A számítógépes bűnözés
SZAKDOLGOZAT

Készítette: Mezey Nándor

Konzulens: Dr. Kőhalmi László

2007.

Tartalomjegyzék

Bevezetés

E dolgozat keretében megpróbálom bemutatni, a számítástechnika, mint a 20. század és napjaink egyik legdinamikusabban fejlődő területének, áldásai mellett az egyik legjelentősebb árnyoldalát, veszélyét is; a számítógépes bűnözést.

Nem hiszem, hogy sokat kellene bizonygatnom, hogy életünkre milyen komoly hatással volt, van az informatika és a számítástechnika fejlődése. Egyre inkább átszövik azt, főleg az Internet elterjedésével egyes társadalmi rétegek, illetve szakmák képviselői számára nélkülözhetetlen segítőtárssá vált. A számítástechnika és a számítógépek sokféle felhasználhatóságára a tudósok után (eleinte kizárólag tudomány célra használták a számítógépeket) a gazdasági élet tagjai is rádöbbentek, s egyre inkább elkezdték használni e technikai eszközt, mellyel többek közt gazdaságosabbá és gyorsabbá tehették tevékenységüket. Ezzel együtt a bűnelkövetők is felismerték a számítástechnikában rejlő lehetőségeket, elsősorban a számítógépek és a számítógépes hálózatok használatának előnyei miatt vált vonzóvá számukra e terület.

Egy-két évtizeddel ezelőtt a számítógépes bűnözés még közel sem jelentett akkora veszélyt, mint manapság, de mára kimondhatjuk társadalmi problémává nőtte ki magát. Az információs társadalom felé vezető úton pedig fokozottan igaz ezen állítás. Az információs forradalom negatív eredményeként a társadalmak egyre kiszolgáltatottabbak lettek az adatfeldolgozó rendszereknek. Napjainkban biztonságunk (gondoljunk a személyes adatokat tároló adatbázisokra), és értékeink (pl.: banki adatbázisok, melyek feltörésével könnyen hozzájuthatnak illetéktelenek vagyonunkhoz) egyre jobban függnek e rendszerek működésének zavartalanságától, s a számítógépes bűncselekmények – többek közt - pont e rendszerek működését támadják. Az előbb elmondottak miatt nélkülözhetetlen, hogy a társadalmak fellépjenek e típusú bűnözés ellen.

A jelenség ellen, mind technikai – pl.: egyre modernebb védelmi szoftverek, technikai berendezések által -, mind jogi eszközökkel fel kell lépni. Hangsúlyoznom kell, hogy a jogi fellépés nem lehet kizárólag büntetőjogi, mivel egyrészt a büntetőjog e problémára legfeljebb átmeneti megoldást adhat - persze ez nem azt jelenti, hogy nélkülözni kéne ezen eszközt. Másrészt a törvényhozónak körültekintőnek kell lennie, mikor meghatározza azon cselekmények körét, melyeket bűncselekménynek minősít, mivel a számítástechnika egyre nagyobb területeken hálóz be, ezért az átlag ember – esetleg tájékozatlansága, járatlansága miatt - sokszor akár akaratán kívül is elkövethet bűncselekményeket. Avagy tudja, hogy bűncselekményt követ el, de vagy nem tud ellenállni a csábításnak, vagy túl nagy a ránehezedő anómiás nyomás (pl.: egy szülő, aki nem engedheti meg magának, hogy gyerekének megvegyen egy számítógépes játékot, s inkább ingyen, igaz illegális, letölti egy warez oldalról, stb.), s ezért követi el a cselekményt. Mi több az is előfordulhat, hogy a közvélemény egyes eseteket nem is tekint igazi bűncselekménynek, márpedig a törvényhozónak figyelemmel kell lennie a közvéleményre is, mivel egy társadalmat nem nyilvánithat büntethetővé, végleges megoldást természetesen – mint minden bűnözés esetében - a jelenség társadalmi gyökereinek kezelése jelentené.

A jelenséggel szembeni hatékony fellépés érdekében elengedhetetlen, egyrészt a nemzetközi fellépés, másrészt az emberek megfelelő oktatása (a közösségi védekezés elégtelen, ha nem társul hozzá egyéni védekezés is), a hatóságokat megfelelően fel kell szerelni számítástechnikai eszközökkel, tagjaikat részletes számítástechnikai ismeretekben kell részesíteni. Mindezek mellett az igazságszolgáltatást is megfelelően fel kell készíteni, hiszen mit ér egy megfelelően felkészített nyomozóhatóság, ha az igazságszolgáltatás nem képes megfelelő választ adni a jelenségre.

A közvéleményben mindenképpen tudatosítani kell, hogy a technika gyors fejlődésével, a számítógépek, s főleg a hálózatok elterjedésével, e jelenség világméretűvé duzzadt, így mind több és több ember életére van hatással, így igenis komoly veszélyt jelent, amit nem lehet félvállról venni már. Jelen dolgozatomban is erre szeretnék rávilágítani.

A dolgozat keretén belül általánosságban szeretném bemutatni e jelenséget, ezen belül annak veszélyeire és egyre növekvő súlyára is fel szeretném hívni a figyelmet. A dolgozat megírása során a magyar illetve rendkívül bőséges külföldi szakirodalom mellett saját tapasztalataimat is felhasználtam, melyeket az Interneten, különböző weboldalakon, chat szobákban olvastam, illetve melyeket saját káromon tapasztaltam meg.

E bűnözés ismertetése során kitérek annak fejlődésére – röviden felvázolom e jelenség technológiai hátterének fejlődését is, ami nézetem szerint elengedhetetlen feltétele volt e bűnözés kialakulásához – és jellemzőire, különös tekintettel azokra, melyek veszélyességét nagymértékben növelik. Szükségesnek tartom, hogy megemlékezzek az elkövetőkről, a motiváló tényezőkről, és a sértettekről is. A dolgozat nem alkotna teljes egészt, ha nem térnék ki benne e bűnözéssel szembeni fellépés és azzal szembeni védekezés kérdéseire is.

I. FEJEZET

A SZÁMÍTÓGÉPES BŰNÖZÉS BEMUTATÁSA

1. A számítógépes bűnözés története, fejlődése

A dolgozatomban vizsgált jelenség pontosabb megértéséhez jövőbeni tendenciáinak feltérképezéséhez elengedhetetlennek tartom a jelenség történetének és fejlődésének bemutatását. Különösen a bűnözés ezen ágának fejlődését segítő tényezőket kell szemügyre venni. A számítógépes bűnözés nem jöhetett volna létre a számítógép és a számítástechnika fejlődése nélkül, ezek nagymértékben befolyásolták a vizsgált bűnözés fejlődését, alakulását, ezért szükségesnek tartom a számítógépes bűnözés története mellett a számítógépek fejlődését is röviden bemutatni.

1.1. Kezdetek

Charles Babbage már 1820-ban, az angol kormány megbízásából, kidolgozta a modern digitális számítógép alapelveit. Ellenben az igazi számítógépre 1880-ig várni kellett. Hermann Hollerith építette meg a világ első lyukkártyás számítógépét, melyet népszámlálási célokra használtak. Nagyobb áttörést Konrad Zuse ért el 1936 és 38 között. Zuse-nek sikerült egy szabadon programozható, 2-es számrendszerben működő, billentyűzettel ellátott számítógépet építenie, melyet Z1-nek nevezett.

Az első teljesen működőképes, szabadon programozható, programvezérelt számítógépet (a Z3-ast) szintén Zuse alkotta meg 1941-ban.

A számítógépek fejlődésében újabb áttörést Claude Shannon 1943-as felfedezése jelentette, aki felfedezte az elektromos kapcsolás és a logika kapcsolatát, s sikeresen megalkotta az áramkörök elméletének alapjait. Elmélete később komoly segítséget nyújtott a digitális számítógépek áramköreinek tervezéséhez és egyszerűsítéséhez.

Az első teljesen automata számítógépet a Harward egyetemen fejlesztették ki (Mark 1-es), jó lehet ez is egy lyukkártyás gép volt még, de a programot magát – mely a gépet vezérelte – már egy lyukszalag tartalmazta (az ezen az elve működő gépeket nulladik generációs számítógépeknek is nevezik).

Jelentős változást hozott a számítástechnika terén az elektroncsövek alkalmazása. Jó lehet már 1904-ben feltalálták e technológiai újítást, de csak 1940-től használták azokat számítógépek építéséhez. Az első elektroncsöves gépet 1943 és 46 között építették és lövedékek röppályájának számítására használták – ENIAC-nak nevezték. Az új megoldás következtében, az addigiaknál jóval gyorsabb gépeket tudtak építeni, a technológiai megoldásnak több hátránya is volt: az elektroncsövek nagyon drágák, megbízhatatlanok voltak, méretük is jelentős volt, rengeteg energiát használtak, ráadásul egyszerre csak egy feladatot tudtak elvégezni, így kizárólag tudományos műszaki célokra használták azokat (1946-tól kb. 54-ig tartó időszakot nevezik a számítógépek 1. generációjának).[1]

A ma ismert számítógépek alapelvét Neumann János dolgozta ki. Ebben az időben ismét technológiai változás történt a számítástechnika terén, a tranzisztorok alkalmazása. Tömegesen csak az 1950-es évek végén kezdték használni azokat – a tranzisztorok felváltották a rövid élettartamú és rendkívül energia igényes elektroncsöveket -, így a számítógépek mérete és energia fogyasztása jelentősen csökkent és sokkal megbízhatóbbá is váltak egyben.[2]
A tranzisztoros gépek jelentik a számítógépek 2. generációját. Jellemzően az 50-es évekig kizárólagos tudományos célokra használták a számítógépeket, így az 50-es évek végéig, sőt még a 60-as években is eléggé szűk körben használták csak.

1.2. Az első számítógépes bűncselekmények és elterjedésük

Az előbb elmondottak ellenére az első számítógépes bűncselekményt mégis ebben a korban regisztrálták. 1959-ben az egyesült államokbeli Walston and Co. alelnöke – hamis lyukkártyák segítségével – 250 000 dollárt sikkasztott.
Abban az időszakban még kivételesek voltak az ilyen cselekmények, s mivel – társadalmi szinten – nem okoztak jelentős károkat sem a nyomozó hatóságok, sem a tudományos élet képviselői nem fordítottak komoly figyelmet a jelenségnek.
A számítógépes bűnözés elterjedése a 60-as években vette kezdetét, leginkább annak tudható be, hogy rohamosan kezdtek elterjedni a számítógépek. Kezdetben a számítógépek jogtalan

használata, csalások és adatállományok manipulálása volt jellemző, de akkoriban jelentek meg az első vírusok és trójai programok, melyeket rombolási, információszerzési céllal fejlesztettek ki.[3]

Jelentős lépést jelentett a számítástechnika terén – s így közvetetten a bűnözés terjedését segítette - Jack S. Kilby felfedezése, aki 1958-ban megalkotta az integrált áramkört (a 3. generációs számítógépek jellegzetes alkotóelemét). A tömegtermelés 1962-ben kezdődött, s '64-ben jelentek meg az első integrált áramkörből épített gépek. A számítógépek mérete sokat csökkent, sebességük, illetve az adatátviteli sebességük is jelentősen nőtt. A számítógépek ára is jelentősen csökkent, megbízhatóságuk pedig nőtt, így a piaci kereslet is jelentősen növekedni kezdett. A műszaki világ az iparban is használni kezdte a számítógépeket.[4]

A számítógépek elterjedése és az egyre hatékonyabb adattárolás – a számítástechnika gyors fejlődése forradalmasította az adatok gyűjtését, feldolgozását, tárolását – következtében egyre gyakoribbak lettek a számítógéppel kapcsolatos bűncselekmények. A bűncselekmények egy része csak átalakította az addig is létező cselekményeket, de addig ismeretlen bűncselekmények is megjelentek.

A 60-as évek közepére megjelentek a számítógépes hálózatok, kialakultak az egyes távadat rendszerek is. Az elkövetőknek viszonylag egyszerű dolguk volt, mivel a gyors technológiai fejlődéshez nem társult egyre modernebb biztonsági rendszerek, megoldások kifejlesztése, leginkább azért nem fektettek komoly hangsúlyt a számítógépek, illetve a számítógépes rendszerek védelmére, mert addig nem volt elterjedt a bűnözés e téren.

Ebből az időből származik az egyik legjelentősebb kárt okozó csalássorozat melyet 1963 és 74 között követtek el. Az Equity Funding Corporation cég alkalmazottai a cég számítógépeinek segítségével hamis kötvényeket készítettek, melyekkel aztán fiktív kifizetéseket eszközöltek, összesen 2 millió dollárt csaltak ki a cégből.[5]

Az 1970-es évek közepétől napjainkig terjedő időszak a számítógépek 4. generációja. A gépek szerkezetében nem történt jelentősebb változtatás a 3. generációhoz képest, csupán a korábbi fejlesztéseket tökéletesítették. A mai gépek nagy integráltságúak, magas szintű nyelveken írják a működésükhöz szükséges programokat.[6] A személyi számítógépek elterjedésének jelentős állomása volt a microprocesszorok megalkotása. Amit úgy értek el, hogy a számítógép működéséhez szükséges alkatrészeket egy szilícium lapra integrálták. Tovább segítette a PC-k elterjedését, hogy egyre több perifériát lehetett hozzájuk csatlakoztatni, így kezelésük könnyebbé vált. 1981-ben hozta forgalom az IBM az első PC-t. A PC-k teljesítményét gyorsan tudták növelni, árát pedig csökkenteni, így sikerült elérniük, hogy a 80-as évek végére igen elterjedtté vált a PC.

A számítógépek elterjedtségét jól példázzák a következő adatok:
- 1978 – USA: *500 000* számítógép használó
- 1986 – USA: *30 000 000* számítógép használó
- 1989 – világszerte több mint *100 000 000* számítógép használó személy.[7]

1.3. Az államok kezdeti reakciói és e bűnözés általános problémává válása

Az egyes államok hamarosan felismerték az új bűnözés veszélyeit, és ezzel együtt ráébredtek az adattárolók, s így maguknak az adatoknak a sebezhetőségére. A számítógépek gyors elterjedése, a védelmi rendszerek gyengeségei remek lehetőséget nyújtott az elkövetőknek. Védekezésképpen az egyes államok megalkották saját adatvédelmi törvényeiket – pl.: 1967: USA; 1978: Franciaország; 1970: Dánia.

A fenti kodifikációs hullámmal párhuzamosan a számítógépes bűnözés sokszínűvé válása és gyakorisága miatt a 70-es évek elején megjelentek az első beszámolók, tudósítások a sajtókban és a tudományok irodalomban is.[8]
A 70-es évek közepétől kezdődtek csak a kriminológiai kutatások. A kutatások kimutatták, hogy hatalmas a látencia e bűnözés terén, s egyben rámutattak a jelenség veszélyeire is.

---

[1] http://www.scitech.mtesz.hu/10kiraly/index.html ; http://hu.wikipedia.org/wiki/Számítógép ; Dr. Laczi Beáta: A számítógép és a büntetőjog, Magyar Jog, 2001/3, 137. ó.
[2] Dr. Laczi Beáta: A számítógép és a büntetőjog, Magyar Jog, 2001/3, 137. ó.
[3] Dr. Laczi Beáta: A számítógép és a büntetőjog, Magyar Jog, 2001/3, 138. ó.
[24] http://larix.emk.nyme.hu/teka/biblio/SzamitastechnikaAlapjai/A/A1.htm
[5] Dr. Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról, Belügyi Szemle, 1999/11, 16. ó.
[6] http://www.scitech.mtesz.hu/10kiraly/kiraly_3.html

A 70-es évek vége, 80-as évek eleje jelentős változásokat hoztak, amíg a 70-es évekre a jelenség elterjedés volt jellemző a 80-as évekre a számítógépes bűnözés általános jelenséggé nőtte ki magát. Több tényező is közrejátszott abban, hogy általános jelenséggé válhatott: **a)** számítástechnika gyors fejlődése és a személyi számítógépek széleskörű elterjedése, **b)** adatátviteli rendszerek robbanásszerű fejlődése, **c)** szoftverkínálat rohamos bővülése, **d)** bankkártyák elterjedése, **e)** és végül a védelmi rendszerek fejlesztése lemaradt, ráadásul a meglévők is gyorsan „amortizálódtak", ami a számítástechnika gyors fejlődésének tudható be. A változások következtében a számítógépes bűncselekmények száma és típusai is változott. Megjelentek az adatmanipulálás útján elkövetett számítógépes csalások; számítógépes hamisítások; védett adatbázisok elleni támadások; illegális szoftver-másolás, terjesztés; visszaélés bankkártyával, telefonkártyával stb.[9]

A helyzeten csak tovább rontott a számítógépes hálózatok, s főleg az Internet elterjedése, minek segítségével a fent említett bűncselekmények elkövetése gyorsabbá, leleplezésük még nehezebbé vált, s még nemzetközi jelleget is kaptak, így tovább nehezítették a hatóságok munkáját. Az Internet-bűnözés további, a már említett mellett, jellemzője, az elkövetési formák dinamikus növekedése és változása.

A számítógépes bűnözés tudományos értékelése a 80-as években megváltozott, akkoriban vált nyilvánvalóvá, hogy az nemcsak a gazdasági bűnözés körébe tartozik, hanem annál szélesebb körű, pl.: személyi jogokat sértő számítógépes bűncselekmények. A tudományos irodalom mellett a közvélemény is rádöbbent, hogy a modern információs társadalom igen sérülékeny, így nagymértékben nőtt az igény egyrészt hatékony védelmi megoldások kifejlesztésére, másrészt a hatóságokon is nőtt a nyomás.[10]

Akkoriban indult meg a kodifikációk második hulláma, mely során az egyes országok a büntető törvénykönyveikbe foglalták az elektronikus adatfeldolgozással összefüggő bűncselekmények törvényi tényállásait, melyeket a jelenség változásával folyamatosan módosítottak.

Az 1990-es évektől a számítógépes bűncselekményeket egyre inkább az Interneten – mint a legjelentősebb hálózaton – követték el, s azóta e tendencia csak erősödött.
Az Internet sajátos jellemzői tették lehetővé, hogy e bűnözés számára ideális elkövetési területté váljék. Ezek: **a)** ***nyitottság*** (az Internet egy nyitott hálózat, bárki csatlakozhat rá, aki rendelkezik a megfelelő feltételekkel; **b)** ***interaktivitás*** (az elektronikus kommunikáció esetében az információ olyan formában is megjelenhet, amely felbontja a linearitás kötöttségeit, és megjelenési formáját tekintve a lehetőségek gyakorlatilag végtelen számú variációját tárják a felhasználó elé); **c)** ***konvergencia*** (a számítástechnika és távközlés integrálódásának összekötõ elemeként jelenik meg az adatok tárolásának és továbbításának digitális jellege, amihez az ugyancsak digitalizálható. információtartalom járul); **d)** ***decentralizáltság***; **e)** ***globalitás***, sokan megemlítik még az ***anonimitást*** (Az anonimitás azonban csak látszat, hiszen a szörfözéseink útvonala bármikor visszakereshető egy naplózó program révén, így a szolgáltató segítségével könnyen megismerhető telefonszámunk és a pontos idő is, amikor tárcsáztunk).[11]

A vizsgált bűnözés egyértelműen nemzetközivé nőtte ki magát, ami ellen hatékonyan csak nemzetközi szinten lehet fellépni.
Az első jelentős lépésnek az OECD kezdeményezés tekinthető, mely szervezet egy ad hoc bizottságot állított föl. Második előrelépés az Európa Tanács 1989-ben készített szakértői jelentése volt. Ugyanabban az évben az ET elfogadott egy a témával kapcsolatos ajánlást is – 1989. évi 9. (az ET a tagállamok számára egy minimum és egy fakultatív listában foglalta össze azon bűncselekményeket, melyeknek büntetőjogi szabályozását ajánlotta).
1994-ben már az ENSZ is megjelentetett egy az informatikai bűnözéssel foglalkozó tanulmányt, melyben meghatározta a számítógépes bűncselekmények lehetséges megjelenési formáit, továbbá különös hangsúlyt fektetett az eljárási kérdésekre is.
Az Európai Gazdasági Közösség Tanácsa 1991-ben fogadta el a „*Számítógépes Programok jogi védelméről*" szóló irányelvet (91/250/EGK). Az irányelvet később kiegészítette a Parlament és a Tanács „*Adatbázisok védelméről*" című irányelve.

---

[37] http://www.scitech.mtesz.hu/10kiraly/kiraly_3.html

[8] Dr. Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról, Belügyi Szemle, 1999/11, 17. ó.

[49] Dr. Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog 2001/12, 726. ó.

[10] Dr. Ulrich Sieber: A számítógépes bűnözés és más bűncselekmények az információtechnika területén, Magyar Jog 1993/1, 45. ó.

Ma már több nemzetközi szervezet is foglalkozik a számítógépes bűnözés kérdéskörével, illetve az ellen való fellépés lehetőségeivel.[12] (A nemzetközi együttműködést részletesebben a 8.1. fejezetben tárgyalom)

A számítógépes bűnözés ellen csak nemzetközi szintű fellépés lehet eredményes, ehhez pedig széleskörű együttműködésre van szükség az egyes államok között.

Az újfajta bűnözés elleni első komoly fellépések a 90-es évek elején történtek. Akkoriban több nagyobb letartóztatás is történt, pl.: Milwaukee-i központú „414" csoport tagjainak letartóztatása, akiket közel 60 számítógépes betöréssel vádoltak. Szintén a 90-es évek elején a letartóztatások hatására aktivizálta magát az igazságszolgáltatás is, több nagy nevű hacker ellen is vádat emeltek, mint például Pat Riddle (Captain Zap álnéven tevékenykedett), aki az amerikai védelmi minisztérium számítógépeit támadta több alkalommal is. Riddle neve mellett megemlíthetjük még Kevin Mitnick vagy Kevin Lee nevét is, akiket szinten akkoriban tartoztattak le.[13]

A 90-es évek második felében a szervezett bűnözésen belül is kialakult az intellektuális elkövetők csoportja. A bűncselekmény elkövetői jellemzően magasan képzett fiatalok, jobbára férfiak, akik 2-3 fős csoportokba szerveződve tevékenykedtek. A korábbi években folytatott pénz-, és bélyeghamisítások mellett megjelentek – nagyobb haszonszerzés és könnyebb elkövetés okán – a telefon és bankkártya hamisítások, illetve az ilyen kártyák felhasználására szerveződött csoportok is feltűntek.

A szervezett bűnözés körében rövid idő alatt megjelentek a hacker klubok, melyek különösen veszélyesek, hiszen a hackerek szervezettebben tudnak tevékenykedni, a leghíresebb klubok: Chaos Computer Club, Legion of Doom, stb.

Összegezve az eddig elmondottakat megállapítható, hogy korunk egyik nagy műszaki találmánya a számítógép (illetve a hozzá kapcsolódó számítástechnika), mely mára rendkívül elterjedt a társadalmak minden szegletében, s különösen az államigazgatás, kereskedelmi, gazdasági életben, az egyes ember életének egyre inkább nélkülözhetetlen részévé vált. Miután a számítástechnika robbanásszerű változáson ment át az elmúlt évtizedekben, maga az információ is még inkább felértékelődött, ezzel szemben viszont az adatfeldolgozó rendszerek védelme nem fejlődött olyan tempóban, mint a számítástechnika. Kellő védelem hiánya találkozva az egyes emberek haszonszerzési vágyával, akik még az Internet előnyeit is felhasználhatják, gyorsan egy újfajta bűnözés kialakulásához vezetett.

A kezdeti próbálkozások után a 70-es évektől – a számítógép elterjedésével párhuzamosan – kezdett dinamikusan fejlődni a bűnözés ezen ága. A 70-es években még csak az USA-ban jelentek meg e bűncselekmények, de a 80-as évekre már a nyugat- európai államokban is fellelhetőek voltak, végül a 90-es évekre a közép és kelet-európai államokat is elérte az új típusú bűnözés.[14] A kezdetek óta rengeteg fajtájú bűncselekmény jelent meg. Ezek közé sorolható a számítógépes hamisítás, adatkikémlelés, a számítógépes programok elleni erőszakos vagy intellektuális támadás, visszaélés bankkártyával, s a gyors fejlődés eredményeként a bűncselekmények listája csak bővülni fog a jövőben.

Várható, hogy a számítógépes bűncselekmények száma – és talán típusai is - növekedni fognak. A számítógépes bűnözés elleni védekezés – jelenség jellemzői, sokszínűsége, változékonysága miatt – roppant nehéz. A bűnözés elleni védekezés komoly terhet rak mind az állam, mind az egyes vállatok vállára.

Napjainkra jellemző, hogy nemcsak az elkövetők száma növekszik, de az elkövetők összetétele is változik. Egyre fiatalabb korosztályok is bekapcsolódnak – elsősorban az egyszerű elkövetési lehetőség miatt. Sajnálatos jelenség, hogy manapság már – főleg haszonszerzési motiváció mellett – politikai célból is követnek el számítógépes bűncselekményeket – pl.: Kínából induló wormok, vagy az izraeli szerverek folyamatos támadása.
Az idők során az elkövetők motivációi nem sokat változtak, ám módszereik – a technológiai fejlődés következtében - rengeteget fejlődtek.

---

[511] http://www.freeweb.hu/gaudy/szakdolgq.html

[12] Dr. Laczi Beáta: A számítógép és a büntetőjog, Magyar Jog, 2001/3, 138-139. ó.

[613] http://www.jogiforum.hu/publikaciok/127 (Varga Balázs: Informatikai bűncselekmények)

[14] Dr. Nagy Zoltán: Informatikai bűncselekmények, Magyar Tudomány 2001/8, 946. ó.

2. A számítógépes bűnözés fogalma és csoportosítása

2.1. Fogalom meghatározás

Az előző fejezetben láthattuk, hogy napjainkra a számítógépes bűnözés egyre elterjedtebbé és egyben egyre jelentősebbé is vált, ennek ellenére még nincsen egységes - szakirodalom által egységesen elfogadott – fogalma. Ennek fő oka a jelenség változékonyságában és sokszínűségében keresendő. Amennyiben valaki alkot egy egzakt, pontos definíciót, könnyen meglehet, hogy holnap már nem sokat mond a jelenségről, annak változásai miatt.

Olyannyira nincs egységes álláspontom a szakirodalom, hogy még egységes elfogadott elnevezése sincs a jelenségnek. A többség számítógépes bűnözésről, míg mások informatikai, adat bűnözésről, megint mások számítástechnikai bűnözést emlegetnek, végül találkozhatunk hi-tech bűnözés megnevezéssel is.

Jómagam a számítógépes bűnözés megnevezést fogom használni, több ok miatt is: **a)** e bűnözés egyik fő jellegzetessége, hogy valamilyen módon kapcsolódik a számítógéphez és a számítástechnikához is, éppen ezért szerintem a *számítógépes bűnözés* megnevezés elég jól kifejezi, hogy milyen bűnözéssel állunk szemben. Az emberek többsége, ha ma számítógépről beszél, egyben gondol a számítástechnikára is, mivel a számítástechnika alapvető alkalmazási területe a számítógép építése, programozása,

b) másrészt a nemzetközi dokumentumok többsége is e megnevezést alkalmazza, s már csak a következetesség, s a félreérthetőség elkerülése végett is célszerűnek tartom az említett megnevezés alkalmazását. Azzal a fenntartással, hogy természetesen a többi megnevezés sem pontatlan, hiszen mind a hi-tech bűnözés, mind mondjuk az informatikai bűnözés megnevezések is elfogadhatóak (már csak azért is, mert a számítástechnika szoros kapcsolatban van az informatikával - az információ keletkezését, továbbítását, feldolgozását és hasznosítását vizsgáló tudománnyal – az elkövetők egyik fő célpontjával, az információ).

Előre kell vetnem a fogalom meghatározása előtt, hogy a számítógépes bűnözés gyűjtőfogalom, már a történeti részben is láthattuk, hogy sokféle – egymástól eltérő – bűncselekményeket foglal magába, éppen ezért nehéz pontos definíciót adni a jelenségre. A jelenség felbukkanása óta sokan sokféleképpen próbálták meghatározni e jelenséget.

2.1.1. Egyes fogalomalkotási kísérletek

- A legegyszerűbb meghatározás szerint:

Minden társadalomra veszélyes, bűnös magatartás, melyben a számítógép szerepet játszik. (a fogalom problémája, hogy túl általános)

- A brüsszeli CDIP (Centre de Droit International Pénal) által javasolt fogalom a következőképpen hangzik:

Információs bűnözés minden olyan tevékenység vagy mulasztás, amely számítógépes rendszerekbe történő közvetett, vagy közvetlen behatolással anyagi, vagy szellemi javakban kárt okoz.

- Egy másik megfogalmazás alapján: azon bűncselekmények összessége, amelyek információ-technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak vagy információ-technológiai eszközöket, rendszereket használnak a bűncselekmény elkövetésének eszközeként.[15]

- Kunos Imre szerint:

Számítógépes bűnözés, azon bűncselekmények összessége, melyek esetén információtechnológiai eszközöket, rendszereket használnak a bűncselekmények elkövetésének eszközéül.[16]

- Megint másik meghatározás szerint:

Azon bűncselekmények összessége, amelyek információ technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányulnak vagy információ technológiai eszközöket, rendszereket használnak a bűncselekmény elkövetésének eszközeként.[17]

---

[15] http://www.bm.hu/proba/xforum.nsf/3d525835ae5a397fc1256fe3002bbd71/ 0B0DD172C66279EEC1256970003E99BE?OpenDocument

[16] Dr. Kunos Imre: A számítógépes bűnözés, Belügyi szemle 1999/11, 28. ó.

[17] http://www.bm.hu/proba/xforum.nsf/3d525835ae5a397fc1256fe3002bbd71/ 0B0DD172C66279EEC1256970003E99BE?OpenDocument

A fenti definíciókhoz sok hasonlót olvashatunk még a témával foglalkozó írásokban. A definiálás másik módja, amikor nem egzakt fogalmat próbálunk alkotni, hanem felsoroljuk milyen bűncselekmények tartoznak e bűnözés körébe.

- Így tett az Európa Tanács is a számítógépes bűnözésről szóló ajánlásában – számítógépes bűnözés az, ami a bűncselekmények felsorolásában és az országok részére készített ajánlásban szerepel. Az ET ajánlása egy minimum és egy fakultatív listát is tartalmaz. A minimum lista 8 olyan bűncselekményt tartalmaz, amelyek esetén a Tanács ajánlja, hogy a tagállamok nyilvánítsák büntetendő cselekedetnek, tehát ez az ajánlás „kemény magját" képező cselekmények, míg a fakultatív lista 4 olyan bűncselekményt tartalmaz, amelyek esetén a Tanács tagjai nem tudtak egyöntetűen megegyezni a cselekmények büntethetőségében.

- Megemlíthető az FBI számítógépes bűnözésre szakosodott csoportja (NCCS - National Computer Crime Squad) által alkotott felsorolás:

-□ Behatolás a publikus kapcsolási rendszerekbe (Public Switched Network)
W Behatolás jelentősebb számítógépes rendszerekbe
.
l□ Magántitok megsértése
Ú
é
□ Egyéb bűncselekmények melyeknél a számítógép a legjelentősebb tényező az elkövetés során.
18

Sokáig lehetne még sorolni a fogalomalkotási kísérleteket, mindegyik esetében találnánk valami hibát, kifogásolnivalót.

Nézetem szerint szükségtelen, sőt nehéz is lenne olyan pontos definíció alkotása, mely pontosan lefedné e jelenséget, pontosan a fenn felsoroltak miatt. Inkább a keretjellegű, általános fogalmakat tartom célravezetőnek, jó lehet az általános fogalmak néha homályosak, akkor is előnyösebbek, mint egy egzakt definíció, mivel egyrészt felöleli szinte az egész jelenséget, másrészt könnyen és gyorsan hozzá lehet igazítani a változó viszonyokhoz.
Pont előbb elmondottak miatt tartom előnyös fogalomnak az FBI csoportja által alkotott felsorolás utolsó eleméként említett meghatározást:

Minden olyan bűncselekmény melynél a számítógép a legjelentősebb tényező az elkövetés során.

Előnyösnek tarom ezt a fogalmat, pontosan általánossága miatt, s mert nem tartalmaz semmilyen megszorító jelzőt, mint pl.: haszonszerzés (hiszen nem biztos, hogy e célból követi el a bűncselekményt); számítógépes hálózatok (nem feltétlenül kell hálózat e bűncselekmények elkövetéséhez), illetve nem korlátozza a jelenséget pusztán adatok megszerzésére, manipulálására, mint egyes fogalmak.

Látható a fentiek alapján is, hogy a számítógépes bűnözés meghatározása, a jelenség sokszínűsége miatt nem egyszerű feladat.

2.2. Csoportosítás

A számítógépes bűnözés egy gyűjtőfogalom, melybe sokféle bűncselekmény tartozik. Az egyes bűncselekmények megértéséhez elengedhetetlen egyes magatartások alapos feltárása és – közös ismérv alapján – osztályozása. Miután e jelenség még viszonylag új keletű és jellegzetességei is eltérnek a hagyományos bűnözéstől, ezért a jelenség több feléképpen is csoportosítható.

Két nagy csoportosítási megoldással találkozhatunk a témával foglalkozó szakirodalomban.

2.2.1. Kategóriák szerinti felosztás

A legelterjedtebb felosztás szerint, a számítógép lehet az elkövetés eszköze, vagy a számítógép a bűncselekmény tárgya.

- Az első kategóriába azon bűncselekmények tartoznak, melyek esetén az elkövetés eszköze a számítógép. Két további alcsoportot különböztethető meg:

□ A számítógép járulékos eszköze az elkövetésnek

818 http://cse.stanford.edu/class/cs201/projects-98-99/computer-crime/definition.html

Ä A számítógép az elkövetés eszköze, számítógép segítségével követik el a bűncselekményt

Az első alcsoport esetén a számítógépet valamely hagyományos bűncselekmény elkövetésekor azért használják, hogy egyrészt a) meggyorsítsák az elkövetést, b) csökkentsék a lebukás lehetőségét, c) megnehezítsék a nyomozást (sokkal könnyebben el tudják tüntetni a bizonyítékokat, hisz egy számítógépen pillanatok alatt lehet törölni mindent). Hangsúlyoznom kell, hogy e bűncselekmények számítógép nélkül is megvalósíthatóak – pl.: pénzhamísítás, pénzmosás.

A második alcsoport esetén kifejezetten számítógéppel követik a bűncselekményeket, tehát arról van szó, hogy egy jogszerűen működő gépet, hagyományos bűncselekmények elkövetésére használják föl (tehát nem a számítógépen tárolt adatok, programokon van a hangsúly, hanem magán a számítógépen, s annak működésén).
Például: Az elkövető egy szabályosan működő számítógép tevékenységét illegális célokra alakítja át, vagy olyan programot ír, mellyel a gép működését módosítja, s így követi el a bűncselekményeket. Tehát lényegében „eltéríti" a jogszerűen működő eszközt.

További jellemzőjük, hogy a közös jogi tárgy már elvontan nem határozható meg. A jogi tárgyat és a sértettek körét azon bűncselekmények határozzák meg, amelyek elkövetéséhez felhasználták a számítógépet.[19]

- A második csoportot alkotják a tényleges számítógépes bűncselekmények. Kifejezetten a számítógépes rendszerek, adatok, programok ellen irányuló támadások tartoznak ide.

Példaszerűen néhány cselekmények, melyet e kategóriába sorolhatunk:
é
l Szolgáltatás megtagadása
o

o
l Számítógépes szabotázs

E kategóriába sorolandók azon cselekmények is, mikor valaki azért tör be kormányzati, igazságügyi adatbázisokba, hogy saját, esetleg más adatait módosítsa.
E kategóriába tartozó cselekményeknek jellemzően 3 fő típusa ismert: **a)** az elkövető belép a védett rendszerbe, s adatokat módosít – pl.: kormányzati, igazságügyi adatbázisok; **b)** *technológiai vandalizmus* (techno vandalism) esetében az elkövető engedély nélkül lép be számítógépes rendszerekbe, s ezzel kár okoz programokban, adatokban. Az elkövetők célja nem haszonszerzés, inkább maga a kihívás, a károkat többnyire véletlenül okozzák, de az is előfordulhat, hogy szándékosan; **c)** *technológiai áthaladás* (techno trespass) esetében az elkövető szintén engedély nélkül hatol be a számítógépes rendszerbe, de csak áthalad azon, s nem okoz semmilyen kárt a rendszerben, az elkövető csak „felméri a terepet". A techno trespass inkább csak közvetett károkat okozhat, egyrészt a számítógép tulajdonosának jogait sérti a betöréssel, másrészt ha mondjuk egy vállalatról van szó, akkor kellemetlen a vállalatnak ha kitudódik, hogy a biztonsági rendszerei nem elég hatékonyak.[20]

Mint láthattuk a második kategóriába olyan bűncselekmények tartóznak, melyek esetében az elkövető a számítógép integritását, védelmi rendszerét támadta, s célpontja a gépen lévő adatok, programok.
A két említett kategóriát együtt *számítógéppel kapcsolatos bűnözésnek* (computer related crime) nevezzük.
Egyes szerzők külön kategóriába sorolják a szoftverlopás, illegális szoftver másolás cselekményét is, nézetem szerint szükségtelen újabb kategória létrehozása, akkor mikor a szoftverlopás besorolható a már felállított kategóriákba, a külön kategóriával legfeljebb csak a cselekmény gyakoriságát vagy súlyosságát lehetne hangsúlyozni.

2.2.2. Bűncselekmények szerinti csoportosítás

Szemben a fenti csoportosítással itt jóval többféle megoldással találkozhatunk, ezek közül csak a legjelentősebbeket mutatnám be.

---

9 [19] Dr. Siegler Eszter: A számítógéppel kapcsolatos és a számítógépes bűncselekmények, Magyar Jog 1997/12, 736. ó.
10 [20] http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc124.html (David L. Carter: Computer Crime Categories: How Techno-criminals Operate)

Az egyesült államokbeli Adler-Mueller-Laufer szerzőpáros a következő bűncselekményeket tekinti számítógépes bűncselekményeknek:

- Számítógépes csalás
- Számítógépes kikémlelés
- Számítógépes szabotázs
- Számítógépes hacking
- Számítógépidő-, szoftver és hardverlopás

Martin Wasik a következő csoportokat állította össze:

- Jogosulatlan hozzáférés a számítógépben tárolt adatokhoz vagy programokhoz;
- Számítógépes csalás;
- Adatok vagy programok jogosulatlan elvitele;
- Számítógépidő és szolgáltatás jogosulatlan használata;
- Rombolás vagy károkozás.

A skót jogi bizottság jelentésében a következő csoportokat állította föl

- Adatok vagy programok meghamisítása anyagi vagy egyéb előnyszerzés céljából;
- Jogosulatlan hozzáférés lehetővé tétele;
- A számítógép lehallgatása;
- Információlopás;
- Adattárolók jogosulatlan másolása;
- Számítógépidő vagy eszközök jogosulatlan igénybevétele;
- Adatok vagy programok szándékos vagy gondatlan törlése;
- Illetékes vagy törvényes felhasználó számára a hozzáférés megtagadása[21]

Látható, hogy a számítógépek megjelenése, és főleg gyors elterjedése, átalakította a korábban már létező bűncselekményeket, mivel az elkövetők gyorsan meglátták a technikai újdonságban rejlő lehetőségeket. Idővel így a bűncselekmények egy része átalakult, sőt ahogy a technológia fejlődik s újabb meg újabb számítástechnikai vívmányok kerülnek piacra, úgy válnak a számítógépes bűnözés célpontjává, vagy eszközévé – gondoljunk csak a mobiltelefonokra, a mostani készülékekkel már internetezni is lehet, de ez egyben azt is jelenti, hogy e bűnözés célpontjaivá válhatnak, gondoljunk csak a vírusokra.

A számítógép megjelenése és elterjedése olyan bűncselekményeket is életre hívott, amik addig vagy nem léteztek, vagy nagyon körülményes volt az elkövetés, pl.: illegális szoftvermásolások, szerzői jogok megsértése. Ráadásul az Internet elterjedése újabb lökést adott e bűncselekményeknek, mivel még egyszerűbbé, könnyebbé tette az elkövetésüket.

3. A számítógépes bűnözés jellemzői

A számítógépes bűnözés jellemzői a következők: **a)** gyorsaság; **b)** magas látencia; **c)** nemzetköziség; **d)** technikai jelleg; **e)** nehéz felderíthetőség; **f)** elkövetési terület; **g)** intellektuális jelleg.

3.1. Gyorsaság

A számítógépes bűnözés egyik fő jellegzetessége, annak realizálódása. Hangsúlyoznom kell a gyors realizálódás nem azt jelenti, hogy a bűncselekmények pillanat szülöttei lennének – természetesen ilyen eset is előfordul, de többségére nem ez a jellemző – éppen ellenkezőleg, a legtöbb ilyen bűncselekmény komoly előkészületeket igényel. Megfelelő szoftverek beszerzése, azok kezelésének megismerése; biztonsági rendszerek kiismerése és egyéb előzetes információk beszerzése és mindezek mellett hosszú tanulás (pl.: főiskolákon, egyetemeken, vagy autodidakta módon), és nem utolsó sorban gyakorlatszerzés előzi meg az elkövetéseket.

A gyorsaság tehát az eredmény realizálódására vonatkozik. A gyorsaságot nagyban befolyásolják: **a)** a kor technológiai, technikai színvonala, értelemszerűen az egyre gyorsabb számítógépekkel egyre gyorsabban lehet elkövetni a bűncselekményeket; **b)** adott elkövető szakmai tudása és rutinja. A mai világban egyre modernebb, és ezáltal gyorsabb számítógépek mellett további gondot jelent az Internet elterjedése, mely segítségével már világszerte, nehezen ellenőrizhetően lehet, nagy gyorsasággal elkövetni számítógépes bűncselekményeket.

[1121] http://www.matud.iif.hu/01aug/nagyz.html (Nagy Zoltán: Informatikai bűncselekmények)

Mai világban további problémákat vet föl az időzítés kérdése. Manapság már az sem lehetetlen, hogy előreprogramozzák a számítógépet, hogy meghatározott időpontban tegyen, vagy ne tegyen valamit. Mindezt úgy teszi a gép, hogy az elkövető nem is ül előtte. Az előbb említett megoldás eredményeként rendkívül jól időzített bűnelkövetéssel állunk szembe, ami csak tovább nehezíti a nyomozó hatóságok dolgát.

3.2. Magas látencia

A számítógépes bűnözés területét jellemző magas látenciának több oka van:

- A bűncselekmények egy része rejtett marad, még a sértett előtt is, vagy ha észleli is azt, már csak túl későn pl.: betörnek a számítógépére, s másolatot készítenek egyes filekről, de ezek kívül nem csinálnak semmit.

- A magas látencia másik fő oka, hogy az esetek egy részét nem jelentik. Elég sajátos jelenséggel állunk szemben, s az sem véletlen, hogy pont a gazdálkodó szervezetekre és főleg a hitelintézetekre, biztosítókra jellemző. Az előbb említett sértetteknek komoly anyagi érdeke is fűződik ahhoz, hogy titokban maradjanak az esetek és ne induljon eljárás. Amennyiben kitudódnának az eset, úgy befektetőket, ügyfeleket veszíthetnének e cégek, hisz az emberek pénzüket féltve más cégekhez fordulnának inkább. A sértett cégek így könnyen elveszíthetik ügyfeleik bizalmát egy ilyen ügy kapcsán, s szélsőséges esetben akár tönkre is mehetnek.

- A látenciát fokozó további tényező a tett és a tettes felfedezésének alacsony esélye. A már említett okokon kívül az alábbiak említhetőek.

Az elkövetőket nehéz elfogni, mivel általában nem tartózkodnak az elkövetés helyszínén, másrészt nincs szükségük külső segítőkre, így tovább csökken a lebukás esélye, harmadrészt a kommunikációs csatornákon könnyedén és nyomtalanul eltűnhetnek.
Szintén tovább növeli a látencia mértékét, a hatóságok nem megfelelő felszereltsége, képzettsége, ennek is betudható, hogy kevés elkövetőt sikerül elfogniuk.[22]

3.3. Nemzetköziség

Nem nehéz belátni, hogy a számítógépes bűnözés nemzetközi jelleggel bír. Többek közt azért, mert az elkövetők az Internetet, vagy egyéb más számítógépes hálózatot használnak az elkövetés során. Az Internet (mint a legjellemzőbb elkövetési terület) egy olyan virtuális világ, melyben nincsenek államhatárok, névtelenség álarca mögé bújhat bárki, mely szinte ellenőrizhetetlen – persze jelenleg is vannak próbálkozások, lásd: Kína. A fenti jellemzőkből is egyértelműen látszik, hogy ideális az elkövetők számára.

Szintén az elkövetőknek kedvez, hogy az Internet hatalmas adatállományát, adatforgalmát nem lehet ellenőrizni, így a visszaéléseket nagyon nehéz nyomon követni, illetve ellenőrizni. Végül maga az elkövetés helyszíne is bizonytalanná válhat a nemzetközi jelleg miatt.

3.4. Technikai, technológiai jelleg

Lényegében közvetetten az összes eddigi jellemző hátterében megtalálható volt ez a jellegzetesség, de mégis szükségesnek tartom külön is kiemelni. A számítógépes bűnözés rendkívüli mértékben függ a technológia, technika szintjétől
A számítástechnikai eszközök – és azok folytonos fejlődése - nélkül elképzelhetetlen lenne e bűnözés létezése, éppen ezért tértem ki külön a történeti részben e bűnözés alapját képező technológiai háttér fejlődésére is.
Megfigyelhető az a tendencia, hogy amint kifejlesztenek egy újabb számítástechnikai vívmányt – nem feltétlen csak hardverekre gondolok, hanem szoftverekre is – a bűnözők idővel felhasználják azokat az elkövetés során. Ha tehát valaki véget akarna vetni a számítógépes bűnözés fejlődésének, annak az alapot képező technikai fejlődést is meg kéne állítania.

Nézetem szerint nem is az a komoly gond hogy folyamatosan változik a bűnözés, ez nagyjából a többi bűnözésről is elmondható, hanem, hogy az elkövetőkkel szembeni hatósági fellépés az országok jó részében – elsősorban anyagi okok miatt – nem megfelelő, s pont az előbbi jellemző miatt ez komoly gond, másrészt e bűnözéssel szembeni védekezés sem megfelelő szintű.

---

[12][22] Dr. Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998. 261-263. ó.

Leginkább, azért mert az emberek nincsenek megfelelően felvilágosítva a jelenség jellemzőiről, s így nem is veszik komolyan, holott napjainkban már szép számmal állnak rendelkezésre védekezést elősegítő technikai megoldások.

3.5. Nehéz felderíthetőség

A számítógépes bűncselekményeket nehéz észlelni és még nehezebb felderíteni, ennek szintén több okra vezethető vissza:
Egyrészről e bűncselekményeket nehezen, vagy csak későn észlelhető módszerekkel hajtják végre, ez a jelenség szintén nehezíti a felderítést.

Másrészről a nyomozó hatóságok nem elég jártasak még a számítógépes bűnözés terén. Továbbá nem egyszerű dolog bizonyítékokat szerezni, hisz még ha le is foglalják a gyanúsított számítógépét, a gyanúsított gyorsan törölhet, vagy titkosíthat mindent, vagy akár magát a gépet, vagy az adathordozót megsemmisítheti, megrongálhatja még a lefoglalás előtt.
Végül a már említett üzleti élet sem érdekelt abban, hogy segítse a hatóságok dolgát.

3.6. Elkövetési terület

A számítógépes bűnözés leginkább két területre koncentrálódik:

- Az egyik fontos (pl.: katonaság, politika, igazságszolgáltatás szempontjából fontos) – vagy akár titkos – információkat, adatokat tároló rendszerek támadása – pl.: valaki betör a BM nyilvántartási rendszerébe, annak érdekében, hogy korábbi priuszát törölje.
- A másik a gazdasági, pénzügyi világ területe.

Mindkét terület hatalmas haszonnal kecsegteti az elkövetőket, ráadásul még az is az elkövetők kezére játszik, hogy roppant kellemetlen mindkét említett terület számára, ha kitudódik egy ilyen eset, így nem áll érdekükben nyilvános eljárást kezdeményezni, hanem inkább maguk próbálják kinyomozni az elkövető kilétét.[23]

3.7. Intellektuális jelleg

A számítógépes bűnözés, döntően intellektuális bűnözés. E bűnözés kialakulásához, a technológiai háttér mellett, jól képzett szakemberek *tömeges* megjelenésére és *tömeges* képzésére volt szükség. A számítógép és a hozzá kapcsolódó eszközök, berendezések használata szakértelmes, felkészültséget igényel(t) az egyes szakemberektől.
Megvizsgálva e bűnözés fejlődését észrevehetjük, hogy amíg a technika és a szakképzés nem vált tömegessé, addig nem is ölthetett olyan mértéket, mint napjainkban.

Az elkövetők általában fiatal, magasan képzett, magas intelligenciájú, általában számítógépes szakemberek, akik nem ritkán 2-3 fős csoportokba szerveződve követik el a bűncselekményeket. Az előbb elmondottakból is következik a ravasz elkövetési módszerek alkalmazása és az előre kiterveltség. Az elkövetői csoportok a globalizáció és a technika – pl.: hálózatok és elsősorban az Internet – felhasználásával követik el a bűncselekményeiket.

Az esetek többségében sokoldalúan szocializált elkövetőkről beszélhetünk – pl.: tisztában vannak a jogaikkal – akik szakképzettségük miatt jobb egzisztenciális körülmények között élnek. Rendezett életkörülményeik folytán jobb ügyvédeket engedhetnek meg maguknak, mint a szegényebb elkövetők. Mindezek mellett általában büntetlen előéletű személyek, akik a hatóság bizalmát élvezik.[24]

Természetesen olyan számítógépes bűncselekményeket is találunk, melyek nem igényelnek magas szakképzettséget, s mégis komoly károkat lehet okozni velük – lásd: vírusok, trójai programok.

A fenti jellemzők szemléltetésére kiváló példa az ***automatizált bűnözés*** jelensége, mivel rendelkezik valamennyi jellemzővel. E jelenség keretében arról van szó, hogy egy számítástechnika terén járatos személy egy olyan programot készít, mely, ha eljut egy célszámítógépre, azon automatikusan – a készítő beavatkozása nélkül – kicsomagolja és futtatja magát. A futtatás során, pedig elkövet valamilyen bűncselekményt, pl.: töröl bizonyos dokumentumokat, avagy lemásolja azokat, s továbbítja a készítőhöz. Miután mindezzel végzett, az elkövetés minden bizonyítékát törli. A bűncselekmény rendkívül gyorsan történik, s a sértett

[1323] http://www.fsu.edu/~crimdo/TA/hao/computer%20crime2.htm (Dr. Cecil Greek: Computer crime)

akkor sem észleli, ha történetesen a számítógép előtt ül, s mivel minden nyomot megsemmisít a program, így a nyomozók nem tudják felderíteni az ügyet, s az elkövető ez idő alatt teljes biztonságban érezheti magát, hiszen ő részt sem vett a bűncselekmény tényleges kivitelezésében.

Ráadásul a készítő az egyes elkövetések során tesztelheti a programot, s folyamatosan finomíthatja, tökéletesítheti azt, a lebukás veszélye nélkül. További veszélye az ilyen programoknak, hogy hálózatokon, pl.: Internet, gyorsan eljuthat rengeteg sértetthez egyszerre. Azon elkövezők, akik nem rendelkeznének megfelelő ismeretekkel egy ilyen program elkészítéséhez, azok különféle hacker oldalakról beszerezhetnek párat.[25]

3.8. Fehér galléros bűnözés – számítógépes bűnözés

Érdemes a számítógépes bűnözés jellegzetességei körében összehasonlítani a ***fehér galléros*** bűnözéssel.

A büntetőjogi szakirodalomban nincs teljes egyetértés arról, hogy a számítógépes bűnözés külön kategória-e, avagy a fehér galléros bűnözés része. A fehér galléros bűnözés fogalmát Edwin H. Sutherland alkotta meg, aki a 40-es években végezte kutatásait – ezt a kifejezést használta a felsőbb osztályok bűnözésének jellemzésekor. Nézete szerint fehér galléros bűnöző az, aki a bűncselekményt tekintélyének és magas társadalmi státuszának felhasználásával munkája folytán követi el.
A kriminológusok kezdettől fogva gazdasági, anyagi motiváltságú foglalkozási bűnözésnek tekintették. Sutherland elméletét a 60-as években Clinnard és Quinney fejlesztették tovább. Ők már a fehér galléros bűnözésen belül megkülönböztettek foglalkozási bűncselekményt (az elkövető munkakörét felhasználva szerez magának jogtalan előnyöket, számítógép felhasználásával – pl.: operátorok, számítógép kezelők, rendszergazdák), illetve szervezeti bűncselekményt (az elkövető a szervezet számára biztosítandó előny, vagyoni haszon érdekében követi el a bűncselekményt – pl.: adó, társadalombiztosítási csalás, üzleti titok megsértése.).[26]

Visszakanyarodva az eredeti kérdéshez megállapítható, hogy a számítógépes bűnözés a fehér galléros bűnözés mindkét típusában előfordul. Ezzel szemben több olyan számítógépes bűncselekmény is létezik, amely nem sorolható a fehér galléros bűnözés körébe. Hiszen a számítógépes bűnözésnél ki kell emelnünk, hogy az elkövetők nem feltétlenül képzett emberek, sőt napjainkban egyre fiatalabb korosztályok is részt vesznek az elkövetésekben, már csak e jelenség miatt sem fedi egymást a két bűnözés. Végkövetkeztetésként leszögezhetjük, hogy mindkét típus önálló kategória, melyek között létezik átfedés, de nem fedik teljesen egymást.

4. Elkövetők, motivációk, sértettek

4.1. Elkövetők

Amikor számítógépes bűnözésről beszélünk – ami egy erősen technológiai bűnözés - sosem feledkezhetünk meg az emberről, az elkövetőről. Önmagában a technika nem veszélyes, az elkövetők azok, akik nem megengedett, illegális célokra használják.
Legelőször azt érdemes tisztázni ki válhat elkövetővé, milyen feltételeknek kell megfelelni ehhez:

- Megfelelő szinten kell értenie a technikai eszközökhöz, azok kezeléséhez.
- Olyan helyzetben kell lennie, mely lehetővé teszi számára a számítógép, vagy egyéb számítástechnikai berendezés használatát, minek segítségével elkövetheti a bűncselekményt.[27]

A társadalmi helyzetüket, munkakörüket tekintve – figyelemmel arra, hogy a számítógépes bűnözés a fehér galléros bűnözéshez áll a legközelebb – az elkövetők többsége fiatal, magasan képzett, törekvő ember. Általában jól ismerik a vállalat, cég felépítését, védelmi rendszereit, működését, ahol dolgoznak. Többségük alkalmi haszonszerzés céljából követi el a bűncselekményt.

Az elkövetők második csoportjába azon személyek tartoznak, akik nem rendelkeznek, olyan szakismerettel, mint az előbbi csoport tagjai, egyszerű beosztottak, akik talán véletlenül

---

[24] Dr. Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998. 264-265. ó.

[25] www.blacksheepnetworks.com/security/info/misc/autocrime1.htm (Donn Parker: Automated crime)

[26] Dr. Nagy Zoltán: Informatikai bűncselekmények, Magyar Tudomány 2001/8, 947. ó.

döbbentek rá, hogy mi mindent tehetnek egy számítógéppel, s egyszerűen csak kihasználják az adandó alkalmat.

A számítógépes bűncselekményeket elkövetők gyakran bizalmi pozíciót töltenek be az adott cégnél, ami nagyban megkönnyíti az elkövetést, hiszen az emberek bizalmával visszaélve könnyen hozzájuthatnak jelszavakhoz, s kijátszhatják a védelmi megoldásokat.[28]
Az elkövetők egy része tehát olyan személy, aki valamilyen indíték hatására, helyzetével, szaktudásával visszaélve követi el a bűncselekményeit. Az előbbi állítást támasztják alá azon amerikai és brit kutatások melyek szerint az elkövetők többsége (kb. 80%) belső személy, s nem külső.

Természetesen a vállalatokat nemcsak belülről, hanem kívülről is érhetik támadások. A külső támadok többsége a ***hacker***-k.
A hacker *olyan személy, aki idegen számítógépes rendszerekbe, azokat védő védelmi programok kijátszása, feltörése révén jut be* (régebben – 50-es, 60-as évek – olyan személyeket neveztek így, akik elegánsan és a szokásostól eltérő módon használták az új technológiát és magas szintű szaktudásukat).[29]

A hackerek általában nem haszonszerzési céllal törnek be az egyes rendszerekbe, hanem saját képességeik tesztelése, fitogtatatása végett. Magasan képzett a számítástechnika és védelmi rendszerek terén jártas személyek a hackerek, akik a rendszerek védelmének gyenge pontjaikat használják föl a bejutás során.

A hackerek motivációik, céljaik elég eltérőek lehetnek: károkozás; védett adatok megszerzése; kíváncsiság; erőfitogtatás; tapasztalatszerzés; de az is előfordul, hogy segítő szándékkal törnek be egy rendszerbe, az utóbbi elkövetőket nevezik *„jó hacker”*-nek. Ők betörnek egy rendszerbe, s nem okoznak semmilyen kárt, hanem felhívják a rendszergazda figyelmét a védelmi hiányosságokra, gyenge pontokra, s ezáltal segítik a hatékony védelmi rendszer kiépítését – természetesen a jó szándék ellenére is komoly károkat okoznak a „jó hackerek” is, hisz a rendszer feltörhető; irreleváns, hogy jobbító szándékkal törték-e föl vagy sem.

Jellemző a hackerekre, hogy többségük nagyobb szakmai gyakorlattal bír, mint a védelmi programok fejlesztői, így nem csoda, hogy fel tudják törni azokat.[30]

Említést érdemel a legális hackerek, a szakértő rendszertesztelők (**etikus hacking**, korábban ezt nevezték számítógépes önbetörésnek is, de mivel napjainkban már külső személyeket kérnek fel e munkára, ezért az önbetörés kifejezés már nem helytálló). A védelmi rendszerrel rendelkező cég megbízásából e hackerek tesztelik a védelmi rendszert, a szerződésben a cég megadja a célszámítógép IP címét[31], s a megbízott hackerek igazi betörőként viselkedve megpróbálják feltörni, s bizonyos ideig próbálkoznak, majd tapasztalataikat egy jelentésben összegzik, amiben fölhívják a megbízó figyelmét, arra, hogy mit és hogyan kéne javítani a védelmen, hogy jobban funkcionáljon.[32]

Legismertebb egyéni hackerek: Nick Whiteley (Mad Hacker); Kevin Mitnick (Condor); Kevin Poulsen (Dark Dante); Pat Riddle (Captain Zap).
A hackerek veszélyességét tovább növeli, hogy a szervezett fellépés érdekében klubokba tömörülnek – leghíresebb klubok: Chaos Computer Club, Bayerische Hackerpost, Legion of Doom stb. Mint minden bűnözés esetén a szervezettség mindig többlet veszélyeket hordoz magában. A klubok segítségével a hackerek összehangolhatják támadásaikat, információikat megoszthatják egymással, tanácsokat adhatnak egymásnak, illetve szakmailag is fejlődhetnek.
Szintén komoly problémát jelent, hogy a szervezett bűnözés is felfigyelt e jelenségre, mint ahogy erre már utaltam a történeti bevezetőben is. A profi hackerek nagyobb és könnyebb haszonszerzés, avagy fanatizmusból, esetleg nagyobb kihívás céljából eladják szaktudásukat a szervezett bűnözőknek, akik felbérlik őket bizonyos munkák elvégzésére.

Napjainkra kialakult egy elkövetői réteg, melyet csak *komputerunderground*-nak neveznek. ***Steven Mizrach*** szerint a következő elkövetők sorolhatóak e kategóriába

- ***Hackerek, crackerek*** (a crackerek annyiban különböznek a hackerektől, hogy jellemzően haszonszerzési célból törnek be védett rendszerekbe)

[1627] Dr. Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998. 279. ó.

[28] Fekete Zsuzsanna: Az információbiztonság a számítógépes bűnözés tükrében, Főiskolai Figyelő 1999/2, 79. ó.

[1729] Parti Katalin: A számítógépes bűnözés és az internet, Kriminológiai Tanulmányok 2003.40, 201. ó

[30] Parti Katalin: A számítógépes bűnözés és az internet, Kriminológiai Tanulmányok 2003.40, 202. ó.

[31] Az internetprotokoll (angolul Internet Protocol, rövidítve: IP) az internet (és internetalapú) hálózat egyik alapvető szabványa. Ezen protokoll segítségével kommunikálnak egymással az Internetre kötött csomópontok (számítógépek, hálózati eszközök, stb.)

[32] Papp Péter: Etikus Hacking, Belügyi Szemle 2022/11-12, 41-43. ó.

[1833] Steven Mizrach: Létezik-e „hackeretika” a 90-es években, Replika 2000/41-42, 303-305. ó.

- ***Phreakek*** (telefonvonalakba, illetve rendszerekbe próbálnak technológiai eszközökkel bejutni)
- ***Vírusírók*** (olyan személyek, akik olyan kódokat írnak, melyek megpróbálnak behatolni más rendszerekbe, s gyakran mellékhatásokat is produkálnak)
- ***Kalózozok*** (a crackerek közül váltak ki, szoftverek védelmi rendszereit feltörő személyek, akik e tőrt-szoftvereket terjesztik is.)
- ***Cypherpunkok*** (olyan programokat terjesztenek, melyekkel bárki adatait erős kódolással láthatja el – nagy teljesítményű számítógépekkel is komoly feladat feltörni az ilyen erősen kódolt adatokat)
- ***Anarchisták*** (törvénysértő, vagy legalábbis morálisan kétes megítélésű információkat terjesztő személyek – pl.: bomba készítés stb. Anarchista a komputerundeground tekintetében olyan személy, aki minden olyan kísérletet, rendelkezést elutasít, amely akadályozná az információ szabad áramlását)
- ***Kiberpunk*** (általában a fentiek valamilyen kombinációja).[33]

Látható, hogy elég sokféle elkövető típus jöhet számításba e bűncselekmények elkövetésekor Az elkövetők tanulmányozásakor egy napjainkban egyre jelentősebb tendenciára is rá kell mutatnom, amire már többször utaltam, mégpedig az elkövetők életkorára.
Egyre jellemzőbb, hogy fiatal – akár még kiskorú – személyek követnek el számítógépes bűncselekményeket. Például egy előre elkészített programmal elkészít egy vírust, s azt útnak indítja az Interneten, ami akár károkat is okozhat.

A fiatal elkövetők között inkább persze a file-cserélés és az illegális szoftvermásolás, terjesztés a jellemzőbb, ami azért enyhébb, mint mondjuk a vírusírás. A jelenség már csak azért is aggaszó, mert egy részük még csak nem is büntethető, másrészt koruknál fogva egy részük nem is látja át tettének következményeit.

Érdemes kitérni az Interneten elkövetett bűncselekmények kapcsán egy érdekes kérdésre, a felelősség kérdésére, vagyis ki vonható felelősségre egyáltalán az Interneten elkövetett bűncselekmények elkövetésért?

- Első csoportban szóba jöhetnek telekommunikációs szolgáltatók, vagyis azon szervezetek, melyek a hálózat fizikai fenntartását biztosítják, tehát megteremtik a számítógépek összekapcsolódásának lehetőségét.

- A második csoportban beszélhetünk a hozzáférés (*Internet access provider*) felelősségéről, vagyis azon szervezetekről, melyek a telekommunikációs szolgáltatók igénybevételével biztosítják a felhasználók hálózathoz jutását.

- Harmadikként szóba jöhetnek a tartalomszolgáltatók (*content provider*), melyek az előbbi két szolgáltató igénybevételével tartalmakat helyeznek el a hálózaton.

- Végül a fenti kategóriákba nem sorolható egyéb szolgáltatók, pl.: cache szerver (átmeneti tároló) üzemeltetője [34]

Az egyes Interneten elkövetett számítógépes bűncselekmények esetén a fentiek közül több szolgáltató felelőssége is megállapítható lehet.
Az előbbi megállapítás különösen az egyik chat szobában általam olvasott hozzászólás fényében válik elgondolkodtatóvá. A hozzászólót az Internet hozzáférést biztosító szolgáltatója felszólította, hogy ha lehet hagyjon föl az illegális tartalmak letöltésével, az illető akkora már több warez oldalról is töltött jó ideje folyamatosan, s a felszólítás után is folytatta e tevékenységét, s mégsem tett semmit a szolgáltató.
Az előbbi példa is jól mutatja, hogy az egyes szolgáltatók pontosan nyomon követik, hogy egyes ügyfeleik mit tesznek (Internet anonimitása már csak ezért is megkérdőjelezhető), így azt is pontosan tudják mikor követnek el azok bűncselekményeket.

Az eddig elmondottak ellenére le kell szögeznem, hogy Internet jellemzői miatt az elkövetők könnyen követhetnek el bűncselekményeket, de ennek ellenére nem elfoghatatlanok!
A letartóztatások körében különösen az amerikai hatóságok jeleskednek, melyek szervezett „hadjáratok" keretében – összefogva más országok hatóságaival - próbálnak hatékonyabban fellépni többek közt e bűnözés ellen. Az egyik legeredményesebb hadjáratuk (Operation Firewall,

[34] http://jesz.ajk.elte.hu/szentkuti15.html (Szentkuti Dániel - Szűts Márton: Az Internet és a büntetőjogi felelősség egyes kérdései

Tűzfal Hadművelet) során 28 embert vettek őrizetbe. Ezen személyek nagy része hitelkártya-számokkal, jogosítványokkal, és egyéb személyes adatokkal kereskedett, és elsősorban a világhálón végezte tevékenységét.

Végezetül érdemes lenne megfontolni, hogy a nagy szaktudású hackerket a társadalom szolgálatába kéne állítani – pl.: vádalku keretében rábírni, hogy a hatóságok munkáját segítse. Ahogy a mondás tartja: „*Betyárból lesz a legjobb pandúr*”.

4.2. Motivációk

A tettesek motivációik rendkívül sokfélék lehetnek. Gyakori motiváció az *anyagi haszonszerzés*. A haszonszerzés motiválja például a bank-automatákat manipuláló személyeket. Szintén e motiváció áll a szoftverek jogosulatlan másolásának, forgalmazásának, a félvezetők tiltott másolásának, kereskedésének hátterében is.
E motivációra jó példa a már említett Kevin Poulsen, aki betört egy telefoncég rendszerébe, s úgy manipulálta a rendszert, hogy ő nyerje meg egy sorsolás fődíját, egy autót.

Motivációk között megemlíthető a *védett személyes adatok, állami, szolgálati, banktitok* jogellenes megismerésére irányuló szándék is. Nyilvánvaló, hogy az előbb említett adatok megszerzése, avagy módosítása, megváltoztatása mögött anyagi haszonszerzés is meghúzódhat, hiszen e titkok és adatok akár komoly értékkel is bírhatnak.
Elrettentő példaként álljon itt a 80-as években történt eset, a KGB hamburgi, hannoveri és egyéb nyugat-berlini fiatalokat bujtott föl, hogy a kelet-berlini kereskedelmi kirendeltség kommunikációs rendszerét felhasználva a Pentagon, NASA és egyéb más fontos amerikai intézmények számítógépes adatállományaihoz férjenek hozzá, a nyugat-német hatóságok leleplezték az elkövetőket, s kémkedés miatt a bíróság el is ítélte őket.

Következő motivációként a *károkozás* emelhető ki. Az elkövetők betörnek rendszerekbe, és védett adatállományokat törölnek, módosítanak, vagy lemásolnak, s így egyrészt komoly károkat is okozhatnak, másrészt megsértik az egyes emberek magánszféráját.

Elsősorban munkahelyeken gyakori motiváció a *frusztráltság, elismerés hiánya*, vagy ami sokkal veszélyesebb a *bosszú*. Olyan eset is előfordul, mikor az elkövetőt az unalom indította a bűncselekmény elkövetésére [35]
A bűnözés intellektuális jellegéből adódóan sokan *szakmai kihívásként* fogják föl a bűnelkövetést. Megint másokat a hírnév-szerzés motivál.

Megemlíthető a *jó szándék* is, mint motívum, a már említett „jó hackerek” esetében. Szintén motiváló lehet e bűnözés jellegzetességeiben rejlő lehetőségek is, melyekre már szintén kitértem dolgozatomban.

Elképzelhető akár további motiváló erőként az Internet-mítosz nyújtotta torz, hamis kép is. E torzkép szerint, amennyiben valaki rendelkezik egy PC-vel, Internet hozzáféréssel, beléphet egy virtuális világba, ami a valós világ mellett létezik, s mely egy külön társadalmat szervez. Egy olyan világba, ahol bármit megtehet (akár bűncselekményeket is elkövethet), bárki lehet. E új világ teljesen más életformát kínál, mint valódi párja, tanulással gyorsan a ranglétra legtetejére emelkedhet (hackerek szintje), s ott már szinte korlátlanok a lehetőségek.[36]
E virtuális világ, ilyen formában nem létezik – még. Az emberek számára komoly csábítást jelenhet egy ilyen lehetőség, s minél jobban megtanulják kezelni a PC-t, Internetet, annál nagyobb lesz a csábítás, s egy esetleg nem megfelelően szocializálódott személy, akár a fenti motiváció által is hajtva elkövet különféle bűncselekményeket

Jay Bloombecker a következő motivációkat emeli ki:

- Egyfajta szórakozás a bűnelkövetés a tettesnek,
- Könnyű elkövetés motivál egyeseket,
- Megoldási módként fogják föl, mellyel megoldhatják anyagi és személye problémáikat,
- Az új technika segítségével új típusú bűncselekményeket követnek le, vagy már létezőket „modernizálnak”
- A számítógépre, mint egyfajta varázspálcára tekintenek, amellyel bármi lehetségessé válik,

---

[20][35] Dr. Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998. 280. ó.

[36] http://www.freeweb.hu/tarrdaniel/documents/Transzhumanizmus/internetmitosz.html (Tarr Dániel: Az internet mítosz)

- Munkaadók és munkavállalók közötti harc egyik fegyvereként tekintenek a számítógépes bűncselekményekre,
- Politikai, ideológiai nézeteiket névtelenségbe burkolózva vallhatják meg.[37]

A fent említettekből is látszik, hogy milyen sokféle tényező motiválhatja az egyes elkövetőket a bűnelkövetésre.

4.3. Sértettek

A számítógépes bűnözés jellemzője, hogy nem kizárólag egy csoport ellen irányul (még ha az eddig elmondottak alapján úgy is tűnhetett, hogy elsősorban a gazdasági életre koncentrál), hanem – kihasználva a különféle számítógépes eszközöket, hálózatokat adta lehetőségeket – bárki ellen. Megállapítható, hogy többségében mégiscsak vállalatok – anyagi potenciáljuk miatt – az elkövetők fő célpontjaik.

A vállalatok, hivatalok sérelmére elkövetett bűncselekmények közül súlyuknál és számuknál fogva kiemelkednek az adatok megszerzésére, vagy manipulálására irányuló bűncselekmények, valamint az anyagi haszonszerzést célzó bűnelkövetések is. Utóbbin belül két csoportot különböztethetünk meg: **a)** az adatok manipulálása útján szerzett anyagi előny, illetve **b)** a zsarolásszerű cselekmények – pl.: valakinek a gépére bejuttatnak egy vírust, s ha a tulajdonos nem fizet bizonyos összes, akkor aktiválják a vírust.

E bűnözésnél is vizsgálni kell a sértetti közrehatás mértékét. Gyakran a sértettek könnyelműsége vezet oda, hogy áldozattá válnak. Nem vigyáznak kellőképpen jelszavaikra – amit ha, megszereznek az elkövetők, könnyen bejuthatnak a kérdéses rendszerekbe, s az esetleges ellenőrzéskor még nem is feltétlen feltűnő, hisz a tettes létező felhasználó adataival lépett be. Nem változtatják meg jelszavaikat kellő gyakorisággal, vagy túl egyszerű jelszót választanak, stb. Jövőben ezért kellene komoly hangsúlyt fektetni a számítógépes bűnözés elleni védekezés oktatására, mivel az emberek csak kellő informáltság mellett képesek felkészülni az ellenek irányuló támadásokra.[38]

5. Látencia mértéke

A számítógépes bűnözés súlyának és veszélyességének érzékeltetésekor általában egyes esetekre szokás utalni. Elsősorban a 70-es, 80-as években folytak - a témát érintő - átfogó kutatások, mely időszakban a számítógépes bűnözést, mely egyre elterjedtebb jelenséggé vált, túlnyomórészt számítógépes csalás, - szabotázs, - kikémlelés cselekmények alkották.
Az előbb említett kutatásokat a rendőri szervek kriminológusokkal együtt végezték, s a kutatások kiderítették, hogy az elkövetéseknek csak töredékét észlelik a hatóságok.
A tárgyalt jelenség 80-as évek közepén történt drasztikus növekedése után a kutatások elvesztették jelentőségüket, s sok államban beszüntették azokat.

A számítógépes bűnözés terén, mint a korai kutatások is jelezték, jelentős mértékű látenciával kell számolni, ami több okra vezethető vissza:

- Mint korábban már említettem, egy technológiai jellegű bűnözéssel állunk szemben, melynek jellemzői nagyban megnehezítik a felderítést.

- További oka a magas látenciának, hogy nem minden hatóság rendelkezik megfelelő technikai felszereltséggel, illetve megfelelő számítástechnikai ismeretekkel. Ráadásul a nyomozást tovább nehezíti, hogy bűncselekményt gyorsan követik el, az elkövető nem tartózkodik a helyszínen, így kevés nyomot hagy hátra.

- Igen jelentős látenciát növelő tényező a vállalatok, cégek, s elsősorban a bankok, biztosítók magatartása, a korábban említettek okok miatt e cégek gyakran nem jelentik a bűncselekményeket, s így tovább növelik a látencia mértékét.

- További ok lehet, az emberek bizalmatlansága a hatóságok felé. Az emberek egy része nem bízik abban, hogy a hatóságok fel tudják deríteni a bűncselekményt. Másik oka lehet annak, hogy az állampolgárok nem jelentik, hogy a bűncselekmény által okozott kár nem éri el az ingerküszöbüket, vagy csak nem akarnak időt pazarolni az eljárásra.

[2137] http://www.scit.wlv.ac.uk/~cm1988/CP3349%20SLAPA/computer_crime.htm

Az emberek hajlamosak „átesni a ló másik oldalára” és túlbecsülni a felderítetlen bűncselekmények számát, ennek szintén több oka lehet:

- A sajtó szenzációként számol be az egyes jelentős károkat okozó esetekről, s ezzel azt sugallja a nézőknek, hogy sokkal veszélyesebb a jelenség, mint amilyen valójában,
- Akik nem dolgoznak számítógépekkel, azoknak e szenzációszerű hírek igaznak tűnhetnek, mert nem tudják megítélni a hír igazságtartalmát,
- Az érzékeny számítástechnikai rendszereket komoly veszély fenyegeti – már csak jellegüknél fogva is – jó lehet még nem érte őket komoly támadás soha.[39]

A látencia mértékének megbecsülése – a fentieken túl – a jelenség változékonysága miatt is nehéz. Szintén megnehezíti a vizsgálatot a jelenség világméretűvé válása, pont e jellemző miatt nem készült még átfogó kutatás e területen.
Amennyiben megvizsgálnánk az egyes országok bűnügyi statisztikáit, ugyanarra az eredményre jutnánk: magas látencia és a felderített ügyek csupán a jéghegy csúcsát képezik.

6. Okozott károk mértéke, a jelenség veszélyessége

6.1. Károk mértéke

A számítógépes bűnözés komoly károkat idézhet elő. E bűnözés egyik nagy veszélye pont az, hogy gyorsan, komoly erőfeszítés nélkül, minimális lebukási veszély mellett és persze minimális szakmai tudással és megfelelő technikai felszereltséggel akár igen jelentős károkat lehet előidézni.

Az esetek többségben *anyagi károkat* - mind közvetlenül, mind közvetetten - okoznak az elkövetők. Közvetlenül okoznak anyagi károkat pl.: adatok ellopásával, törlésével. Közvetetten pedig, ha a cselekmény által okozott kár nem jelentős, de annak anyagi hatásai annál inkább pl.: bankok esetén. Utóbbira jó példa a következő eset:
Carnegre Mellon Egyetem két kutatója megvizsgált 18 vezető céget (IBM, Microsoft stb.) és kimutatták, hogy amint kiderült, hogy e cégek által készített valamely szoftver sebezhetőségét bejelentették, azok részvényeinek árfolyama átlagosan 0,6%-val esett.[40]
A fenti példából is látszik, hogy nemcsak a sértett vállalatnak okoz kárt az elkövető, hanem még a szoftver gyártó cégeknek is. A cégek mellett az egyes felhasználóknak is közvetetten okozhatnak károkat – pl.: egy cég valamilyen on-line szolgáltatást nyújt, s az elkövetők megbénítják a rendszert, így a szolgáltatás átmenetileg nem üzemel, tehát a felhasználó nem tudja azt igénybe venni.

Az anyagi veszteség mellett *nem anyagi kárral* is kell számolni minden elkövetés esetén.

A fentieken túl a cégeknek hosszútávon is anyagi veszteséget okozhatnak az elkövetők, hisz egy betörés után a cégnek több pénzt kell fordítani a hatékonyabb védelem kialakítására, esetleg újabb embereket kell alkalmaznia, stb., ami sok pénzbe kerül, amit könnyen lehet, hogy a szolgáltatásaikat igénybevevőkre hárítanak át, így az egész szolgáltatás drágábbá válhat.

6.2. A jelenség veszélyei

A számítógépes bűnözés által okozott károk és veszélyeinek szemléltetésére álljon itt néhány eset:

- Az első Cleveland-ban, Ohio-ban történt 2005-ben. Kenneth J. Flury 2004. április 15. és május 4.-e között betört a Citibankba s több ügyfél bankkártya számát, pin-kódját, és egyéb személyes adatait lopta el, majd ezen adatok segítségével bankkártyákat gyártott. Három hét leforgása alatt , az ATM automatákból a lopott pin-kódok és hamisított kártyák segítségével *384.000 dollárt* vett ki. Flury-t 32 hónap szabadságvesztésre ítélte a bíróság.[41]

- A második eset szintén bankkártya csalásokkal kapcsolatos. Hat ember (Andrew Mantovani, Kim Taylor, Jeremy Stephens, Brandon Monchamp, Omar Dhanani, Jeremy Zielinski) állítottak bíróság elé – és ítéltek el - Washington-ban a következő ügy kapcsán: Az említett hat ember közösen üzemeltette a „hadowcrew.com” oldalt, az egyik legnagyobb internetes központot, ami lopott bankkártya, hitelkártya számokkal, adatokkal és azonosítókkal foglalkozott. Az említett oldalon az azonosítókkal és adatokkal üzleteltek, az oldal vezetőségét (említett 6 főt) 2004 októberében fogták el.

---

[22] [39] Dr. Nagy Zoltán: Az informatikai bűncselekmények kriminológiai aspektusai, Ferenc Zoltán emlékkönyv 2004., 236. ó.
[2340] http://www.nol.hu/cikk/375750/ (Szentgyörgyi Zsuzsa: Mibe kerül az e-bűnözés?)

Az oldal működése során összesen 1.5 millió lopott bank-, hitelkártya adatai cseréltek gazdát, mellyel összességében *4 millió dollár* kárt okoztak.

A tettesek a bíróságon beismerték tetteiket, sőt Mantovani azt is beismerte, hogy 2004. szeptemberében jogtalanul hozzájutott kb. 18 millió e-mail címhez, (továbbá felhasználói nevekhez, belépési jelszókhoz, egyéb azonosításhoz szükséges személyes adatokhoz) – ebből 60 000 esetén hozzájutott olyan személyes adatokhoz is, mint: vezetéknév, keresztnév, nem, lakóhely adatok, telefonszám.

A vádlottak 5 év letöltendő szabadságvesztésre ítélték, és 250.000 $ megfizetésére kötelezték őket.

A hat elkövető mellett összesen 21 további embert vettek őrizetbe, akik közül 12-t el is ítéltek, továbbá külföldön is több embert is őrizetbe vettek.[42]

- A következő eset egy számítógépes csalás. Jessice Quitugua Sabathia-t 2004. október 6.-n bűnösnek találta a bíróság, mivel számítógépével több, mint *875.000* dollárt sikkasztott a North Bay Health Care Group-tól ("North Bay"). North Bay egy non-profit szervezet, mely Vacaville-ben és Fairfield-ben (California) található kórházakkal és klinikákkal működik együtt.

Sabathia, aki az említett szervezetnél dolgozott a munkaadója engedélye nélkül, számítógépével, belépett a North Bay számlázási szoftverébe, s saját magának 127 csekket állított ki, összesen a fent említett értékben. Sabathia úgy állította be a szoftvert, mintha a csekkeket a szervezet ügyfeleinek utalták volna. A nyomozó hatóság, viszont leleplezte a csalást, s letartoztatták[43]

- Ivanov ellen több bűncselekmény miatt emeltek vádat, hacking, számítógépes csalás, bankkártya csalás. Ivanov volt azon orosz hackerek egyike, akik az Egyesült Államok béli szervereket támadták több alkalommal is. Felhasználói neveket, jelszavakat, bankkártya információkat, adatokat loptak, a sértetteket azzal fenyegették meg, hogy letörlik az adataikat, s tönkre teszik a számítógépes rendszereiket. A bíróság Ivanov-t tette felelőssé kb. *25 millió dollár* károkozásért.

Alexey V. Ivanovot a bíróság 48 hónap végrehajtandó szabadságvesztésre ítélte.[44]

- A Cisco Systems, Inc., könyvelői Geoffrey Osowski és Wilson Tang hatáskörüket túllépve behatoltak a vállalat számítógépes rendszerébe és közel 8 millió dollárt átutaltak maguknak.

Az állam és az elkövetők között létrejött vádalku értelmében, mindkettőjüket 1 rendbeli számítógépes csalás miatt ítélték el, továbbá az állam elkobozza a tőlük lefoglalt pénzt. Ezen felül jóvátételt fognak fizetni, még pedig az ellopott összeg és a tőlük lefoglalt ékszerek, gépjárművek értékesítéséből kapott összeg különbözetét

A vádalku értelmében mindkét elkövető beismerte, hogy 2000. október és 2001. március 27. között – jogosultsági körüket túllépve – az említett összegű csalást elkövették.
Az említett időszakban összesen *7,868,637 dollárt* sikkasztottak el.
A bíróság 2001, augusztus 20.-n mindegyik vádlottat 34 hónap szabadságvesztésre, és 7,868,637 $ kártérítés megfizetésére ítélte a bíróság.[45]
Úgy vélem a fenti néhány példa is jól szemlélteti, hogy milyen hatalmas anyagi károkat okozhatnak az elkövetők.

7. A számítógépes bűnözéssel kapcsolatos büntetőjogi problémák

A vizsgált jelenség mind a jogalkotás, mind a jogalkalmazás terén sok fejfájást okoz. A legnagyobb probléma, hogy e bűncselekmények egy része nem vagy csak nehezen sorolható be a klasszikus bűncselekmények rendszerébe, pl.: kiterjesztő értelmezéssel könnyedén be lehetne sorolni, de e megoldás tiltott a büntetőjog területén.
Mint ahogy már megemlékeztem róla a bűncselekmény kodifikálása során az amerikaiak voltak az úttörők az 1970-es években, majd őket követve indult el az első nagy kodifikációs hullám, majd azt követve a második is.

Alapvetően a jogalkotó kétféleképpen oldhatja föl a felmerült problémákat:

2441 http://www.cybercrime.gov/flurySent.htm
[42] http://www.cybercrime.gov/mantovaniPlea.htm
2543 http://www.cybercrime.gov/sabathiaPlea.htm
[44] http://www.cybercrime.gov/ivanovSent.htm
[45] http://www.cybercrime.gov/Osowski_TangSent.htm

- A már létező tényállásokat egészíti ki, e megoldás hátránya, hogy csak azon cselekmények esetén működik, melyeket már korábban is elkövettek – és szabályozta is a jogalkotó – és a számítógép csak megkönnyíti a megvalósításukat. Azon bűncselekmények esetében tehát, melyeket még nem követtek el korábban, új tényállásokat kell alkotni. E megoldást választotta Olaszország, Németország.

- A másik megoldás pedig, ágazati törvények alkotását jelenti, melyre példaként hozható Anglia, vagy Spanyolország.

Le kell szögeznem, hogy a törvények önmagukban nem elégségesek, s nem is nyújtanak kellő védelmet, azokat más megoldásokkal és a leginkább hatékony fellépéssel kell ötvözni. Személy szerint úgy vélem egyes társadalmi értékek, érdeke védelme nem igényel feltétlen büntetőjogi szabályozást, hiszen tekintettel a büntetőjog eszközeinek súlyára, illetve a szubszidiaritás elvére, az csak ultima racio lehet minden esetben. Amennyiben ezen eszközhöz kell folyamodni, a jogalkotónak körültekintően kell mérlegelnie milyen eszközöket választ a büntetőjogon belül, kerülni kell az értelmetlenül túl szigorú szabályozást.

A fenti érveléssel szemben igazat kell adni azoknak is, akik azt állítják, hogy e jelenséggel szemben jogon kívüli, illetve jogon belül polgárjogi illetve közigazgatás jogi eszközök nem nyújtanak akkora védelmet, mint a büntetőjogiak, így azok elégtelenek.

A büntetőjog alkalmazása esetében elengedhetetlen egy jól kimunkált fogalmi rendszer és a következetes jogalkalmazás ellenkező esetben jogbizonytalanság keletkezhet, ami semmiképp sem kívánatos. A jogalkotónak arra is figyelemmel kell lennie, hogy a Büntető törvénykönyveket mindig hosszú távú elképzelések alapján kell (kéne) módosítani.

A büntetőjog következő problémája a technika, mivel az adatfeldolgozó, - átviteli rendszerek fejlődése állva hagyta a büntetőjogi szabályozást.

A jelenség a jogalkalmazás számára is komoly gondokat okoz, hisz az esetlegesen pontatlanul, vagy nem teljes körűen szabályozó törvények mellett a legtöbb országban nincs komoly jogalkalmazói gyakorlat – kivételként említhető pl.: USA. Így a jogalkalmazók még csak az általános gyakorlatot sem hívhatják segítségül.

Tovább nehezíti a jogalkalmazók munkáját, hogy e bűncselekményeken belül előfordulnak határesetek is. E cselekmények az illegalitás – legalitás határán helyezkednek, mintegy szürkezóna, összefoglalóan ***számítógéppel való visszaélésnek*** nevezzük ezeket. Legfőbb jellemzőjük, hogy elmossák a legalitás határait, illetve - negatív hatásaik ellenére - gyakran csupán technikailag tűnhetnek hibásnak. Az elkövetőket gyakran a legjobb szándék vezérli, cselekedetük morálisan mégis kifogásolható. Álljék itt néhány példa e bűncselekményekre:

- Egy irodai alkalmazott irodai gépén egy kisebb adatbázist üzemeltet, melynek segítségével végzi másodállását.
- Egy szülő felajánlja gyermeke iskolája számára, hogy lemásol számukra egy olyan programot, melyet az iskola nem tudna megvásárolni.

A fentieken után látszik, hogy a számítógépes bűncselekmények jogi minősítése nem egyszerű dolog. A minősítés nehézsége főleg két tényezőre vezethető vissza, *egyrészt* nincsenek még kiforrott definíciók e témán belül, *másrészt* az adat, elektromágneses impulzus nehezen értelmezhető a tradicionális kategóriákkal.[46]

A büntetőjog eddig ugyanis hagyományosan „megfogható” kategóriákkal dolgozott, az új technológiai fejlődés viszont felértékelte az adatok szerepét, ami viszont nehezen megfogható, így nehezen helyezhető el e büntetőjogi jogviszonyokat elhelyezni a tradicionális rendszerben.

[2646] Dr. Nagy Zotán: Konferencia az információtechnikai bűnözésről, Magyar jog 40. 1993/2., 102. ó.

II. FEJEZET

A SZÁMÍTÓGÉPES BŰNÖZÉSSEL SZEMBENI FELLÉPÉS KÉRDÉSEI

8. Számítógépes bűnözés elleni fellépés

A szakdolgozat eddigi fejezeteiben a tárgyalt jelenség kialakulását, fejlődését, jellemzőit, veszélyeit törekedtem bemutatni. Az eddig sorra vett kérdések csak az érem egyik oldalát jelentették, a másik a jelenséggel szembeni fellépés alkotja, melyet fontossága miatt érdemes részletesebben tárgyalni.

A jelenséggel szembeni fellépésnek több szintjét különböztetem meg:
- Legtágabb szintje: a nemzetközi összefogás (8.1),
- Második szintje: a nemzeti, állami szint (8.2),
- Végül pedig: az egyéni szint (8.3).

A 3 szint egymásra épül, s kiegészíti egymást, mivel e bűnözés esetén kifejezetten igaz, hogy hiába a magas szintű az állami fellépés vagy, és az egyéni szint, nemzetközi összefogás nélkül nem sokat ér
Ideális esetben a 3 dimenzió szintjén kellően hatékony a fellépés, s úgy komoly eredményeket lehet elérni az egyes típusú bűncselekményekkel szemben.

Az elkövetkezőkben a 3 szintet fogom külön-külön megvizsgálni, bemutatni, a teljesség igénye nélkül, a változó viszonyokra és lehetőségekre tekintettel ezt nem is tartom célszerűnek. Az egyes szinteknél csak a legjelentősebb, legfontosabb lehetőségekre térek ki csupán.

8.1. Nemzetközi összefogás

A soros nemzetközi együttműködés és jogegységesítés több okból is fontos e téma kapcsán. Az adatátviteli hálózatokon hatalmas mennyiségű adatot tárolnak, melyeknek nagy a mobilitása, illetve a hálózatok, s köztük a legjelentősebb, az Internet egyik jellemzője, hogy átnyúlnak a határokon, s az adatok szinte ellenőrizhetetlenül mozognak (az eddig alkalmazott ellenőrzési megoldások nem tökéletesek, s komoly erőforrásokat kötnek le), többek közt ennek eredménye, hogy az elkövetők könnyedén követhetnek el külföldön is bűncselekményeket.
A számítógépes bűnözéssel szembeni hatékony fellépés és a számítógépes rendszerek védelme érdekében is szükséges az összefogás.[47]

A jogegységesítés segítségével pedig, egyrészt csökkenthető az országok közötti szabályozási eltérések (elég nagy eltérések létezhetnek az országok között), ami a bűnelkövetőknek kedvez természetesen. Ezen eltérő szabályozások következtében jöttek létre az *informatikai paradicsomok*, melyek olyan helyeket jelölnek, ahol nem vagy nagyon enyhén büntetik csak e cselekmények elkövetőit és a lebukás veszélye is minimális, illetve a jogértelmezés szempontjából is elengedhetetlen. A fentiekre tekintettel mindenképp méltányolható egyes nemzetközi szervezetek – pl.: ENSZ, Európa Tanács – lépései. Következőkben e lépéseket veszem sorba.

8.1.1. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD)

A szervezet által 1983 és 1985 között kiküldött ad hoc bizottság elemezte az európai országok e bűnözés terén szerzett tapasztalatait, s e tevékenységével iránymutatást kívánt adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez és kodifikációjához.
A bizottság megpróbálta rendszerezni e kategóriába tartozó bűncselekményeket, de az általuk felállított csoportosítás nem fedi le a teljes jelenséget, hanem pusztán a szoros értelembevett számítógépes bűncselekményeket.

A bizottság munkájából egyértelműen kiderült, hogy az egyes államokat foglalkoztatja e jelenség, s fel kívánnak lépni ellen, nem véletlen, hisz pontosan ebben az időszakban kezdett jelentős méreteket ölteni e bűnözés.

Másik e szervezethez köthető lépés 1996-ban történt: a francia és belga kormányok az Internettel kapcsolatos nemzetközi együttműködési megállapodás megkötésére tettek javaslatot.

[27] [47] http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (Ulrich Sieber (1998): Legal Aspects of Computer-Related Crime in the Information Society, 3-4. ó.)

[48] http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (Ulrich Sieber (1998): Legal Aspects of Computer-Related Crime in the Information Society, 157-158. ó.)

Az elkészült dokumentum 3 részre tagolható: **a)** *alapelvek*; **b)** *rendőri és igazságszolgáltatási alapelveket* is lefektette; **c)** meghatározta azon irányelveket, melyet betartásával garantálhatóak az alapvető etnikai szabályok védelme, illetve melyekkel javíthatóak az egyes felhasználók védelme.[48]

8.1.2. Európa Tanács (ET)

Az ET első harmonizáció irányába tett lépése az 1981-es adatvédelmi konvenció volt, mely egyik fontos szakasza szerint az aláíró felek megfelelő szankciókat vezetnek be az adatvédelmi alapszabályokat megsértő személyekkel szemben. Igaz a szankciók megállapítása a tagállamok feladata volt, de ennek ellenére jelentős lépés volt egy egységes rendszer felé.

A második fontos lépése e szervezetnek az 1989. szeptember 13.-án kibocsátott ajánlás volt. Az ajánlásban javasolta a tagállamok számára, hogy nemzeti törvényeik módosításakor, illetve új törvények alkotásakor vegyék figyelembe a számítógéppel kapcsolatos bűnözés elleni fellépés szükségességét.
Az ajánlás alapját az 1985-ben alakított szakértői bizottság jelentése képezte. A jelentés nemcsak a számítógépes bűnözéssel kapcsolatos elméleti és gyakorlati ismereteket, illetve nemzetközi tapasztalatokat rendszerezte, hanem arra is törekedett, hogy dogmatikailag megalapozott legyen. A szakértő bizottság e jelentéssel kívánt iránymutatás nyújtani a tagállamok törvényhozói számára, egy egységes szabályozás létrehozásához.[49]
A szakértő bizottság arra a következtetésre jutott, hogy először az alapelveket kéne kidolgozni - melyeket minden állam figyelembe venne a kodifikáció során – s csak ez után sorra venni az alapelvekre tekintettel az egyes bűncselekményeket. A bűncselekményeket, pedig az OECD ad hoc bizottsága által készített felsoroláson kéne alapulnia.
A fentiek alapján a következő alapelveket dolgozták ki: a) büntetőjog ultima ratio szerepe a magánélet védelme terén (ultima ratio elve); b) a büntetőjogi szabályozás esetén annak pontosnak kell lennie, kerülni kell a generál klauzulákat, illetve a kazuisztikus jogalkotást (pontos szövegezés elve); c) előző elvvel összefüggésben: a büntetendő cselekményeket pontosan körbe kell írni, kerülni kell pontatlanságokat (egyértelműség elve); d) különböző számítógépes bűncselekményeket, különbözőképpen kell büntetni (differenciáltság elve); e) e bűncselekmények elkövetőit csak szándékos elkövetés esetén kéne büntetni (szándékosság elve); enyhébb magánélet elleni számítógépes bűncselekmények esetében sértett kívánatára büntetendőek csak (panasz elve).[50]

A fenti jelentés alapján készített ajánlás nem határozta meg a számítógépes bűncselekmény fogalmát, helyette az egyes elkövetői magatartási módozatokat sorolta föl két csoportra osztva. Az első csoport – minimum lista – 8 elemből áll, az ajánlás kemény magja. E 8 bűncselekmény esetében a Tanács javasolta a tagállamoknak, hogy mindenképp teremtsék meg a büntethetőség lehetőségét. E bűncselekmények: a) számítógépes csalás; b) számítógépes hamisítás; c) számítógépes adatokban, programokban történő károkozás; d) számítógépes szabotázs; e) jogellenes behatolás; f) jogellenes titokszerzés; g) védett számítógépes programok jogellenes másolása; h) félvezető topográfiák jogellenes másolása.

A második csoportba – fakultatív lista – 4 bűncselekmény tartozik, e cselekmények büntethetővé nyilvánításában nem jutottak egyességre a tagállamok, így pusztán ajánlják a tagállamoknak büntethetővé nyilvánításukat. E bűncselekmények: a) számítógépes adatok és/vagy programok megváltoztatása; b) számítógépes kémkedés; c) számítógép jogellenes használata; d) védett programok jogellenes használata.[51]

Az ajánlást egyesek az OECD jelentés továbbfejlesztéseként értelmezik, mivel az előbbi egyrészt tartalmilag bővebb, másrészt pontosabban elhatárolja az egyes bűncselekményeket egymástól.
Jómagam egyetértek azokkal, akik azt állítják, hogy az ajánlás nem jelent előrelépést a szabályozott bűncselekmények számát tekintve. Már csak azért sem, mivel a két dokumentum eltérő céllal jött létre. Az OECD jelentés az egyes számítógépes bűncselekmények körülírására törekedett, az ET ajánlás, pedig a nemzeti törvényhozások számára kívánt iránymutatást

---

[28] [49] http://iroga.hu/internet&politika/bacsko.htm (Bacskó László: Bûnözés az Interneten); http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (Ulrich Siebert (1998): Legal Aspects of Computer-Related Crime in the Information Society, 153. ó.)

[50] http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (Ulrich Sieber (1998): Legal Aspects of Computer-Related Crime in the Information Society, 154. ó.)

nyújtani, továbbá az ajánlás a számítógéppel kapcsolatos bűncselekményeket vette alapul, így szélesebb alapról indított, mint a jelentés. .

8.1.3. Egyesült Nemzetek Szervezete (ENSZ)

E szervezet esetében két lépést emelnék csak ki:

- 1994-ben kiadott egy útmutatást, mely a számítógépes bűnözéssel szembeni védekezés kérdéseivel foglalkozott, s jelentősen támaszkodott a fent említett ET ajánlásra.
- 1989-es gyermekek jogairól szóló New York-i egyezmény, mely több szabályt is tartalmazott a gyermeknek a káros tartalmakkal szembeni védelméről.

8.1.4. Európai Unió (EU)

Az első lépéseket az EU Tanács tette meg 1996-ban, a rasszizmus és xenophobia elleni közös fellépés meghirdetésével. E közös fellépés alapján minden tagállamnak biztosítani kellett a hatékony fellépés, együttműködés feltételeit. A közös együttműködés ki kell terjednie a nyomozás, igazságszolgáltatás területeire egyaránt.

Az illegális tartalmakkal szembeni fellépés terén az EU Bizottság is jó néhány dokumentumot bocsátott ki. E dokumentumok több illegális, veszélyes tartalmakat nevesítenek, s szabályozási megoldásokat is ajánlanak. A dokumentumok következtében az Interneten tevékenykedő valamennyi személy (felhasználók, rendszergazdák, szerzők stb.) a tagállamok szabályozásának tárgyává váltak.

A szintén 1996-ban született *zöld könyv* a fiatalkorúak fejlődését és az emberi méltóságot sértő tartalmak elterjedésének megakadályozására és e tartalmakkal szembeni fellépés alapvető kérdéseivel foglalkozik. E dokumentum 10 alapkérdést vizsgál meg, annak érdekében, hogy a későbbiekben egy koherens kerethatározat születhessen e témában.

Végül kiemelhető még az EU Parlament által kiadott egy STOA (Scientific and Technological Options Assessment) tanulmányt, mely a veszélyes tartalmak blokkolásának technológiai lehetőségeivel foglalkozik.

8.1.5. Association International de Droit Pénal (AIDP)

Elsősorban az 1994-ben Rio de Janero-ban a számítógépes bűnözésről tartott konferenciát kell kiemelni. A konferencián szóba kerültek az ET és az ENSZ fenti megállapításai. A kongresszus résztvevői is a büntetőjogon kívüli eszközöket kívánták előnyben részesíteni e bűnözéssel szembeni fellépés, illetve a magánélet védelme esetében.

A résztvevők fontosnak tartották, a magánélet védelme mellett az adatok szabad áramlása, s azok megismeréséhez fűződő érdekeket is.

Abban is egyetértettek, hogy a büntető jogi eszközök csak akkor alkalmazhatóak, ha minden más próbálkozás kudarcot vallott.[52]

Az előbbiekben példálózóan kiemelt néhány szervezetnek és dokumentumnak köszönhetően a számítógépes bűnözés elleni fellépés és annak szabályozása sokat fejlődött. A jövőben viszont további lépéseket kell tenni, különösen a következő területeken:

- Az együttműködést olyan területekre is ki kell terjeszteni, ahol még nem történtek jelentős lépések – pl.: üzleti titkok védelme;
- Szélesebb alapokra kell helyezni az együttműködést, be kell vonni azon államokat is, melyek eddig nem fordítottak komoly figyelmet a témának, csak így szüntethetőek meg az információs paradicsomok,
- Fokozni kell a tudományos együttműködést is a hatékonyabb védekezés érdekében.

8.2. Állami, nemzeti szint

Az állami szinten belül is többféle eszköz, lehetőség áll rendelkezésre. Tekintettel e bűnözés jellemzőire a hatóságoknak is újfajta hozzáállást kell kialakítaniuk

---

[29][51] Dr. Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998. 285. ó.

[3052] http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html (Ulrich Sieber (1998): Legal Aspects of Computer-Related Crime in the Information Society,, 170-174. ó.)

Miután a számítógépes bűncselekményeket egyre inkább az Interneten követik el, érdemes feltenni két kérdést:

a) Lehet-e szabályozni, korlátozni az Internetet?
b) Kell-e szabályozni, korlátozni?

Az első kérdésre könnyen válaszolhatunk: *igen*.
Az Internetet lehet szabályozni, s ha szabályozunk valamit, azt egyben korlátok közé szorítjuk. Gondoljunk csak arra, hogy az Internet szolgáltatás, tartalmak Interneten elhelyezése, weboldalak beüzemelése, hírközlés, stb. is szabályozott, feltételekhez kötött.
Az előbbi néhány példa is mutatja, hogy az Internet szabályozott jelenség, mind jogilag, mind technikailag (szoftver szintén: egyes gépre telepíthető megfigyelő programok; hardver szinten is: pl.: modem maga).

Az emberek többsége a korlátozás, szabályozás szavak hallatán sokkal drasztikusabb megoldásokra asszociál. Gondolok itt többek közt Kínára, ahol kemény eszközökkel próbálják korlátozni az Internetet – weboldalak betiltása, törlése; tartalom cenzúrázása, azok hatóság általi szűrése; e-mail-k; Internet tartalomkeresők szűrése. A kormány megtesz mindent a nem kívánatos tartalmak szűrése, korlátozása érdekében (elsősorban politikai vallási, emberi jogi, témákkal foglalkozó tartalmakra kell gondolni, de a pornográfia sem éppen elfogadott).
Persze nem Kína az egyetlen hasonló eszközöket alkalmazó ország, igaz egyben a legagresszívabb módszereket alkalmazó; megemlíthető még: Irán, Vietnám, Burma, Kuba. Az országok jó része csak minimális mértékben szűri az Internetes tartalmakat – pl.: gyűlölet beszédek esetén.[53]

A második kérdésre már nehezebb válaszolni. E kérdés esetében a korlátozás alatt nem a durva, agresszív módját értem, hanem a működéshez szükséges minimális mértékű szabályozást. E kérdés kapcsán már megoszlanak a vélemények. Egyesek az Internet szabadságára, s általa nyújtott lehetőségekre hivatkozva ellenzik a korlátozásokat. Mások – jómagamat is beleértve – szükségesnek tartanak valamilyen szintű korlátozást. Elengedhetetlennek tartom az Internet szabályozását, korlátozását, annak ellenére, hogy az rendelkezik egy belső önszabályozó rendszerrel is.

Az említett önszabályozás két részből áll: **a)** egyrészt az emberek nagy többsége tiszteletben tartja az emberi együttélés alapvető szabályait az Interneten is (annak ellenére, hogy az egyes kultúrák találkozásakor számolni kell konfliktusokkal, amik szélsőséges esetben akár különféle támadásokba torkolhatnak: vírus küldözgetése, szerverek támadása, oldalak feltörése stb.); **b)** másrészt a weboldalak adminisztrátorai, fórum moderátorok, rendszergazdák szintén egyfajta belső korlátot jelentenek (gondoljunk csak az egyes fórumok szabályzataira, melyek betartatása a moderátorok feladata).

Ezen önkontroll viszont elég törékeny, mivel az Internet látszólagos anonimitása mögé bújva egyes emberek sok mindent megengednek maguknak, továbbá a moderátorok, adminisztrátorok is emberek, figyelmetlenség, hanyagság, avagy együttérzés végett előfordulhat, hogy nem végzik a munkájukat, sőt esetleg ők maguk az elkövetők, s ekkor összeomlik az önkorlátozási rendszer.
Az előbb mondottak miatt szükséges a külső - elsősorban rendőrség általi – kontroll.

8.2.1. Internet-rendőrség (web-police)

A világon az első számítógépes bűnözéssel foglalkozó rendőri egységet 1971-ben, Angliában a Scotland Yard hozta létre. Akkoriban a hatóságok még nem szenteltek akkora figyelmet e jelenségnek, mint napjainkban, ezt jól jelzi, hogy az említett egység 1985-ig összesen 1 tisztből állt.

Későbbiek során, ahogy változott a helyzet egyre több olyan jelenség jelent meg, mely rendőri beavatkozást igényelt, gondoljunk csak a világhálón található illegális tartalmakra, avagy az Interneten elkövetett számítógépes bűncselekményekre.
Így más államokban is felmerült az igény egy olyan egység iránt, mely a számítógépes bűnözés nyomába eredhet: 80-as évek második felében az USA-ban létrehozták az FBI keretében a már említett NCCS-t. 1998-ban a németek létrehozták a Bunderkriminalamt (BKA). Megemlíthető a Japán 1999-es kezdeményezés is, hogy Kínáról ne is beszéljünk.[54]

Egyik legújabb kezdeményezésként, pedig Északrajna-Wesztfáliában felállított virtuális rendőrség

---

[3153] http://www.theatlantic.com/doc/200605/chinese-internet (Matthew Quirk: The web police)
[3254] http://iroga.hu/internet&politika/bacsko.html (Bacskó László: Bűnözés az Interneten)

Az Internet-rendőrséggel kapcsolatban érdekes kérdés, hogy milyen mértékben ellenőrizhetik a világhálót. Egyrészt a hatóságoknak fel kell lépniük a bűnözéssel szemben, de egyben ügyelniük kell arra, hogy ez ne legyen aránytalanul erős fellépés, egyfajta arany középutat kell találni. A rendőrök számára több lehetőség is adott: viselkedhetnek egyszerű felhasználóként, így tarthatják szemmel a világhálót, többségében a Chat szobákat, weboldalakat, letölthetnek tartalmakat stb.

Másik megoldás a fedett tevékenység, e megoldás csak akkor alkalmazható, ha sértett és másik jogainak sérelme arányban áll a bűncselekmény súlyával, vagy bizonyíték felkutatása, elkövető elfogása várható ettől a megoldástól.

Nehéz választ adni a korlátozás mértékének kérdésére. Látható, hogy a világ országai eltérő módszereket alkalmaznak, legyen szó akár erős cenzúrázásról. Több mint kérdéses, hogy egyáltalán fönntartható-e a durva cenzúrázás, mivel ahogy nő az Internetezők száma úgy kell minél több energiát és pénz áldozni a korlátozási szint fenntartására, másrészt minél többen 'neteznek' annál nagyobb eséllyel játszható ki a rendszer.

Nézetem szerint szükséges a rendőrségek szervezetén belül egy külön a számítógépes bűncselekmények felderítésére, megelőzésére szakosodott egység létrehozása (melyet már több ország fel is állított).

Egy ilyen csoport működése szempontjából elengedhetetlenek a következő feltételek:

- Megfelelő technikai felszereltség (megfelelő teljesítményű, gyors számítástechnikai eszközök, amiket a hardverek fejlődésével továbbfejlesztenek)
- Elégséges személyzet biztosítása, akik nem csupán rendőrök, hanem informatikusok, számítástechnikai szakemberek. A megfelelő számú ember már csak a folyamatos működés tekintetében is lényeges.
- Elengedhetetlen a személyzet képzettsége, illetve folyamatos továbbképzése. Nélkülözhetetlen, hogy a csoport tagjai járatosak legyenek a számítástechnika, Internet használata, biztonsági rendszerek működése terén.

8.2.2. Nyomozás a számítógépes bűncselekmények esetében

Itt tartom indokoltnak, hogy röviden kitérjek a nyomozás és bizonyítás egyes kérdéseire, kapcsolódva az Internetes-rendőrség témaköréhez.

A számítógépes bűncselekmények esetében a nyomozás és különösen a bizonyítás nem egyszerű dolog, mivel sok tekintetben eltér a hagyományos nyomozástól.
Sajátos jellegénél fogva, illetőleg erős technológiai alapja miatt speciális nyomozati módszereket igényel a hatóságok részéről e bűncselekmények felderítése.
Komoly gondot okoz, mint már kitértem rá, hogy egyre inkább az Interneten követik el e cselekményeket, mivel ez egy egyszerű, gyors, biztonságos módja az elkövetésnek.

A nyomozást sok tényező nehezíti, ezek a következők:

- A korábban már említett változékonyság, itt nem pusztán a technológiai változékonyságra gondolok, e jellemző nehezíti a nyomozást is, mivel az elkövetés nyomait könnyen és gyorsan meg lehet semmisíteni, módosítani.
- Az előbbi tényező át is vezet a második okra, a bizonyítékok hiányára, előfordul, hogy alig marad valami használható nyom, amin elindulhatnak a nyomozók.
- Fontos szerepe van az időtényezőnek, mivel a bűncselekményeket gyorsan követik el, így a hatóságoknak is gyorsan kell reagálniuk, különben odaveszhetnek a bizonyítékok.
- Külön problémát jelent az adatokhoz hozzájutni Internetes elkövetés esetén, hiszen ha vesszük a freeweb tárhelyeket (olyan internetes oldalak, ahol általános szerződési feltételek elfogadása után bárki díjmentesen helyezhet el tartalmakat), melyek esetében a szolgáltató a szerződéskötés után törli a felhasználó adatait.[55]
- Anonimitás is komoly gondot okozhat, mivel az adatbázisokat nem feltétlen egy pontosan meghatározható gépről érik el, hanem például hálózatba csatolt gép valamelyikéről, így az elkövető kilétének megállapítása is nehéz.[56]
- Nehezíti a nyomozók dolgát az esetleges szervezettség. Például bankkártyákkal való visszaélés esetén egyre inkább megfigyelhető a szervezett elkövetés.[57]
- Nehezíti a nyomozást a sértett figyelmetlensége, mivel előfordulhat, hogy észre sem veszi, hogy bűncselekményt követtek el sérelmére, avagy pusztán jól formált üzleti érdekei miatt nem jelenti azt.

---

[33] [55] Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései, Kriminológiai Tanulmányok, 2004. 41., 265-265. ó.

- Nehezítheti a nyomozást, hogy a potenciális elkövetők tippeket adhatnak egymásnak az Interneten, így egyre profibb módon követik el a bűncselekményeket.
- Következő ok lehet a nemzetköziség. Előfordulhat, hogy olyan országból követik el a bűncselekményt, ahol nem is büntetendő. Amennyiben ott is büntetik a hatóságok együttműködése nem feltétlen túl olajozott, avagy a két állam nem is kötött jogsegély egyezményt stb.
- A hatékony nyomozás feltétele a különböző szakmák hatékony együttműködése, ami megint csak hiányozhat.
- További probléma lehet, hogy az Internet szolgáltatók – adatvédelmi okokra hivatkozva, vagy hírnévféltés miatt – nem sietnek kiadni az általuk birtokolt fontos adatokat – pl.: adott időpontban adott IP címet ki használta.[58]

A fenti felsorolásból is látszik, hogy jó néhány tényező nehezíti a nyomozók munkáját, s e tényezőkkel szemben igazából csak egy komoly tényező állítható szembe:
A számítógépek, hálózatok, adatbázisok rengeteg adatot tárolnak, némelyiket évekig is akár, s ezen adatok átvizsgálása – ami persze időigényes munka – által olyan esetekben is előrelépés érhető el, amikor látszólag semmilyen nyom nincs.[59]
Azokban az esetekben mikor hagyomány bűncselekményeket követnek el számítógépes környezetben, a hatóságok alkalmazhatják az eddig jól bevált módszereket, ellenben a tényleges számítógépes bűncselekmények esetében, melyeket számítógépes hálózatokon, Interneten követnek el, a hatóságoknak újfajta szemléletmódot, s újfajta módszereket kell alkalmazniuk.

Elsősorban kulcsfontosságú a nyomozók felkészültsége, egy hiányos ismeretekkel rendelkező nyomozó persze segítséget kérhet egy szakértőtől, de ennek ára van. A nyomozás elhúzódik, ami semmiképp sem jó. Amennyiben rendelkezik némi ismerettel, akkor is fennáll annak a veszélye, hogy nem a legcélszerűbb döntést hozza, s így elveszítenek bizonyítékokat.

A szakismeret mellett szükséges a hatóságok együttműködése, mind nemzeti, mind nemzetközi szinten, mint ahogy ezt már korábban többször hangsúlyoztam.

A nyomozás során sokféle bizonyítékot kell összegyűjteniük a hatóságoknak. Digitális bizonyítékokat (számítástechnikai eszközről származó adat) akkor kell beszerezni, ha számítástechnikai eszközön tárolt, feldolgozott, információk a bűncselekményhez kapcsolódnak, s mivel e bűncselekmények jobbára ilyen adatokhoz kapcsolódnak a nyomozás során ilyen adatok beszerzésére kell törekedni.

Peszleg Tibor témával foglalkozó egyik írásában következőképpen csoportosította a digitális bizonyítékokat.

- Digitális dokumentumok: jobbára egyszerű dokumentumok, képek, videók, programok, illetve bármely olyan adat, mely számítástechnikai eszközön tárolható, vagy ilyen eszközzel rögzíthető. Ezen adatok minden számítógép használó számára elérhetőek, nincs szükség szakismeretre megismerésükhöz.

- Digitális nyomok: Olyan adatok, melyek számítógép működése közben keletkeztek, s a felhasználó nem is észleli létrejöttüket, de a rendszer működéséhez elengedhetetlenek – pl.: programok által készített ideiglenes állományok.

A hatóságok számítástechnikai adathordozóról, eszközről adatokat akar szerezni, nyomokat rögzíteni – elsősorban digitális nyomokra vadásznak. Ezen adatok már nem minden felhasználó számára elérhetőek, illetve szakértelem szükséges felkutatásukhoz.

- *N*apló és regisztrációs adatok: egész számítástechnikai rendszerek működése, kommunikációja során keletkező adatokról van szó, melyek tehát nem egyes gépekhez kapcsolhatók.

---

[56] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 726. ó.
[57] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 727. ó.
[34] [58] Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései, Kriminológiai Tanulmányok, 2004. 41., 265-265. ó.
[59] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 726-727. ó.
[35] [60] http://www.police.hu/elemzesek/bunuldozes/int_nyom_001.html (Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés)

a) Naplók (log file-k): rendszer működése közben naplóznak minden tevékenységet – pl.: le – és feltöltések, stb.
b) Regisztrációs adatok: akkor keletkeznek ilyen adatok, mikor egy szolgáltatónál valaki igénybe vesz egy szolgáltatást, s regisztrálja magát.[60]

8.2.2.1. Bizonyítékok és bizonyítási eszközök

A számítógépes bűncselekmények nyomozása, bizonyítása során, főleg a következő bizonyítékokat és bizonyítási eszközöket kell beszerezniük.

1) Tanú, tanúvallomás

A tanúk között a legfontosabb maga a sértett, mivel rengeteg kulcsfontosságú információval rendelkezik, melyek hasznosak lehetnek. Gondolok itt különösen az általa használt jelszavakra, számítógépén tárolt adatokra, általa használt rendszer jellemzőire, általa használt jelszavakat kik ismerhették, esetleg kiknek árulta el azokat.
Esetek egy részében a sértett az egyetlen tanú – pl.: valakinek a személyi számítógépére betörtek, az egyetlen tanú a gép használója.

A fent említett jelentősége miatt fontos, hogy a sértett együttműködjön a hatóságokkal, ami nem feltétlen egyszerű dolog, mivel előfordulhat, hogy a sértett nem észleli a bűncselekményt, vagy egyéb érdekeire tekintettel nem működik együtt.

A sértett mellett célszerű lehet kihallgatni minden olyan személyt, aki az adott rendszert használja, azon dolgozik. Fontos kihallgatni a rendszergazdá(ka)t (számítógépes rendszer esetében), mivel neki(k) több jogosultságuk van, így több információhoz hozzájuthatnak, mint felhasználók. A kihallgatandó egyéb személyek számát mindig az ügy határozza meg, pl.: bankkártyával való visszaélés esetében érdemes kihallgatni a kártyát-elfogadókat is, Interneten elkövetett bűncselekmény esetében az Internet szolgáltatót stb.[61]

2) Szakértők

A különleges szakértelmet igénylő területeken nélkülözhetetlenek a szakértők, ilyen területnek számít a számítástechnika is – a számítógépek, s számítástechnikai ismeretek terjedése mellett is.
A büntető eljárások során kulcsfontosságú szerep jut a szakértők számára. Igaz sajnos sokszor fölöslegesen rendeleik ki őket, s ez akár jelentősen drágíthatja az eljárást, illetve lassítja is. Persze az sem előnyös, ha bárki hozzányúl a bizonyítékokhoz, hisz azzal a bizonyítékok hitelességét veszélyeztethetik, így még mindig jobb, ha képzett ember vizsgálja azokat.
A szakértelmük folytán komoly segítséget nyújthatnak e személyek a nyomozóknak, főleg azáltal, hogy megállapítják pontosan milyen bűncselekmény is történt, milyen adatokat, milyen forrásból kéne beszerezni, illetve az adatok beszerzése során számítógépek lefoglalása után ők vizsgálják meg azokat. A vizsgálat során feltárják az elkövetés módját, folyamatát, de ők adnak véleményt a szoftver jogtisztaságáról, forgalmai értékéről. Mindezen feladatok mellett célszerű bevonni a szakértőket a kihallgatásokba is, ahol célirányos kérdéseikkel segíthetik a kihallgatót.[62]

Súlyuk folytán jelentős felelősség terheli a szakértőket, amennyiben helytelenül határozzák meg a vizsgálandó tényeket, adatokat könnyen tévútra vezethetik a nyomozást.
Meg vannak a maga hátrányai is annak, ha a szakértők ekkora jelentőségre tesznek szert egy eljárásban. Éppen ezért célszerű a nyomozókat tovább képezni e területen is.

3) Tárgyi bizonyítási eszközök

E kategóriába sorolható minden olyan dolog, mely a bizonyítandó tény bizonyítására alkalmas. Így bizonyítási eszközök a hardverek; hamis telefon -, bankkártyák; számítógép segítségével előállított bankjegyek; elektronikus adathordozók (CD, DVD lemezek, winchesterek, pen-drivek stb.), de az elektronikus adat maga bizonyíték, s nem bizonyítási eszköz. Összegezve minden, ami az elkövetés nyomait magán viseli.

---

[36] [61] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 727-728. ó.

[37] [62] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 728. ó.

4) Okirat

Okirat általában minden olyan irat, amely valamely tény, vagy körülmény igazolására állítottak ki és a bizonyítandó tény, körülmény igazolására alkalmas is.
Az irat abban különbözik az okirattól, hogy az előbbi magán viseli a bűncselekmény elkövetésének nyomait, addig az utóbbi kifejezetten bizonyítás céljából készült.

A nyomozás során rengeteg irat gyűjthető össze – pl.: tranzakciók leírása, híváslisták, regisztrált felhasználók listája, stb. – melyek segítségével meghatározható a nyomozás irányai.

A hatóságok legtöbbször megkeresés keretében kérnek információkat az érintettektől. Míg a tartalomszolgáltatóktól a szervereiken tárolt webhelyek; regisztrációs adatok (ezen adatok alapján megállapítható ki az elkövető); dokumentációk; naplók (ezen adatok alapján megállapítható mely gépről lépett föl a világhálóra.); tárhelyek tartalmát illetően kérnek adatokat. Addig a távközlési szolgáltatóktól bekért adatokból megállapítható egy adott IP címet adott pillanatban ki használta. A megkeresések eredményeit okiratként fel lehet használni bizonyítás során.[63]

5) Terhelt vallomása

A terhelt vallomása minden bűncselekmény bizonyítása során fontos bizonyíték. A számítógépes bűncselekmények esetében halmozottan igaz ezen állítás, több okból is.

- Bizonyítékok beszerzése nehezebb, mint a hagyományos bűncselekmények esetében, így fontos lehet a terhelt vallomása;
- Az elkövetők egy része ismeretek szintjén felkészültebb, mint a nyomozók, így a vallomása újabb lehetséges bizonyítékokra irányíthatja a hatóságok figyelmét.

8.2.2.2. Kényszerintézkedések

A továbbiakban érdemes szemügyre venni a legjelentősebb kényszerintézkedéseket is.

1) Házkutatás

A házkutatás célja, hogy tárgyi bizonyítási eszközre leljenek a hatóságok. A házkutatás irányulhat a számítógép felkutatására, de irányulhat egy speciális célra is: elektronikus adatok megtalálására. Ezen adatokat a számítógépes rendszer tárolja, így e kényszerintézkedés helyszíne maga a számítógépes rendszer, melyben megpróbálják fellelni a bizonyítékokként felhasználható adatokat.

2) Lefoglalás

Annak a biztosítása céljából alkalmazható e kényszerintézkedés, hogy a tárgyi bizonyítékok állandóan rendelkezésre álljanak a bizonyítási eljárás során. E kényszerintézkedéssel kapcsolatban több kérdést is meg kell vizsgálni.

Az első kérdés, amire választ kell adni e bűncselekmények kapcsán, hogy mit kell lefoglalni. A bűncselekmények elkövetését legtöbbször elektronikus adatok bizonyítják, tehát ezeket kell lefoglalni, de mivel ezen adatok fizikailag megfoghatatlanok, így az azokat hordozó eszközöket kell lefoglalni.
A lefoglalt adatok között a későbbiekben majd szelektálni kell, mivel sok olyan adatot is lefoglalnak a hordozó eszközök lefoglalásával, melyek nem kapcsolódnak a bűncselekményhez.

A második kérdés a lefoglalás módjára irányul. A lefoglalást úgy kell végrehajtani, hogy egyrészt a lefoglalt bizonyítási eszközök későbbiekben is felhasználhatóak legyenek, másrészt a kényszerintézkedés elszenvedője ne használhassa fel azokat.
A legcélszerűbb lenne a lefoglalás után törölni minden adatot a rendszerből, de ez semmiképp sem alkalmazható, mivel komoly problémákat okozhatna egy ilyen cselekedet – pl.: Internet szolgáltatást nyújtó cég esetében.

---

38 63 http://www.police.hu/elemzesek/bunuldozes/int_nyom_001.html (Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés)

Harmadik kérdés a lefoglalás mértékére irányul. Egyik megoldás az egész számítógép/rendszer (több gépből álló hálózat esetében) lefoglalását eredményezi, míg a második megoldás szerint elégséges csak a megfelelő egység kiemelése is.

Az első módszert támogatók szerint az egész gépet le kell foglalni, s majd a szakértő kiválogatja, mi kell neki, s mi nem.
E megoldást a következő érvekkel támasztják alá: a) számítógép egy egységet alkot, amit nem lehet megbontani, b) a lefoglalást végzők nem tudják eldönteni a helyszínen mit kéne lefoglalni, s mit nem, c) kárt okozhatnak a szakszerűtlen szétszereléssel.[64]

Nézetem szerint viszont elégséges egyes elemek kiemelése. Elégséges a winchesterek, illetve minden egyéb adatrögzítő, hordozó eszköz lefoglalása, mivel ezek tartalmazzák az eljárás szempontjából fontos elektronikus adatokat, így elegendő pusztán ezek lefoglalása.
Nem értek egyet a másik tábor képviselői által felsorakoztatott érvekkel, mivel ha a nyomozók nem értenek a gép szétszereléséhez, vihetnek magukkal egy szakembert, aki majd szétszedi, így nem okozhatnak kárt.
Szükségtelen a számítógép egységére hivatkozva lefoglalni az egész gépet, mivel a már említett adathordozók elvitelével minden szükséges információt megszereztek, így egyben az is lényegtelen, hogy a helyszínen lévő nyomozók tudnak-e szelektálni vagy sem, ha minden adathordozót lefoglalnak, minden adatot megszereztek.

Egy harmadik lehetőségként megoldható, hogy az eredeti adathordozó lefoglalása nélkül hiteles másolatot készítenek a nyomokról, egy speciális eszközsegítségével, s e „fényképet" vizsgálja a szakértő.
E megoldás alkalmazása a terhelt esetében nem célszerű, mivel a szükséges adatokhoz hozzájutnak a hatóságok, de nem akadályozzák meg az elkövetőt az adatok felhasználásában, így e megoldás csak 3. személyekkel szembeni lefoglalás esetében használható, velük szemben viszont a lefoglalásnál enyhébb megoldást jelent az adatok megőrzésére kötelezés.

8.3. Egyéni szint

Mint minden bűnözés esetében, ezen esetben is kulcsfontosságú az egyének és kisebb közösségek (pl.: munkahelyi hálózatok) bűnözéssel szembeni fellépése. E szint fontosságát növeli, hogy hatékony egyéni bűnözéssel szembeni védekezés esetében a magasabb szinteknek már egyszerűbb dolga van, csupán ki kell egészíteni, illetve össze kell hangolnia az egyének és kisebb közösségek védekezési megoldásait. E bűnözés esetén is igaz, hogy az egyének roppant sokat tehetnek saját maguk védelme érdekében.

E fejezetben, akárcsak a többiben, a sokféle megoldás közül csupán néhányat emelnék ki, elsősorban azokat, melyek használatához, üzemeltetéséhez nem szükségeltetik komoly szakértelem, így vélhetőleg az egyszerű felhasználók is alkalmazhatják azokat.
Előre kívánom vetni, hogy e fejezet inkább technikai jellegűbb lesz, az egyes védelmi megoldások bemutatása miatt.
Mind emellett az egyes védelmi megoldások esetében inkább csak tippek adására vállalkozom, felhívom a figyelmet egyes lényeges jelenségekre, s a technikai részletekbe nem megyek bele.

Mielőtt rátérnék az egyes megoldások ismertetésére, érdemes röviden megismerkedni a védelem mögött álló ***számítógép-biztonsággal*** is.

8.3.1. A számítógép-biztonság

E fogalom alatt – *szűkebb értelemben* – az adatok, információk illetéktelen hozzáféréstől való védelme, elsősorban azok titkossága értendő.
Tágabb értelemben, pedig az előbbi titkosság mellett az integritást, elérhetőséget, megbízhatóságot is.
Fontos ismételten kiemelni, hogy a védelem középpontjában a számítógépes adatok állnak, mint a legnagyobb értéket képviselő dolgok.

[3964] Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog, 2001/12., 730-731. ó.
[40] [65] Fekete Zsuzsanna: Az információ biztonság a számítógépes bűnözés tükrében, Főiskolai Figyelő, 2/99, 85. ó.

Az információ értéke miatt, a rendszerek esetében célszerű hangsúlyt fektetni külön is az információvédelemre, mely keretében fontos betartani a következőket: titoktartás (engedély nélkül nem lehet hozzáférni az adatokhoz), adatok sérthetetlensége (tulajdonos engedélye nélkül nem módosíthatóak az adatok), következetesség (folyamatosan az elvárásoknak megfelelően működjön a rendszer), elkülönítés (a rendszer egyes részeinek elérhetőségét különbözőképpen kell szabályozni), felügyelet felállítása.[65]

A megfelelő óvintézkedés(ek) kiválasztása előtt szükséges számba venni a lehetséges sebezhetőségi forrásokat, egyes veszélyforrásokat:

1) Sebezhetőség:
   - Fizikai sebezhetőség,
   - Hardver, szoftver, adathordozók sebezhetősége,
   - Kommunikációs sebezhetőség,
   - Humán sebezhetőség

2) Veszélyforrások:
- Fizikai (tűz, víz, nedvesség, villámlás, rengések, stb.),
- Szándékos károkozás,
- Gondatlanság,
- Hardver hiba, stb.

A megfelelő szintű védelem kialakítása érdekében, jó menedzsment szükséges, mind az egy-, mind a több felhasználós rendszerek esetében. Az egy falhasználós rendszer esetében a felhasználónak célszerű biztonság és védelmi megoldásokat eszközölni (lásd 9.3.2 fejezet), s viszonylagos rendszerességgel ellenőrizni azok állapotát, esetleges frissítések szükségességét.

A több felhasználós rendszerek esetében, pedig külön szakember(eke)t kell alkalmazni a fenti feladatok elvégzésére. Emellett külön írott és jól tervezett, jól átlátható, érintettek által megismerhető biztonság és védelmi politikát kell létrehozni. Elengedhetetlen a pontos feladat és hatáskör elhatárolás, így pontosan lehet majd tudni, ki férhetett hozzá az adott szerverhez mondjuk. Akárcsak az egy felhasználós rendszerek esetében itt is ügyelni kell a fizikai védelemre (ne léphessen be akárki, például egy vezérlőterembe, érdemes beléptető rendszereket felállítani, stb.)

Egy menedzsment feladatai közé tartoznak példálózó jelleggel a következők: naplózás; log file-k ellenőrzése; vírusellenőrzés (ideértve a megfelelő programok telepítését, frissítését is); tűzfalak üzemeltetése; jelszó-menedzsment; rendszeres mentések; stb.[66]

8.3.2. Egyes védelmi megoldások

1) Jelszavak

Számítógépes bűnözés elleni védekezés egyik kulcsfontosságú eleme. A számítógépek védelme érdekében célszerű, hálózatok esetében – felhasználók számára – szükséges is.

Számítógépünk jobb védelme érdekében célszerű a gépet BIOS-ban beállítani, hogy a gép indításkor jelszót kérjen, s annak begépelése nélkül el se induljon, avagy ha magára hagyjunk munkahelyünkön a gépet, tanácsos olyan képernyőkímélőt használata, ami csak akkor áll le, ha begépeljük a jelszót.

Jelszavaink esetében célszerű megfontolni a következőket:
- Többszintű jelszavak alkalmazása (lásd: gép indításakor is jelszót kér, illetve a fiókba belépéshez is);
- Minden rendszerhez külön jelszót alkalmazzunk;
- Időnként változtassuk meg jelszavainkat;
- Jelszavainkat kezeljük bizalmasan, ne adjuk ki azokat másoknak, még ismerősöknek se (pl.: Chat szobákban, fórumokon),

41 66 http://mek.oszk.hu/01200/01280/html/2.08/index.htm (Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, 1-6. ó.)

- Törekedjünk erős, jó jelszavak alkalmazására. A jelszó kitalálásakor érdemes figyelembe venni a következő néhány szempontot:
    - Legyen nehezen kitalálható,
    - Legalább 4-5 karakterből álljon,
    - Véletlenszerűen szerepjenek benne kis és nagy betűk, jelek, számok is – pl.: B45den6V
    - Gyorsan begépelhetőek legyenek, így nehéz kifigyelni mely billentyűket üti le az illető,
    - Kerülni kell olyan jelszavak használatát. Mint saját név, becenév, internetes becenév, telefonszán, stb. Egyszóval bármely közismert információ alkalmazása kerülendő.[67]

A jelszavak egyetlen igazi gyengéje a felhasználók hanyagsága, vagy a rossz jelszóválasztás.

2) Mentések

A mentések során a gépen tárolt adatokról biztonsági másolatot készít a felhasználó. E tevékenység célja az esetlegesen sérült – pl.: támadás következtében – állományok helyreállítása. A mentés céljára tekintettel szintén kulcsfontosságú eszköz.

Különbség tehető:

- **Full backup**: rendszer összes adatát mentik,
- **Incremental backup**: előző mentéshez képest változott adatokat mentik csak,
- **Partial backup**: egyes adatokat, vagy adatcsoportokat mentik,
- **Zero day backup**: rendszer kezdő állapotának mentése.[68]

A mentést célszerű – mentés típusától függően – előre meghatározott időközönként végezni. A mentést elvégezhetjük a számítógépben lévő másik merevlemezre, vagy az adott merevlemez másik partíciójára, fontos adatok esetében jobb külső adathordozóra elvégezni e biztonsági lépést (CD, DVD, pen-drive, gépből kivett merevlemezre stb.), de ez esetben ügyeljünk arra, hogy olyan eszközre írjuk ki, mely várhatóan még a jövőben is kapható lesz.
Különösen fontos adatok, pl.: titkok, esetében célszerű lehet titkosítás eszközéhez nyúlni.

3) Vírusirtó programok

E programok különösen két okból jelentősek:
a) Az elektronikus levelezés elterjedése miatt, gondolok itt a levelek és csatolmányok ellenőrzésére,
b) Egyre több mindent töltünk le az Internetről, vagy egyéb hálózatokról, továbbá a hálózaton töltött idő is megnőtt. A számítógépre így könnyen bejuthatnak mindenféle ártó szándékkal készített programok.

Nevükkel ellentétben a vírusirtók (pl.: Norton Anti-Virus; McAfee stb.) nemcsak vírusokat képesek elpusztítani, hanem – kereső motortól függően – egyéb olyan ártó programokat is, melyek veszélyt jelenthetnek a felhasználóra nézve. Néhány szót érdemes szólni ezen ártó programokról.

- Vírusok: Minden vírus egy olyan programkód, mely önmagukban működésképtelenek, melyeket egy program tartalmazza, s a program futtatásakor aktivizálódnak és elkezdik replikálni magukat. A vírusok hatástalanok. ha nem aktiválják azokat.[69]

- Férgek (Worm): Ellentétben a vírusokkal ezek önálló programok, egyébként más tekintetben hasonlóak a vírusokhoz. Önmagukban nem változtatnak meg programokat, adatokat, de szállíthatnak egyéb károkozó programokat, pl.: vírusokat. Nagyobb potenciális veszélyt jelentenek, mint a vírusok, mivel az utóbbiak lassabban terjednek, s hamarabb kiszúrják azokat a vírusirtók.

[4267] www.rbs2.com/cvict.htm (Ronald B. Standler: Tips for Avoiding Computer Crime)
[43] [68] http://mek.oszk.hu/01200/01280/html/2.08/index.htm (Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, 8. ó.)
[44]

- Trójai falóvak: Olyan kódok, programok, melyeket más programok rejtenek. A trójai falovakat rejtő programok hasznos programoknak látszanak, pont ezért az emberek egy része le is tölti azokat. Amíg a felhasználó azt hiszi, hogy a program az ő utasításait végzi, valójában mással foglalkozik – pl.: adatokat töröl, megváltoztat, stb.

- Bombák: Olyan programkód, melyet valamely más program tartalmaz, s valamilyen feltétel bekövetkeztekor a bombák „robbannak" (vagyis végrehajtanak olyan eljárásokat, melyek nem feladata az adott programnak; pl.: leállítanak programokat, tönkretesznek adatokat, stb.).[70]

- Baktériumok, nyulak: E programok nem okoznak károkat, ellenben feladatuk a számítógép elfoglalása, s olyan szinten leterhelés, hogy az használhatatlanná váljék. E célt úgy érik el, hogy gyorsan sokszorosítják magukat (rendkívül találó e programok elnevezése).

A fenti programok több szempontból is kárt okoznak: egyrészt adatvesztéseket, szoftver meghibásodásokat okozhatnak, avagy túlterhelik a rendszert, oly mértékben, hogy az használhatatlanná válik; másrészt az elpusztításukra fordított erőfeszítések, sok energiát és időt leköthetnek (pl.: egy nagy cég esetében),ami további veszteségeket okozhat (pl.: ez idő alatt szüneteltetnie kell a szolgáltatásait).

Mindenképp célszerű vírusirtó programokat használni, s azokat rendszeresen frissíteni, különösen akkor, mikor egy újfajta gyorsan terjedő vírus válik ismertté.
Helyi hálózatok esetén érdemes figyelem bevenni a következő javaslatokat:

- Vírusvédelmi politika kialakítása,
- Korlátozni kell a vírusok bejutásának lehetőségét (pl.: egyes gépekből ki kell venni a cd/dvd meghajtókat, feltéve, ha nélkülözhetőek),
- Vírusirtók használata
- Alkalmazásokat szerverről kell futtatni, így azok fertőződöttsége könnyen ellenőrizhető, illetve meg is akadályozható.

Az elektronikus levelezés elterjedése miatt érdemes kitérni az e-mail-ek és csatolmányaik kérdésére is. Érdemes megfontolni a következőket: **a)** semmiképp se nyissunk meg *névtelen leveleket*; **b)** soha ne nyissunk meg olyan csatolmányt, mely olyan file-ket tartalmaz, melyek *futtathatóak* – pl.: *.exe file; **c)** olyan csatolmányt se nyissunk meg, mely *dupla kiterjesztéssel* rendelkező file-ket tartalmaz – pl.: *.doc.exe; **d)** üzleti partnereinktől a levelek, dokumentumok hitelességének megállapíthatósága érdekében, kérjük, hogy *elektronikus aláírással* (titkosított karaktersor, mely alapján feltételezhető, hogy küldő titkosította, s melyből kiderül, hogy módosították-e azt illetéktelenek) lássák el azokat.[71]

4) Tűzfalak (firewall)

A tűzfalak (pl.: ZoneAlarm, Sygate pro stb.) nem a számítógép, hálózatok elleni támadások lehetőségét akarják kiküszöbölni, hanem akadályt állítanak a támadás elé, így csökkentik a sikeres betörések esélyét.
Léteznek *külső* és *belső* tűzfalak (előbbi a helyi hálózatot választja el a Világhálótól, míg az utóbbi a helyi hálózat egyes részeit a többitől). [72]

A hackerek sok olyan programok készítenek, melyek az Internetet böngészik olyan gépeket keresve, melyek nyitott (védtelen) porttal csatlakoznak a Világhálózatra. Az ilyen gépekbe könnyen betörhetnek a hackerek és különböző károkat okozhatnak, szélsőséges esetben át is vehetik fölötte az irányítást, s felhasználhatják bűncselekmények elkövetésére.

A tűzfalak bizonyos protokollokat átengednek, bizonyosokat nem. Beállítástól függően, egyes protokollokat csak egyik irányba engedik, vagy bizonyos portokat blokkolni is lehet segítségükkel.

---

45 [69] http://mek.oszk.hu/01200/01280/html/2.08/index.htm (Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, 16. ó.)
[70] http://mek.oszk.hu/01200/01280/html/2.08/index.htm (Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, 17-18 ó.)
4671 www.rbs2.com/cvict.htm (Ronald B. Standler: Tips for Avoiding Computer Crime)
[72] http://mek.oszk.hu/01200/01280/html/2.08/index.htm (Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, 23. ó.)

További jelentősége e programoknak, hogy minden ki és belépést naplóznak, így egy esetleges nyomozás során fontos információkhoz juthatnak a nyomozók.
Különösen azon gépek, hálózatok esetében fontos e program használata, melyek folyamatosan csatlakoznak az Internethez.

Saját tapasztalataim alapján is igazolhatom a vírusirtók és a tűzfalak hatékonyságát is. Előbbire jó példa:
Egy Windows újratelepítés után, voltam annyira figyelmetlen, hogy nem telepítettem föl a vírusirtómat, mielőtt még csatlakoztam volna a Internetre, hogy letöltsek egy programot. 20 perc múlva a számítógép erőteljesen belassult, majd végül szinte használhatatlanul lassú lett, a vírusirtóm tucatjával irtotta a vírusokat, trójai falovakat, kém programokat, de a helyzet nem sokat javult, így végül ismét Windows újratelepítés lett belőle. Másodjára már körültekintőbb voltam, s úgy csatlakoztam a Világhálóra, hogy előtte telepítettem a vírusirtót…a csatlakozás után rögtön fönnakadt a védelmen jó néhány vírus. E példa is jól jelzi a gépekre mennyi káros program akar bejutni.

Utóbbi programnak szintén nap, mint nap hasznát veszem (már jó ideje a ZoneAlarm-t használom), jó néhányan szerettek volna már bejutni a számítógépemre, de a tűzfalnak köszönhetően kudarcot vallott minden eddigi próbálkozásuk.

Végül a védekezéshez még egy hasznos tanács: aki wireless (drót nélküli) hálózatot használ, annak célszerű megpróbálni valamilyen módon leárnyékolni a rendszert, mivel a wireless rádió frekvencia használatán alapszik, ami könnyen lehallgatható, sőt használható is, így illetéktelen személyek könnyedén bejuthatnak rendszerünkbe.

Úgy vélem a fenti néhány egyszerű program használatával, illetve szabályok betartásával viszonylagos védettségre tehet szert bárki. Hangsúlyozni kell, hogy e védettség csak viszonylagos, mivel egy profi elkövető úgy is kijátssza a védelmet, de a kevésbé tapasztaltabbakkal szemben mindenképp használható.

9. Információs társadalom és a számítógépes bűnözés

Az információs társadalom ma még csak a jövő zenéje, igaz történtek, s történnek komoly lépések e társadalom létrehozása érdekében (pl.: e-kormányzat, e-közigazgatás, számítástechnika elterjesztése és hozzá kapcsolódó képzés stb.), de még ha létre is jön egy ilyen társadalom, az semmiképp nem holnap lesz.

E társadalom felé vezető úton a tárgyalt bűnözés jelentősége folyamatosan növekedni fog, s mikor létrejön az információs társadalom a bűncselekmények túlnyomó többségét e bűnözés körébe sorolható bűncselekményeket teszik majd ki.
Kétségtelen, hogy maradnak majd olyan bűncselekmények, melyek nem alakulnak át, vagy nem vesznek ki, tekintettel az emberi faj jellemzőire – pl.: élet és testi épség elleni bűncselekmények. A többség viszont átalakul, s beolvad a számítógépes bűncselekmények közé, vagy eltűnik.
Az információs társadalom rövid, vázlatszerű bemutatását mindenképp indokoltnak tartom a fenti állításom alátámasztása céljából. Az újfajta társadalom jellemzőinek, jellegzetességeinek számbavétele után látható lesz, hogy egy erősen technológia, tudás és információ alapú társadalomban a legnagyobb kincs maga az **információ** (ami a számítástechnikai háttér miatt leginkább elektronikus adat), így a bűncselekmények is ezen érték köré szerveződnek majd, annak valamilyen formában történő megszerzése lesz az elkövetők fő célja.

9.1. Az információs társadalom

Az egyes társadalmi korokat gyakran összekapcsolják a termelési eszközök valamilyen fejlettségi szintjével – pl.: vaskorszak, ipari társadalom, információs társadalom. A társadalmat természetesen nem lehet egy dimenzió, a termelési eszközök, alapján jellemezni, összetettsége miatt.
A jövő társadalmára is többféle elnevezést alkalmaznak, pl.: információs-, cyber-, kommunikációs társadalom stb., igaz mindegyik megnevezés pontatlan, hisz elkövetik azon hibát, hogy egy ismérv alapján írják le a társadalmat (a továbbiakban a legelső megnevezést használom). Fenti elnevezéseket a 70-es években vezették be a posztmodern társadalom jellemzésére.

Az információs társadalomról beszélhetünk, mint poszt-indusztriális, tudásalapú, tanuló, informatizált ipari társadalomról. Pontos meghatározás még máig sem született.[73]
Műszaki oldalról nézve e posztmodern társadalom ismérvei: számítástechnika, távközlés, mikroelektronika rohamos fejlődése és összeolvadása emelhető ki. E társadalom létrejöttének fő alapfeltétele a telekommunikációs bázisú információs infrastruktúra, melynek elérésének alapfeltétele egy információs forradalom.[74]

Az információs társadalom a gazdaság, kultúra és az egész társadalom – alapvetően - az információk gyártására, cseréjére, értékesítésére épül. Egyszerre jelent hatalmas mennyiségű információt, új technológiát, új információ vezérelt gazdaságot, illetve új társadalmat is. Az informatizáltság javítja a termelés szervezettségét is, növeli a technológiai fegyelmet, eredményességet. Hierarchikus rendszerek helyét, az önálló részrendszerek kooperatív rendszere váltja föl.
Mind globális, mind lokális társadalom az új technológia alkalmazásának hatására átalakul és hálózatba szerveződik (eddigi társadalmakkal szemben ez esetben nem beleszületik valaki egy társadalmi csoportba, hanem tudatosan válik az általa választott csoport tagjává).
A hálózatba szerveződés másik előnye, hogy így mindenki aktív tagjává válik a rendszernek és részt vesz az információk gyártásában, forgalmazásában. Harmad részt információs csomópontok alakulnak ki.

Az új társadalom szerkezetét a tudásáramlás, eloszlás fogja meghatározni, melynek alapja az információ, melynek pedig a technológia alkalmazása az alapja. Egyes régiók lemaradhatnak e folyamatban (pl.: adott technológiát nem tudják beszerezni), s kialakulhatnak információ gazdag és információ szegény területek, ami komoly konfliktusokhoz, ellentétekhez vezethet.

Az információs társadalom jellemzői:
- Információt nyersanyagként használják (nem pusztán mennyiségi, hanem minőségi – használati értéke – is fontos tényező),
- Az új technológia hatással van az összes kollektívára és valamennyi egyénre is, átformálja életüket, az információ társadalom az élet összes területére behatol,
- Tudás és információ fölhalmozás jellemzi (a felhalmozott tudást mind tudományos területen, mind nem tudományos területen – pl.: közigazgatás - alkalmazzák),
- Információ mobilitása (könnyen mozgatható a rendszeren belül),
- A rendszer rendkívül rugalmas,
- Integrált rendszer,
- Decentralizáltság,
- Demokratikus rendszer, mivel bárki hozzájuthat az információhoz, technológiához,

Az információs társadalom ***alapelvei***: **a)** élethosszig tanulás, **b)** globális szabadverseny, **c)** közös célokért együttes fellépés, **d)** demokrácia, **e)** civil kontroll.[75]

Bármennyire is tökéletesnek is tűnik e társadalom, sok problémát, konfliktust tartogat.
- Egyrészt a rengeteg információ közötti kiigazodáshoz szakemberek kellenek, akik szerepüknél fogva túl nagy hatalomra tehetnek szert. Ugyanúgy túl nagy hatalomhoz vezethet a sok információ birtoklása is, könnyen vissza lehet élni e hatalommal.
- Az informatizáltság következtében rengeteg munkanélküli ember lesz, akik egyben informatika terén képzettek, így könnyen a bűnözést választhatják, mint járható utat, hiszen egy információ és technológia alapú társadalomban egy ilyen téren képzett ember könnyen visszaélhet tudásával.
- Szintén az informatizáltság következtében csökken az értelmes munkával töltött idő, az emberek szórakozás végett, vagy frusztráltság miatt is elkövethetnek bűncselekményeket.
- Az elkövetőket segíti a decentralizáltság, s a hierarchikusrendszer hiánya, információk mozgékonysága, mivel így sokkal nehezebb nyomon követni információk, adatok mozgását. Nehezíti a felderítést.

---

47 [73] http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/FarkasJelmeletek.htm (Dr. Farkas János: Elméletek az információs társadalomról)
[74] http://www.bibl.u-szeged.hu/inf/szakdoli/2004/seredine/htm/elmeleti_megkozelites.htm (Az információs társadalom)
4875 http://www.bibl.u-szeged.hu/inf/szakdoli/2004/seredine/htm/elmeleti_megkozelites.htm (Az információs társadalom)

- További bűncselekmény elkövetési ok lehet az egyes területek közötti információ mennyiségbeli különbség, az információ éhség könnyen motiválhat az embereket, hogy illegális úton szerezzék meg a szükséges információkat.

A rendszer egy ördögi kör is egyben, mivel ahhoz, hogy komoly tudást halmozzon föl valaki - így komoly hatalomra tegyen szert -, ahhoz sok információra van szüksége. Sokaknak viszont nincs munkájuk, így pénzük sem, tehát az információ megszerzéséhez szükséges technikát sem tudják beszerezni, még ha azok kezeléséhez szükséges szakismerettel rendelkeznek is. Így marad az eszközök beszerzésének illegális módja – a lopás.
Az információk beszerzése két előfeltételének (technika, tudás) biztosítása után, sokkal egyszerűbb az információkat illegális úton megszerezni, hisz az információs társadalom amúgy is behatol az élet minden területére, ebből következik, hogy rendkívül sok és sokféle információt tárol a rendszer.

Megfelelő szakismeret és technikai felszereltség mellett bármilyen és bármennyi információ, így tudás, tehát hatalom megszerezhető (melyekkel kereskedni is lehet a későbbiekben, így pénzhez juthat, vagy még értékesebb információkra cserélheti azokat), mivel aki sok információval rendelkezik, irányíthatja a társadalmat.

Sokak számára nyilván csábító lesz majd egy ilyen helyzet. Éppen ezért lesz kulcsfontosságú kérdés a rendszer megfelelő védelme. A számítógépes bűnözéssel együtt az ellen fellépés és védekezés kérdése is ugyanúgy felértékelődik majd.

Az említett okok miatt várható nézetem szerint a bűnözés jelentős módosulása egy ilyen társadalomban, a számítógépes bűnözés előretörése által. Miután az információs társadalomban az elkövetők az információk megszerzésére koncentrálnak, melyek megszerzéséhez az egyes számítógépes hálózatokat használhatják föl, így az elkövetők többsége vagy a technikai eszközök beszerzésére fog „szakosodni", avagy az információk beszerzésére (elsősorban számítógépes bűncselekmények elkövetésével), megint mások azok terjesztésére szakosodnak majd, így kialakul az elkövetők között egy munka és feladat megosztás.
Hangsúlyoznom kell, hogy jelenleg a mai társadalmak tekintetében még nem beszélhetünk információs társadalmakról (vagy legalábbis csak részben), így a fenti rövid fejtegetésem is csak egy feltevés, egy jövőbeli társadalom lehetséges veszélyeiről.

10. Konklúziók

A XX. század egyik jelentős találmánya a számítógép volt, ami nagyban megkönnyítette az emberek életét, s mára már szinte nélkülözhetetlen részévé vált annak. A társadalom minden részében használják e technológiai vívmányt.
Minden technikai fejlődének és eszköznek meg van a maga hátránya is, a számítógép elterjedésével a bűnelkövetők is rádöbbentek az eszköz előnyeire, s a benne rejlő lehetőségekre. Napjainkra egyre inkább növekszik ezen eszközök segítségével elkövetett bűncselekmények száma.

Kezdetekben még csak ritkán fordultak elő e bűncselekmények, s nem is okoztak akkora kárt, mint egyéb bűnözési típusok, ezért se a hatóságok, se a tudományos élet nem törődött túlzottan a jelenséggel. Későbbiekben egyre inkább elkezdtek szaporodni az elkövetések – köszönhetően annak, hogy gyors ütembe kezdtek elterjedni a számítógépek, s már nemcsak tudományos, hanem gazdasági, üzleti célokra is használták azokat. Az üzleti élet belépésével az elkövetők kis erőfeszítések árán, hatalmas összegekre tehettek szert, vagy komoly károkat is okozhattak. Kezdetekben szoftvereket másoltak, idővel egyre több szakértő került az elkövetők közé, s mára már egyre súlyosabb bűncselekményeket követnek el a számítógép segítségével.

E jelenség köszönhetően az Internet elterjedésének, melynek következtében a számítógépes bűnözés az egész világon elterjedt jelenséggé vált. Manapság kellő szakértelemmel és egy Internet hozzáféréssel rendelkező számítógép segítségével hatalmas károkat lehet másoknak okozni, rendkívül gyorsan.

A jelenség jellemzőinek számbavételekor láthattuk, hogy jelen kor egyik veszélyes bűnözési formájával állunk szemben, veszélyességének egyik legfőbb forrása, hogy igazából bárki lehet elkövető, csak a szükséges technikai felszereltség (ami manapság már viszonylag olcsón beszerezhető) és némi szaktudás szükségeltetik, szemben mondjuk egyes hagyományos bűncselekményekhez, amelyekben akár erős fizikum, drága felszerelések kellenek. Tovább növeli a jelenség veszélyességét, hogy a legtöbb államban bizonytalan a jogi szabályozottság, főleg az legfőbb elkövetési területé (Internet), így a kiskapukat, joghézagokat kihasználva könnyebben tevékenykedhetnek az elkövetők.

Jó lehet, e bűncselekmények, számszerűleg messze alulmarad a többi bűncselekménnyel szemben, ellenben az okozott károk könnyen felveszik a versenyt az egyéb bűncselekmények által okozott károk mértékével.

Leszögezhetjük, hogy ezeknek a bűncselekményeknek a jó részük megelőzhető lenne, ha az emberek komolyabban vennék a számítógépes bűnözés veszélyeit, s megtennének minden szükséges óvintézkedést, persze, mint a legtöbb védelmi rendszernek ennek is az ember a legtöbb hibát hordozó eleme. Az emberek egy része könnyelműségből, lustaságból, esetleg képzetlenség folytán nem fektet komoly hangsúlyt védelmi megoldások alkalmazására. Pontosan a fentiekre tekintettel a számítógépes bűnözés elleni fellépés hangsúlyos részét kéne képezni annak, hogy az embereket figyelmét rendszeresen felhívnák a veszélyre, illetve megismertetnék velük a védekezés lehetőségeit, módszereit.

Mindannyian tudjuk, hogy bármilyen védelmi rendszert is építünk ki tökéletes biztonság nincs. Ráadásul az informatika, számítástechnika fiatal és gyorsan fejlődő szakterület, amin belül gyakran inkább a funkcionalitás érvényesül, mintsem a védekezés.

Szerencsére a nemzetközi és szupranacionális szervezetek viszonylag korán felismerték e jelenségben rejlő veszélyeket, s lépéseket tettek a nemzeti szabályozások harmonizációja felé, valamint sürgették, sürgetik a nemzeti fellépések összehangolását. Legjelentősebb szervezetekként megemlíthetőek az OECD, EU, ET, de az ENSZ, Interpol szerepe sem elhanyagolható. Ki kell emelnem, hogy a nemzetközi összefogás még mindig nem terjed ki minden területre, s a rendelkezésre álló eszközök sem mindig hatásosak, de maga a tény, hogy létezik egyfajta nemzetközi összefogás, mindenképp bíztató.

Ami a jövőt illeti, ismételten hangsúlyozni szeretném, hogy az információs társadalom térhódításával (ami nem is biztos, hogy annyira távoli jövő) együtt a számítógépes bűnözés jelentősége s egyben veszélye is csak nőni fog. Az információs társadalom jövőképe a tudástársadalom. Ez már egy új minőségű, tudásközpontú, hálózati jellegű, a globális-lokális digitális különbözőségeket csökkentő társadalom. Rendkívül fontos szerepe lesz az információnak, és a számítástechnikának. Egy információs társadalomban, ahol mindenki a mainál sokkal jobban függ a számítógépektől, számítógépes rendszerektől, s azok működőképességétől, illetve ahol az információ s annak biztonságos megőrzése társadalmilag fontos tényező, elég komoly veszélyt jelent e bűnözés. Miután egy olyan világban, ahol mindenki rendelkezik számítógéppel és csatlakozik egy hálózatra, bárki számítógépes bűncselekmény(ek) sértettévé válhat, illetve e bűncselekmények hatásai is nagyobbak lesznek a maiénál.

Természetesen a mai társadalmak tekintetében még nem beszélhetünk a dolgozat korábbi részében bemutatott információs társadalmakról, de a fejlett országok egyértelmű lépéseket tesznek annak irányába. Gondoljunk csak az e-közigazgatás, e-kormányzat intézményeire, vagy az elektronikus megoldások preferálására - pl.: elektronikus banki szolgáltatások, Interneten keresztül vásárlás, általában az e-kereskedelem jelensége stb. Sőt manapság már az intelligens, számítógép vezérelt házak sem tartoznak a tudományos fantasztikum világába, melyek ráadásul az Internetre is felcsatlakozhatnak, s ebben az esetben már egy egész épület válhat támadások célpontjává.

Az előbb felsorolt tényezők mind fölvetik a védelem és a védekezés kérdéskörét. Ráadásul egy információs társadalomban különösen fontos a hatékony védelem, sőt már napjainkban is, különösen a tényt figyelembe véve, hogy egyre inkább elektronikus adatbázisokban tárolják az emberek, intézmények, szervezetek az általuk használt adatokat, információkat, melyek feltörésével bő információ forráshoz juthat az elkövető, amellyel korlátlanul visszaélhet.

10.1. Új kihívás a jogalkotó, jogalkalmazók számára

Az újfajta bűnözés újfajta szemléletmódot és leginkább komoly felkészültséget követel mind a törvényhozótól, mind a jogalkalmazóktól. Minél inkább elterjed e technikai eszköz és azzal együtt az Internet, annál több probléma és jelenleg nehezen megválaszolható kérdés fog a felszínre kerülni. Gondoljunk csak például az Internet jog kérdésére, anyagi, eljárásjogi kérdésekre, büntetőjog terén e területre vonatkozó bűncselekmények esetleges újraszabályozása, azok bővítése, stb.

A jogalkotónak alapos elemzéseket kell folytatnia az egyes jogszabályok megalkotása előtt, rendelkeznie kell megfelelő számítástechnikai ismeretekkel (vagy legalábbis ilyen szakértőket kell segítségül hívnia), mivel elengedhetetlen, hogy pontos ismeretekkel rendelkezzen a szabályozandó területről. Feltétlenül tekintettel kell lennie a nemzetközi megoldásokra, egyes

szervezetek ajánlásaira. Ösztönöznie kell a jogalkalmazó szerveket más államok szerveivel való együttműködésre.

Talán még a jogalkotónál is nagyobb felkészültséget igényel e jelenség a jogalkalmazóktól. Hiába kielégítő a jogi szabályozás, ha az azt alkalmazók nem képesek végrehajtani megfelelő tudás hiányában. A nyomozó szerveket mind technikailag (pl.: modern, gyors számítógépek) és e területre vonatkozó ismeretek terén is meg kell erősíteni, a hatékonyság növelése érdekében

Nélkülözhetetlen az ügyészek és bírák felkészítése is. Egyrészt munkájukat könnyíti meg az informatika (pl.: gyorsan hozzájuthatnak a szükséges információkhoz), másrészt kellő ismeretek birtokában könnyebben boldogulnak majd a számítógépes bűncselekmények terén. Számukra különösen fontos, hogy naprakész információkkal rendelkezzenek, pl.: ne kelljen külön szakértőt kirendelni annak megállapításához, hogy az adott szoftverek vajon ingyenesen hozzáférhetőek-e, vagy illegálisan használja az elkövető azokat, stb. A bíróságok szerepe elengedhetetlen lehet a jogszabályok értelmezés terén is, így már csak ezért is szükséges a folyamatos továbbképzés.

Végezetül megállapíthatjuk, hogy a számítógépes bűnözés napjaink egyik komoly problémája, s a számítógépes rendszerek, adatátviteli technikák fejlődésével a probléma csak súlyosabb lesz. A probléma mindenképpen határozott fellépést igényel. A fellépésnek elsősorban nemzetközi szinten kell zajlania, hisz egy nemzetközi bűnözés ellen csak nemzetközi szinten lehet hatékonyan fellépni, de hangsúlyozni kell, hogy e fellépés nem lehet pusztán büntetőjogi, mivel minden bűnözésnek meg van a maga társadalmi gyökere, s ezt kell megpróbálni felszámolni.

Felhasznált irodalom

Bacskó László: Bûnözés az Interneten, http://iroga.hu/internet&politika/bacsko.html
Balogh Zsolt György: Jogi informatika, Dialóg Campus Kiadó, Budapest-Pécs, 1998.
Carter, L. David: Computer Crime Categories: How Techno-criminals Operate, http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc124.html
Dravecz Tibor - Párkányi Balázs: Hogyan védjük hálózatra kötött számítógépes rendszereinket?, http://mek.oszk.hu/01200/01280/html/2.08/index.html
Farkas János: Elméletek az információs társadalomról, http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/FarkasJelmeletek.html
Fekete Zsuzsanna: Az információbiztonság a számítógépes bűnözés tükrében, Főiskolai Figyelő 1999/2,
Greek, Cecil: Computer crime, http://www.fsu.edu/~crimdo/TA/hao/computer%20crime2.htm
http://cse.stanford.edu/class/cs201/projects-98-99/computer-crime/definition.html
http://hu.wikipedia.org/wiki/Számítógép;
http://larix.emk.nyme.hu/teka/biblio/SzamitastechnikaAlapjai/A/A1.htm
http://www.bibl.u-szeged.hu/inf/szakdoli/2004/seredine/htm/elmeleti_megkozelites.html
http://www.bm.hu/proba/xforum.nsf/3d525835ae5a397fc1256fe3002bbd71/0B0DD172C66279EEC1256970003E99BE?OpenDocument
http://www.cybercrime.gov/flurySent.htm
http://www.cybercrime.gov/ivanovSent.htm
http://www.cybercrime.gov/mantovaniPlea.htm
http://www.cybercrime.gov/Osowski_TangSent.htm
http://www.cybercrime.gov/sabathiaPlea.htm
http://www.freeweb.hu/gaudy/szakdolgq.html
http://www.scit.wlv.ac.uk/~cm1988/CP3349%20SLAPA/computer_crime.html
http://www.scit.wlv.ac.uk/~cm1988/CP3349%20SLAPA/computer_crime.htm
http://www.scitech.mtesz.hu/10kiraly/index.html
http://www.scitech.mtesz.hu/10kiraly/kiraly_3.html
Kunos Imre: A számítógépes bűnözés, Belügyi szemle 1999/11
Laczi Beáta: A számítógép és a büntetőjog, Magyar Jog, 2001/3
Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései, Magyar Jog 2001/12
Mizrach, Steven: Létezik-e „hackeretika” a 90-es években, Replika 2000/41-42
Nagy Zoltán: A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról, Belügyi Szemle, 1999/11
Nagy Zoltán: Az informatikai bűncselekmények kriminológiai aspektusai, Ferenc Zoltán emlékkönyv 2004.
Nagy Zoltán: Informatikai bűncselekmények, Magyar Tudomány 2001/8
Nagy Zotán: Konferencia az információtechnikai bűnözésről, Magyar jog 40. 1993/2
Papp Péter: Etikus Hacking, Belügyi Szemle 2022/11-12
Parker, Donn: Automated crime, www.blacksheepnetworks.com/security/info/misc/autocrime1.htm
Parti Katalin: A számítógépes bűnözés és az internet, Kriminológiai Tanulmányok 2003.40
Parti Katalin: Az internetes bűncselekmények nyomozásának egyes kérdései, Kriminológiai Tanulmányok, 2004. 41
Peszleg Tibor: Interneten, számítógépen történő nyomrögzítés, http://www.police.hu/elemzesek/bunuldozes/int_nyom_001.html
Quirk, Matthew: The web police, http://www.theatlantic.com/doc/200605/chinese-internet
Sieber, Ulrich: A számítógépes bűnözés és más bűncselekmények az információtechnika területén, Magyar Jog 1993/1
Sieber, Ulrich: Legal Aspects of Computer-Related Crime in the Information Society (1998), http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html
Siegler Eszter: A számítógéppel kapcsolatos és a számítógépes bűncselekmények, Magyar Jog 1997/12
Standler, B. Ronald: Tips for Avoiding Computer Crime, www.rbs2.com/cvict.html
Szentgyörgyi Zsuzsa: Mibe kerül az e-bűnözés?, http://www.nol.hu/cikk/375750/
Szentkuti Dániel - Szűts Márton: Az Internet és a büntetőjogi felelősség egyes kérdései, http://jesz.ajk.elte.hu/szentkuti15.html
Tarr Dániel: Az internet mítosz, http://www.freeweb.hu/tarrdaniel/documents/Transzhumanizmus/internetmitosz.html
Varga Balázs: Informatikai bűncselekmények, http://www.jogiforum.hu/publikaciok/127