderítésével és a bűnüldözési szakemberek képzésével foglalkozó részleget. E tevékenység kibontakozására ugyanakkor csupán a kilencvenes évek második felében került sor és a későbbiekben is olyan fenyegetések révén erősödött, mint a 2000-ben mintegy 10 milliárd dollár kárt okozó „I love you" vírus, vagy a new york-i Citibank ellen elkövetett támadás.[596]

Magyarországon az előzőekhez hasonló jelentőségű események nem kerültek nyilvánosságra, ugyanakkor azok a kezdeményezések, melyek a nyomozó hatóságok munkatársainak informatikai alapú képzésére vonatkoztak sem váltak zsinórmértékké. A következőkben egy példát mutatok be a kommunikációs zavar hatékony közömbösítésére.

3.1 A digitális bűnfelderítés gyakorlata

2008-ban járunk, amikor jelen sorok szerzőjének kezdeményezésére a Baranya Megyei Rendőr-főkapitányság és a Pécsi Regionális Képző Központ az Európai Uniós forrásokból megvalósult HEFOP 5.3.1 – „Korszerű felnőttképzési módszerek kidolgozása és alkalmazása" projekt keretében képzési együttműködést kötött egymással. Az együttműködés lénye az volt, hogy a Képző Központ munkatársai képzési programokat dolgoznak ki a számítógépes bűncselekmények felderítésének támogatására, illetve az állomány általános informatikai ismereteinek fejlesztése céljából a következő témakörökben:

- Digitális bűnfelderítés gyakorlata.
- Small Office Home Office üzemeltetés.
- Számítógép üzembe helyezés és üzemeltetés.
- Operációs rendszerek használata.

Amint az a programok elnevezéséből is kitűnik, egy képzési program készült közvetlenül a nyomozati munka támogatására, a további három pedig az általános informatikai készségek és képességét célozta fejleszteni különböző aspektusokból. A Digitális bűnfelderítés gyakorlata programban a következő tématerületeken fejlesztették a résztvevők ismereteit és készségeit a Képző Központ instruktorai:

Alapfogalmak

- Operációs rendszerek.

[596] Thomas A. Johnson:(szerk.): i.m. 29-30. o.

– Internet.
– Számítógép hálózatok (hardver/szoftver).
– Szakértői szoftverek és hardver eszközök.
Műveletek
– Fájlkezelés, fájlátvitel.
– Információmegtalálás (adatbányászat?).
– Szakértői vizsgálati módszerek.

A 60 tanórás kurzusok (25 % elmélet és 75% gyakorlat) során a résztvevő 70 fő részletesen megismerte azokat az rendszereket (operációs rendszerek, irodai alkalmazások) amelyeket a mindennapi munkájuk során is alkalmazniuk kell, betekintést nyertek a különféle számítástechnikai eszközök felhasználásával elkövetett cselekmények technikai-technológiai hátterébe:

– számítógépes hálózati forgalom figyelése helyi számítógép hálózaton (sniffing),
– spoofing (átverés): URL, file-sharing, e-mail, login,
– phishing (adathalászat),
– fájlcserélő hálózatok (server/client és peer-to-peer rendszerek),
– port scanning (behatolási pont felderítés),
– összehangolt támadások (DoS, DDoS).

A tematika összeállításában jelentős szerepet játszott az a tény, hogy jelen sorok írója részt vett az I. Nyíregyházi Igazságügyi Informatikai Szakértői Konferencián. A kollégáktól ott kapott inspiráció révén jött létre az képzés ötlete és szerveződött meg az a gyakorlatban is. A képzés zárásakor 70 fő vehette át a sikeres vizsgáról szóló tanúsítványt a Baranya Megyei Rendőr-főkapitányság és a hozzá tartozó kapitányságok munkatársai közül. A személyes visszajelzések igazolták azt a várakozást, mely feltételezte, hogy nem csak a munkában, hanem a privát életben is hasznosítani tudták a hallgatók a tanultakat. Az állomány mellett a vezetők is kedvezően értékelték a képzést, ugyanakkor a folytatás elmaradt. Az okok feltárására a későbbiekben térek ki.

3.2. Külföldi példák

Ahogy azt korábban vázoltam az észak-amerikai térségben már korábban felfigyeltek a nyomozó hatóságok az informatikai ismeretek hiányából adódó problémákra és speciális egységek felállításával kezelték a helyzetet. Amint az informatika egyre nagyobb teret hódított a mindennapokban szükségessé vált a speciális képzettség helyett vagy az mellett egy általános képzési programokra is, amelyek az informatikai írástudást alapozzák meg, vagy erősítik az állomány tagjai között. Ezek a programok a következő követelményeket fogalmazzák meg:[597]

1. Bűnügyi helyszínen fellelt, feltehetően bizonyítékokat tartalmazó számítógépek és más elektronikus eszközök azonosítása és kezelése.
2. Ellenőrizhető digitális lenyomat fájlok (image) készítése az adatok további vizsgálatához.

[597] H. Armstrong – P. Russo: Electronic Forensics Education Needs of Law Enforcement. CISSE, West Point. USA 2004. 94. o.

3. Bizonyítékok kinyerése a számítógéprendszerekből és egyéb elektronikus eszközökről.
4. Az elektronikus bizonyítékok elemzése és jelentés készítése az eredményekről.
5. A bizonyítékok bemutatása a bíróság előtt.

A felsorolt képességek és készségek gyakorlati alkalmazására Nelson, Phillips, Enfinger és Steuart tett javaslatot, ahol is három kategóriába sorolták az alkalmazói szinteket az alábbiak szerint:

1. szint: a digitális bizonyíték megszerzése és lefoglalása, ez rendszerint a rendőr járőr (street police officer) feladata
2. szint: high-tech vizsgálatok irányítása, a számítógépes szakkifejezések ismerete, mit lehet és mit nem lehet kinyerni a digitális bizonyítékokból, ez rendszerint a nyomozók (detective) feladat
3. szint: digitális bizonyítékok kinyerése, adat helyreállítás, számítógépes hálózati bűnfelderítés, internetes csalások vizsgálata[598]

Amint látható a felsorolásból a law enforcement officer feladatköre legalább részben egyesíti a magyarországi rendszerben szereplő nyomozó és igazságügyi informatikai szakértő feladatkörét. A bűnügyi informatikai ismeretek és készségek három szintű elkülönítése a nyomozati munkában betöltött szerephez is igazodik. A magyarországi rendszerben a felsorolt készségekhez és képességekhez hasonló kompetenciákkal a kriminalisztikai területen dolgozó bűnügyi technikusok rendelkeznek. Nem véletlen, hogy felvetődött a bűnügyi technikusok szakterületének részbeni kiterjesztése iránti igény is: „*…megfontolandó a nyomozó hatóság állományában informatikai szaktudással rendelkező bűnügyi technikusok (computer forensic) alkalmazása, akik az egyszerű megítélésű ügyekben az egyes adathordozók, szoftverek vizsgálatára, segédprogramok felkutatására, és vizsgálatuk leírására megbízhatóan képesek.*”[599] A felvetés kétségtelen előnyökkel rendelkezik: a nyomozati munka gördülékenységét, gyorsítását és költségeinek csökkentését várhatjuk tőle. Ugyanakkor fel kell ismerni azt is, hogy a digitális bizonyítékok nyomozó hatóság általi kinyerése és elemzése ellentmond annak a törvényalkotói szándéknak, mely megteremtette a nyomozóhatóságoktól független igazságügyi szakértő szerepkörét és a bizonyítékok elemzését és részben begyűjtését is az ő feladatául rendelte. Annak a megállapítása, hogy melyek az „egyszerű megítélésű ügyek” szintén számos buktató rejtőzhet, így a bűnügyi technikusok szakterületének kiterjesztése az informatikára valószínűleg még várat magára. A fentiekben vázolt irányvonal ugyanakkor azt mutatja, hogy az informatikai kihívásokra létezik naprakész, autentikus válasz külföldön is. E válasz egy pontját emelem ki részletesebb tanulmányozásra, mely által visszakanyarodok a magyarországi megoldási lehetőségekhez. Ez a részlet pedig nem más, mint az ausztráliai Curtin University és a Police Academy of Western Australia közös programjában[600] szereplő Cisco CCNA (Cisco Certified Network Associate) képzési modulok felhasználása.

[598] Bill Nelson – Amelia Phillips – Frank Enfinger & Chris Steuart: Computer Forensics and Investigations. Thomson Course Technology. Boston. MA. USA. 2004.
[599] Szathmáry Zoltán: Bűnözés az információs társadalomban. PhD értekezés, PTE ÁJK Doktori Iskolája Pécs, 2013. 184. o.
[600] H. Armstrong – P. Russo: i.m. 95. o.

3.3. Alternatív hazai lehetőségek

A Cisco Systems Inc. (nemzetközi számítógépes hálózati technológiai vállalat) az alapismereti képzéstől a mérnöki szintig terjedő informatikai e-learning képzési rendszerrel rendelkezik, melyet a világ több mint 180 országában (így hazánkban is) használnak. A Curtin University és a Police Academy of Western Australia közös képzési programjában a fejlett hálózati infrastruktúra és a hálózati biztonság témakörét a CCNA tananyagra alapozva oktatják a law enforcement officer munkatársaknak. Ez a középszintű elektronikus tananyag CCNA Dicovery változatában magyar nyelven is elérhető a Hálózati Tudás Terjesztéséért Programiroda Alapítvány felügyelete alatt több egyetem és középiskola révén. A közép szint mellett úgynevezett belépő szintű (például az IT Essentials) elektronikus tananyagok is rendelkezésre állnak. Ezek a tények akkor kapják meg értelmüket, amikor visszakanyarodva a Digitális bűnfelderítés gyakorlata képzéshez elemezni kezdjük a képzések folytatása elmaradásának okait, melyek közül az első két ok minden bizonnyal: a képzési költségei, és az állomány időbeosztása lehet. Az első esetben a pénzhiányt határozhatjuk meg hátráltató indokként, a második esetben a szolgálatvezénylés és a kontakt oktatás időzítési problémát okozhat. Az e-learning képzési rendszer (online tananyag és vizsga) lehetőséget nyújt a tanulási idő szolgálaton kívüli és/vagy kisebb leterheltségű időszakokra történő koncentrálására, illetve a rendszer a kontakt órák és tanterem bérlet költségeit is részben kiválthatja az online konzultációs lehetőségek és a tanulóközösségek által nyújtott további segítség által.

4. Összefoglalás

A számítógép alapú technológiák az élet egyre több területén jelennek meg. Ebből adódóan a bűnelkövetés és a bűnüldözés is egyre nagyobb számban találkozik a technológia kézzel fogható (hardver) és meg nem ragadható (szoftvereke és új viselkedési minták) jellemzőivel. Ezeket a komponenseket az elkövetők hol eszközként, hol pedig egyszerű mindennapi tárgyként használják, s ily módon a cselekmények digitális lenyomatait, digitális bizonyítékait (digital evidence) hagyják maguk után. Ezek a bizonyítékok gyakran nem láthatók, vagy hétköznapi eszközökkel nem hozzáférhetők. beszerzésükhöz, rögzítésükhöz, megőrzésükhöz és bemutatásukhoz megfelelő – a legtöbb esetben magas szintű – informatikai szakmai tudásra és gyakorlatra van szükség. Ez utóbbi képességekkel és készségekkel az igazságügyi informatikai szakértők rendelkeznek, aki a bizonyítékok feltárásával és később interpretálásával segítik a nyomozó hatóság, majd a bíróság munkáját. A szakértők munkájának hatékonysága nem csupán a szakismereteken múlik, hanem azon is, hogy milyen minőségű kommunikációs kapcsolatot hoznak létre a büntetőeljárás további szereplőivel nyomozókkal, ügyészekkel, bírákkal és ügyvédekkel. A nyomozati szakban a legfontosabb partner a nyomozó. A hatékony kommunikációhoz nélkülözhetetlen az azonos kommunikációs kód, leegyszerűsítve a szakmai köznyelv és a mögöttes fogalmi háttér. Ennek az összhangnak a megteremtésére a számítógépes bűnözés csaknem ötven évvel ezelőtti megjelenése óta van igény, és az utóbbi évtized óta külföldi és hazai gyakorlat is. A kommunikációs akadályok lebontásának egyik módja a bűnügyi munkatársak bűnügyi informatikai – digital forensic – képzésének megszervezése. Erre olyan költség és időtakarékos, ugyanakkor hatékony módszereket kell alkalmazni, mely lehetővé teszi az állomány folyamatos képzését a munka hátráltatása nélkül és egyben támogatja az informatikai szakértőkkel történő együttműködést is.