7. SZÁMÍTÓGÉPES BŰNCSELEKMÉNYEK ÉS AZ ELLENÜK VALÓ VÉDEKEZÉS

Az informatikai védelemmel kapcsolatban elengedhetetlen hogy a számítógépes bűncselekmények is szóba kerüljenek. A két fogalom szoros kapcsolatban áll egymással, hiszen a számítástechnika elterjedése magával hozta a számítógépes deliktumokat és ugyanakkor az informatika biztonság és- védelem kialakítására való igényt is.

Először az informatikai jog, mint a jogtudomány egyik ága kerül bemutatásra, mint a számítógépes környezetben elkövetett bűncselekmények alapja. Majd az egyik legdinamikusabban fejlődő, jelenleg nem kizárólag csak a nyomozó hatóságok, hanem a nemzetek és nemzetközi szervezetek számára kiemelt problémát okozó deliktum, az informatikai bűnözés rövid ismertetése következik.

1.1. Az informatikai jog értelmezése.

Az **informatika önálló tudományág**, amely az adatok rögzítésével, kezelésével, rendszerezésével, továbbításával foglalkozik. Az informatika összefügg a számítástechnikával olyannyira, hogy a mindennapi szóhasználatban keveredik is vele. Ezt a tevékenységét főként számítógépeken végzi:

- elméleti úton azáltal, hogy módszereket, modelleket, formalizmusokat dolgoz ki a számítógépek készítéséhez és működtetéséhez;
- mérnöki tevékenységgel úgy, hogy számítógépeket készít, illetve azokhoz elektronikai eszközöket alkot (hardver);
- rendszertervezéssel és - készítéssel azáltal, hogy a számítógépek működtető eszközeit hozza létre, illetve azokat működteti (szoftver);
- alkalmazza a számítógépet azáltal, hogy különböző feladatok elvégzésére alkalmassá teszi, például: orvosi alkalmazások, kereskedelmi rendszerek, nyilvántartások stb.

Egy másik megfogalmazás szerint az informatikai jog azon **tudományos nézetek összessége**, amelyek a különböző eszközökkel és módszerekkel, de mindenekelőtt a számítógéppel megvalósított információ-kezelésre vonatkoznak.

A XX. század végén megjelent jogi informatika fogalmáról elmondható, hogy az a jogi élettel kapcsolatos információknak, a különböző eszközökkel és módszerekkel, de mindenekelőtt a számítógéppel megvalósított és kezelésére vonatkozó tudományos nézetek összessége. Olyan területeket foglal magába, ahol fontos az információkezelés. Tehát a jogi informatika az információáramlás szabályozásával foglalkozik. A jogi informatika az élet egészét érintő fogalom, hiszen átfogja az élet politikai, társadalmi, gazdasági, kulturális és más szféráit.

A **jogi informatika** fogalmának meghatározásaként nem tévedünk, ha kimondjuk, hogy az nem más, mint a jogi élettel kapcsolatos információk - különböző eszközökkel és módszerekkel, de mindenekelőtt a számítógéppel megvalósított - kezelésre vonatkozó **tudományos nézetek összessége.** A jogi informatika fogalmának meghatározásából következik az is, hogy párhuzamos a büntető joggal és azon belül is az informatikai bűnözéssel.

7.2. A számítógépes bűncselekmények fogalma és jellemzői.

A számítógépes bűncselekmények megjelenése egyidős a számítógépek megjelenésével. Már a XX. század 50-es, 60-as éveiben is követtek el ilyen típusú bűncselekményeket, mégis a köztudatban csak az utóbbi évtizedekben vált ismertté a számítógépek és az internet térhódításával.

7.2.1. Alapfogalmak

A számítógépes bűncselekményekkel kapcsolatos alapfogalmakról első fontos dokumentumban, az OECD[1] 1983-85-ös iránymutatásában esett szó. Ez az iránymutatás, amely öt alrendszerbe rendezte a **számítógépes bűncselekmények**et alkalmazta az alábbi kifejezéseket:

- információlopás;
- számítógépes szabotázs;
- az adatok tisztességtelen manipulálása vagy megváltoztatása;
- jogosulatlan használat;
- jogosulatlan hozzáférés.

Az Európa Tanács (ET) 1989. szeptember 13-án kibocsátott ajánlása a számítógépes-környezetben elkövetett bűncselekményekről szóló ET 9(89). számú ajánlásában volt található a számítógépes bűncselekményekről egy, ún. minimális (minimum), és egy fakultatívnak nevezett lista, amely újabb fogalmakat vezetett be.

Az ET **minimális lista** azokat a bűncselekményeket tartalmazza, amelyeket az ET a tagállamoknak büntetendővé nyilvánítását ajánlja. Ilyenek:

- a számítógépes csalás;
- a számítógépes hamisítás;
- a számítógépes programokban vagy adatokban történő károkozás;
- a számítógépes szabotázs;
- a jogosulatlan hozzáférés;
- a jogellenes behatolás, amely a számítástechnikai rendszerbe vagy a hálózatba történő illegális bejutás a biztonsági intézkedések révén;
- a jogellenes titokszerzés;
- a védett számítógépes programok jogellenes másolása;
- a félvezető topográfiák jogellenes reprodukciója.

Az ET **fakultatív lista** azokat a bűncselekményeket tartalmazza, amelyekben az ET nem tudott állást foglalni a büntetendővé nyilvánítással kapcsolatban. Ezek:

- a számítógépes adat vagy számítógépes program megváltoztatása;
- a számítógépes kémkedés;
- a számítógép jogosulatlan használata;
- a védett számítógépes program jogosulatlan használata.

[1] Gazdasági Együttműködési és Fejlesztési Szervezet (*Organisation for Economic Co-operation and Development)*

A 2011 novemberében, Budapesten aláírt, és Magyarországon 2004-ben kihirdetett Egyezmény számítástechnikai bűnözésről újfent kibővítette a számítógépes bűncselekményekkel kapcsolatos fogalomrendszert.[2]

Bár már az Egyezmény előtt is az államok felismerték a számítógépes bűncselekmények elszaporodását, veszélyét, különös tekintettel a gyermekpornográfia, a szerzői jogok megsértése és a csalások számítástechnikai környezetben történő elszaporodására. Az Egyezmény alapvető célja az ilyen típusú bűncselekményekkel kapcsolatos közös büntetőpolitika kialakítása – a megfelelő jogszabályi háttér és nemzetközi együttműködés megteremtésével – a társadalom védelme.

Az Egyezményben elismerték és rögzítették azt is, hogy különféle információk (szöveg, kép hang) számokkal kódolt és így számítógépekkel olvasható formába való átalakítása (digitalizáció) és az élet, szinte minden területét (termelés, fogyasztás, szolgáltatás, kutatás, kommunikáció, stb.) csúcstechnikai színvonalú információ-feldogozó eszközökkel történő tevékenység (informatika) elterjedése egy új típusú bűncselekmény megjelenését és veszélyét is magában hordozza. Ez is felvetette egy gyors és hatékony nemzetközi együttműködés minél előbbi megvalósítását, hogy a számítógépes környezetben elkövetett bűntetteket, bűncselekményeket (deliktumokat) jogszabályi keretek között szorítsák vissza. Annál is inkább, mivel az informatikai eszközök és rendszerek veszélyeztetik mind az állami, mind pedig a magánszektort.

Az Egyezmény preambulumában lefektették – többek között – hogy az aláíró államok részéről szükség van egy közös büntetőpolitika kialakítására. Felismerték, hogy olyan mértékben nőtt a társadalomra a számítástechnikai eszközökkel elkövetett bűntények száma, amely azonnali reagálást tesz szükségessé.

Szükségesnek ítélték egy alapfogalmakat tartalmazó keret meghatározását is, hogy definiálni lehessen az olyan jellegű bűncselekményeket, amelyek elkövetési módja és eszköze folyamatosan változik. Az Egyezményben meghatározták – többek között és mindenek előtt – a számítástechnikai rendszer és a számítástechnikai adat fogalmát is.

S**zámítástechnikai rendszer** minden olyan eszköz, illetve egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelynek egy vagy több eleme egy adott programnak megfelelően adatok automatikus feldolgozását végzi.[3]

Számítástechnikai adat a tényeknek, információknak, illetve fogalmaknak minden olyan formában való megjelenése, mely számítástechnikai feldolgozásra alkalmas, ideértve azon programot is, mely valamely funkciónak a számítástechnikai rendszer által való végrehajtását biztosítja.[4]

A számítógép és az internet mind a gazdasági-, pénzügyi életben, mind pedig a magánszférában egyre fontosabb szerepet tölt be. A papír alapú és a személyes hivatali ügyintézést egyre inkább felváltja az e-ügyintézés. Ez megkönnyíti és meggyorsítja mind az ügyfél, mind a hatóság részéről az adott ügy intézését, dokumentálását és kezelését. Ugyanakkor a bűnözői oldalon megjelent az igény a különböző adatok (személyes adatok,

---

[2] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

[3] Számítástechnikai bűnözésről szóló egyezmény. Első rész. Értelmező rendelkezések. 1. Cikk a) pont

[4] Számítástechnikai bűnözésről szóló egyezmény. Első rész. Értelmező rendelkezések. 1. Cikk b) pont

felhasználónevek, jelszók, PIN és más hozzáférési kódok, stb.) megismerésére és megszerzésére.

A különböző szakirodalmak nem egységesek az informatikai-, információs-, számítógépes-, csúcstechnikai-, csúcstechnológiai- (high-tech), vagy éppen a számítógépes fogalmak (pl. cyber, kiber) használata tekintetében a számítógépes környezetben elkövetett bűncselekmények vonatkozásában. Úgy vélem, hogy leghelyesebb a számítógépes bűncselekmény vagy a számítógépes környezetben elkövetett bűncselekmény elnevezés használata.

Fentiekre is tekintettel, végül is, mit értünk a **számítógépes bűncselekmény** alatt?

A fogalom pontos meghatározását a szakirodalomban sem találjuk meg. Tágabb értelemben minden olyan deliktum minősülhet informatikai bűncselekménynek, amelyet bármilyen, az informatikában használt eszközzel, vagy eszközzel kapcsolatban követnek el. Szűkebb értelemben a számítógépes bűncselekmény a számítástechnikai eszközre és/vagy adatra irányuló vagy azzal elkövetett támadást jelenti.

A fogalom könnyebb megértéséhez a következő **szempontok** nyújtanak segítséget:

- Az informatikai bűncselekmény társadalomra veszélyes, jogellenes magatartás, amelyben a számítógépnek vagy a számítástechnikának kiemelt szerepe van.
- Az informatikai bűncselekmények felderítéséhez, a nyomozások lefolytatásához, valamint a büntetőeljárás során mind az ügyészi, mind pedig a bírói szakban elengedhetetlen a számítástechnika ismerete.
- Számítástechnikai bűntett vagy bűncselekmény mindaz a cselekmény, amely közvetlenül vagy közvetetten kapcsolatban van a számítástechnikai rendszerbe történő behatolással.

Fentiek figyelembe vételével kapcsolatban szükséges azt is leszögezni, hogy a technika gyors fejlődésének köszönhetően már nem csak a szó szerint vett számítógépekre (számítógépekkel) követhetnek el bűncselekményt, hanem a különböző kommunikációs eszközökre (eszközökkel) és berendezésekre (berendezésekkel) is irányulhat, (megvalósulhat) ez a cselekmény.

E fejezetben gyakran használt, alábbiakban felsorolt alapfogalmak ismertetése és megismerése az anyag könnyebb elsajátítását teheti lehetővé.

Az **informatika** a számítógéppel támogatott információs rendszerek strukturális és dinamikus vizsgálatával, az információk keletkezésével, hasznosításával és továbbításával foglalkozó tudomány.

Az **informatikai rendszer** a hardver és szoftver elemek kombinációjából álló rendszer, amely az adat-, illetve az információfeldolgozás különböző feladatainak végrehajtására szolgál.

Az **informatikai biztonság** fogalma alatt az informatikai rendszer olyan állapotát kell érteni, amelyben a fenyegető tényezők miatti kockázatokat ellenintézkedésekkel az elviselhető mértékűre csökkentették.

Az **informatikai technológia** az informatikai rendszerekkel kapcsolatos eszközök, módszerek és eljárások összessége.

Az **internet** olyan globális számítógépes hálózatok összessége, amely az „internet protokoll” (IP) révén felhasználók milliárdjait kapcsolja össze és teszi lehetővé olyan elosztott rendszerek működését, mint a www (World Wide Web). Az internet kapcsolja össze a kisebb

és nagyobb számítógépeket, ami által kialakul az úgynevezett kibertér.[5] A **kibertér** (cyberspace) nem más, mint a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben. A kifejezést William Gibson alkotta meg Neuromancer című regényében, amelyben a globális internet társadalmát vetíti előre."[6] Valóban az internet és a számítógép terjedése, népszerűsége miatt valamennyi felhasználó egy új típusú veszélyforrással találta és találja magát szembe, amellyel kapcsolatban hosszú időn keresztül szinte semmilyen szabályozás, az elkövetőkkel szembeni igazi szankció nem létezett.[7]

Az informatikai bűncselekmények elkövetése jellemzően az információs társadalomban történhet. Az **információs társadalom** az a társadalom, amely számára az információ előállítása, elosztása, terjesztése, használata és kezelése jelentős gazdasági, politikai és kulturális tevékenység. Ennek a társadalomtípusnak a sajátossága az információ-technológia központi szerepe a termelésben, a gazdaságban és általában a társadalomban. Az információs társadalmat az ipari társadalom örökösének is tekintik.[8]

Az internet megjelenésével nemcsak az adat-és információtárolás, áramlás, közlés vált gyorsabbá, hanem azok jogosulatlan megismerésére való törekvés, az azok „sérelmére" elkövetett támadások, visszaélések is elszaporodtak, mindennapivá váltak. Megjegyzem, hogy bár korábban a papír alapon tárolt információk esetében sokkal nagyobb volt az esély arra, hogy az idő múlásával használhatatlanná váljanak, viszont kisebb volt az esélye azok jogosulatlan megismerésének is.

7.2.2. A számítógépes bűncselekmények osztályozása

A számítógépes bűncselekmények részletes ismertetése előtt elmondható, hogy az internet és a számítógép elterjedésének köszönhetően olyan helyzet alakult ki, amely gyors fejlődésének köszönhetően közvetlenül is veszélyezteti a társadalmat, a nemzetgazdaságot, az államok nemzetbiztonságát, a pénzügyi életet és a magánélet szentségét (a természetes személlyel kapcsolatba hozható adat, az adatból levonható következtetés miatt) és a különböző informatikai támadásokkal elképzelhetetlen károkat okozhat.

Az **informatikai támadások** megnyilvánulhatnak:

- a számítógépeken vagy az informatikai eszközökön tárolt dokumentumok bizalmasságának vagy hitelességének megsértésében;
- internetes oldalak illegális megváltoztatásában;
- támadás rosszindulatú programokkal (malware), vírusokkal;
- Dos (Denial of Service) támadásban, vagyis az internetes oldalak szolgáltatásainak túlterheléses támadásával;

---

[5] http://hu.wikipedia.org/wiki/Internet (letöltve: 2014.09.04.)
[6] http://www.kfki.hu/~cheminfo/hun/olvaso/lexikon/c.html
[7] Ilyen példa lehet a 2000-es évek egyik legismertebb számítástechnikai bűncselekménye az Elender-ügy. 2000-ben feltörték az Elender szerverét, kicserélték a honlapjuk főoldalát, valamint ellopták közel 2000 ügyfelük jelszavát, amit közszemlére tettek. Az elkövetők hárman voltak, két fiatalkorú és egy felnőtt korú személy. Az elkövetők arra hivatkoztak kihallgatásukkor, hogy az Elender cég nem népszerű az internetes társadalom körében, a biztonsági rendszerük gyenge és több hiányosságot is találtak a cég információs rendszerében, amit nem javítottak ki. Mivel az elkövetésük idejében a büntető törvénykönyvben még nem szerepelt semmilyen számítástechnikai bűncselekmény tényállása, így a Fővárosi Bíróság közérdekű üzem megzavarása, valamint magántitok megsértése miatt emelt az elkövetők ellen vádat.
[8] http://hu.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3s_t%C3%A1rsadalom_(fogalom) (letöltve:2014.09.06.)

- Ddos (Distributed Denial of Service) azaz az elosztott szolgálatmegtagadással járó támadással, az informatikai szolgáltatás teljes vagy részleges megbénításával, helyes működési módjától való eltérítéssel;[9]
- adatlopással.

Az informatikai bűncselekmények osztályozása több szempont szerint történhet. Az alábbiakban tekintsünk át közülük néhányat.

Az **egyszerű osztályozás** szerint a bűncselekmény elkövetésekor a számítógép lehet:

- célpont;
- vagy eszköz.

A Sieber-féle osztályozás szerint az informatikai bűncselekmény lehet:

- A számítógépes manipulációval elkövetett csalás (fraud by computer manipulation). Ide tartoznak, többek között, a bankkártyával végrehajtott manipulációk valamint a szoftver illegális megváltoztatásával elkövetett visszaélések.
- A számítógépes kalózkodás és szoftver-lopás. (computer espionage and software theft). A szoftverrel kapcsolatos szerzői jogok megsértése (szerzői jogi védelem alatt álló szoftverek illegális másolása, terjesztése és felhasználása) tartozik ide.
- A számítógépes szabotázs (computer sabotage), ami tulajdonképpen a számítógépes rendszer működésének megzavarása. Ezzel az elkövetőnek az a célja, hogy kárt vagy üzemzavart okozzon más rendszerekben.
- A szolgáltatás-lopás (theft of services), vagyis a díjfizetéshez vagy egyéb feltételhez kötött számítógépes vagy távközlési szolgáltatás ellenszolgáltatás nélküli, jogosulatlan igénybevétele.
- Az adatfeldolgozó rendszerhez való jogosulatlan hozzáférés (unauthorized access to data processing systems), melynek során jogosulatlan adatok megismerése és/vagy megszerzése a cél.
- Az adatkezeléssel elősegített hagyományos gazdasági bűncselekmény (traditional business offences assisted by data processing), vagyis a számítógépes bűnözés és a fehér-galléros bűnözés.

Wasik-féle osztályozás szerint megvalósulhat:

- jogosulatlan hozzáférés számítógépen tárolt adatokhoz, illetve programokhoz;
- számítógépes csalás;
- adatok vagy programok jogosulatlan elvitele;
- számítógép-szolgáltatás vagy gépidő jogosulatlan használata;
- rombolás vagy megsemmisítés.

Bequai-féle osztályozás megkülönböztet:

- adatbűncselekményt;
- szolgáltatás-lopást;
- tulajdonnal kapcsolatos jogsértést;
- ipari szabotázst;
- politikai szabotázst;
- egyéb rombolási cselekményt;

[9]http://hu.wikipedia.org/wiki/Szolg%C3%A1ltat%C3%A1smegtagad%C3%A1ssal_j%C3%A1r%C3%B3_t%C3%A1mad%C3%A1s. 2014.augusztus 16.

- személyiséget sértő cselekményt;
- pénzügyi bűncselekmény.

Young-féle rendszerezésben előfordulnak**:**

- hagyományos lopásszerű jogsértések;
- szellemi tulajdonnal kapcsolatos jogsértések;
- szolgáltatás megszakítások, lopások és számítástechnikai eszközrongálások;
- számítógépes pornográfia és fiatalkorúak kihasználása;
- magánszféra számítógép általi megsértése;
- számítógépes kikémlelés;
- egyéb hagyományos bűncselekmények.

7.2.3. A számítógépes bűncselekmények jellemzői

Gyorsaság, ami nem azt jelenti, hogy az elkövetők az adott helyzetet kihasználva követik el a bűncselekményt, hanem inkább azt, hogy a cselekmény végeredménye gyorsan bekövetkezik. Ezért könnyű a bűnelkövetők és nehéz a nyomozóhatóságok helyzete. A gyorsaság nemcsak az adatok, információk sebességét jelenti, hanem a technika fejlődését is, mellyel lépést kell tartani. A gyorsaság miatt a sértettek vagy potenciális sértettek is veszélyben vannak, hiszen előfordulhat, hogy nem észlelik időben a sérelmükre elkövetett bűncselekményt, vagy annyi idő telt már el az elkövetés óta, ami a nyomozást megnehezíti. Ugyanakkor a gyorsasággal kapcsolatban fontos kiemelni, hogy a cselekmény előkészítése, maga az elkövetés nem biztos, hogy gyorsan történik, hiszen a különböző programok elkészítése hosszú időt vesz igénybe. A gyorsaság függ a kor technikai újításaitól és az elkövetők szakmai fejlettségétől, tudásától.

Magas fokú látencia, amelynek az egyik oka, hogy a számítógépes bűncselekmények áldozatai egyáltalán nem vagy nem időben észlelik, hogy bűncselekmény áldozatai lettek. A sértettek, mivel a jogsértés a virtuális térben történik, így nem veszik észre, hogy az informatikai rendszerben tárolt adataikkal visszaélés történt. Ugyanakkor sok esetben előfordul az is – főleg bankok vagy nagyobb cégeknél – hogy az ellenük elkövetett bűncselekményeket eltitkolják és/vagy az esetek többségét nem jelentik a hatóságok felé[10]. Sok esetben azért, mert attól félnek, hogy az ügyfelek bizalma irányukban meginog. Másik oka a magas fokú látenciának, hogy az elkövetőknek nem szükséges az elkövetés helyszínén tartózkodni. A különböző kommunikációs eszközök segítik, hogy a cselekményüket távolról irányíthassák, így a tettenérés szinte kizárt, a nyomozó hatóság részéről a felderítés a hagyományos eszközökkel lehetetlen. Nehezíti a nyomozóhatóság munkáját természetesen az is, hogy a bűnözők nemcsak, hogy távolról irányítják az eszközöket, hanem előfordulhat az is, hogy egy előre meghatározott időpontra aktivizálják az adott programot, ami idő bekövetkeztekor hajtja végre a módosításokat, szerzi meg az adatokat az áldozatok eszközeiről.

Nemzetközi jelleg, amely azt is jelenti, hogy az internet nem ismeri az országhatárokat. Az információ áramlását nem nehezíti meg, hogy az óceánon túlra kell eljuttatni, hiszen minden a virtuális térben történik. Nem szükséges, hogy az elkövető és az áldozat egy helyen tartózkodjon.

[10]Sok esetben a pénzintézetek, hitelintézetek nem jelentik, hogy akár ők maguk, vagy az ügyfeleik támadás áldozatai lettek.

Technikai, technológiai jelleg, ami abban nyilvánul meg, hogy a különböző számítástechnikai eszközök és azok fejlődése okozza számítógépes bűnözést. Minden újabb és újabb számítástechnikai vívmányt a számítástechnikai bűnözők felhasználják bűncselekmények elkövetése során. A legnagyobb problémát az jelenti, hogy sem a hatóságok, sem a társadalom nincsenek felkészítve e bűnözés elleni védelemre.

Nehéz felderíthetőség, ami azt jelenti, hogy a számítógépes bűncselekmények elkövetését nehezen vagy csak későn lehet észlelni. Sokszor a nyomozó hatóságok járatlansága, képzetlensége is nehezíti a nyomozást. De ugyanúgy nehézséget jelent a különböző nyomozó szervek rosszabb technikai felszereltsége és felkészültsége. Elkövetői oldalról nézve, a felhasználók névtelensége vagy álnevek használata miatt nehéz a személyazonosság meghatározása. Megnehezíti a felderítést az elkövetők által megszerzett adatok titkosítása és/vagy megsemmisítése. A számítástechnikai eszközök, berendezések helyrehozhatatlan megrongálása is megnehezíti a nyomozóhatóság munkáját. Tekintettel arra, hogy a kibertérben nincsenek országhatárok, az elkövetés helyét is nehéz meghatározni.

Intellektuális jelleg, hiszen az elkövetők általában fiatal, magasan képzett, magas intelligenciájú (szak)emberek. Az intellektuális jelleg nem minden informatikai bűncselekmény esetén igaz, hiszen vannak olyan bűncselekmény típusok, melyek nem igényelnek nagy szakképzettséget, mégis jelentős károkat képesek okozni. A bűncselekményeket sokszor jómódú, többrétűen szocializálódott, 18 és 45 év közötti emberek (jellemzően férfiak) követik el.

Névtelenség (anonimitás) is kedvez a bűncselekmény elkövetőinek. A világháló névtelenséget biztosít. Jelenleg nincsen olyan hazai és/vagy nemzetközi jogszabály, amely büntetné azokat, akik egyáltalán nem adják meg nevüket, adataikat, vagy fiktív névvel regisztrálnak. Ez az a jellegzetesség, ami miatt a számítógépen elkövetett bűncselekmények száma felfelé ível.

7.2.4. A számítógépes bűnelkövetés jellemző területei

A számítástechnikai bűncselekményeket alapvetően **gazdasági területen** követik el, hiszen az elkövetés, jellemzően, anyagi, gazdasági és pénzügyi haszonszerzési célzattal történik. A másik jellemző szféra pedig az **információ-biztonsággal kapcsolatos terület**.

Az informatikai rendszerekben adatok formájában tárolt információk védelmet igényelnek, melyre az **információvédelem** vonatkozik. Ez utóbbi fogalom olyan eljárások és intézkedések összességét jelenti, amely lehetővé teszi az azonosítási és hitelesítési eljárások kialakítását, a hozzáférési rendszer létrehozását (jogosultságok kiosztását, a jogosultságok ellenőrzését), az adatok és a programok sérthetetlenségének biztosítását, az adatok bizalmasságának (titkosság: az információkhoz vagy adatokhoz csak az arra jogosultak és csak az előírt módon férhetnek hozzá) garantálását, a naplózási rendszer megvalósítását a szervezeten belül. A különböző védett, bizalmas adatok sértetlenségéhez fűződő érdek kiemelten fontos, és aminek illetéktelen személyek vagy csoportok általi megszerzése nemcsak komoly károkat okoz, hanem az elkövetőknek akár elképzelhetetlen bevételi forrás is. Ez utóbbi például a rendvédelem, igazságügy vagy nemzetbiztonság területén a személyes illetve minősített adatok illetéktelen megszerzése.

7.2.5. A számítógépes bűncselekmények elkövetői

A számítógépes bűncselekmények elkövetőiről általánosságban elmondható, hogy ők magasan képzett szakemberek. Életkoruk alapján általában a 18-45 évesek, és jellemzően férfiak. Jellemző az is, hogy magányosan, esetleg kis létszámú bűnözői csoportban követik el a bűncselekményeket.

Az elkövetők **főbb kategóriái** közül a legismertebbek:

A **Hacker** az a személy (szakember), aki az internet segítségével fér hozzá a védett adatokhoz más számítógépén. Általában a rosszindulatú hackerek az ismertebbek, pedig ugyanúgy léteznek olyan, a számítástechnikai rendszerekben jártas szakemberek, akik a tudásukat a különböző rendszerek fejlesztésére, tökéletesítésére, biztonságosabbá tételére fordítják. Székely Zoltán szerint a „*White-hat hacker: Számítástechnikai szaktudását a világ jobbá tételére használó szakember. Black-hat hacker: Számítástechnikai szaktudását önző módon saját céljaira hasznosító szakember*[11].

A **Cracker** az informatikához magas színvonalon értő személy, aki tudását elsősorban a saját céljaira használja fel, elsősorban anyagi haszonszerzés (pl. a szerzői jogi védelmet biztosító technikai intézkedést játssza ki) vagy társai elismerése céljából úgy, hogy más számítógépében behatol jogtalanul és onnan információkat szerez meg, amelyekkel visszaél, eladja.

A **pszichológiai manipulátor** (social engineer) nem más, mint a védelmi intézkedéseket a jogosultságokkal rendelkező felhasználók megtévesztésével kijátszó hacker. Azaz, egy jogosultsággal rendelkező felhasználó olyan személy számára, aki nem rendelkezik jogosultsággal, bizalmas információkat, adatokat, vagy a belépéshez szükséges jelszókat ad át.

A **kalóz**, aki megtévesztésből, vagy meggyőződésből anyagi haszonszerzés végett követi el a bűncselekményt számítógépes környezetben.

7.3. A számítógépes bűncselekmények típusai

A számítógépes bűncselekmények különböző vírusok és férgek (worm) írásával és terjesztésével kezdődtek. Ezek nem okoztak igazán nagy károkat. Ezt követően viszont, a bűnözők is felismerve a lehetőséget, már megindultak a rosszindulatú programok (malware), a gyökércsomagok (rootkitsek), és más rosszindulatú támadások, amelyekkel már ténylegesen nagy anyagi haszonszerzésre és károkozásra törekedtek az elkövetők. Tekintettel arra, hogy az informatikai bűncselekmények napról-napra változnak, meghatározásuk nem könnyű.

A továbbiakban a **számítógépes bűncselekmények** csoportosításánál a már ismertetett számítástechnikai bűnözésről szóló Egyezmény szerinti **felosztást** is alapul véve az alábbi négy típust tegyük vizsgálat tárgyává:

- A számítástechnikai rendszer, valamint adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények
- A számítógéppel elkövetett bűncselekmények
- A tartalom jellegű bűncselekmények

[11] http://www.pecshor.hu/periodika/2008/szekely.pdf 2014. augusztus 27.

- Egyéb jellegű bűncselekmények

7.3.1. A számítástechnikai rendszer, valamint a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények

Ebben kategóriában találhatók azok az alábbiakban felsorolt bűncselekmény-típusok, amelyek a számítógépen tárolt adatok, azok megbízhatósága, sértetlensége és elérhetősége ellen irányulnak:

- a számítógépes rendszerbe történő jogosulatlan belépés;
- a számítógépek közötti adatcsere jogosulatlan lehallgatása;
- az informatikai rendszerben tárolt adatok sértetlensége ellen irányuló jogtalan cselekmények (az adatok jogosulatlan törlése, megrongálása, szándékos megkárosítása, megváltoztatása, stb.);
- a számítástechnikai rendszerek sértetlensége ellen irányuló cselekmények, amelyek megvalósulhatnak a rendszer szándékos tönkretételével, illetve a számítógépbe vagy számítástechnikai rendszerbe történő és annak működését zavaró vagy tönkretevő adatok, programok (vírusok, férgek stb.) bevitelével.
- visszaélés eszközökkel.

A felsoroltak közül elterjedtségük és hatásuk miatt is ki kell emelni a számítástechnikai rendszerek sértetlensége ellen irányuló **rosszindulatú programoka**t. Ezekkel minden számítógép felhasználó találkozhat. Jellegzetességük, hogy ellenük megfelelő szoftverek segítségével védekezni lehet.

A rosszindulatú programok között leggyakoribbak a **vírusok** (1983 óta használják ezt a kifejezést), amelyek valójában olyan programok, amelyek saját kódjukat valamilyen módon hozzácsatolják más végrehajtható programokhoz, és a megfertőzött gazdaprogram indításakor áveszik attól ideiglenesen a vezérlést, majd végrehajtják a beléjük programozott utasításokat. Ezek a vírusok önmagukban életképtelenek, működésükhöz megfelelő hardver- és szoftverkörnyezet szükséges. A vírus indítása rendszerint valamilyen időzítéshez (dátum, időpont), eseményhez vagy egyéb feltételhez kötött."[12] A számítógépes vírusok legtöbbször olyan kicsik, hogy azt szinte észre sem lehet venni. A vírusok lehetnek kártékonyak, ami miatt az számítógép használhatatlanná válik. A legtöbb vírus azonban inkább zavaró. Van olyan vírus is, amely azonnal kifejti hatását. Létezik olyan is, amely csak bizonyos feltétellel (pl. a számítógép bizonyos számú ki és/vagy bekapcsolása esetén) aktiválódik. **A vírusok (gyakori) jellemzői:**

- a gazdaprogramok megfertőzése (szinte minden vírusra jellemző);
- az önsokszorosító viselkedés (szinte minden vírusra jellemző);
- kis méret;
- az operációs rendszerek fertőzése (legtöbbjük a Microsoft Windows operációs rendszerekben fertőz) ;
- a futtatható állományokat képesek megfertőzni;
- általában ártó szándékkal készítették őket;
- gyakran akár válogatva, időzítve tönkretesznek más fájlokat;

[12] http://www.antivirus.hu/virved/index.php?CN=30&CIE=0. 2014. augusztus 25.

- rejtetten működnek, esetleg akkor fedik fel magukat, ha feladatukat elvégezték;
- egyre fejlettebb intelligenciával rendelkeznek (pl. változtathatják saját kódjukat és aktivitásukat) ;
- céljaik nem feltétlenül csak a rombolás (lehet haszonszerzés vagy személyes adatok megszerzése) ;
- terjedhetnek e-mailekben (az azokhoz csatolt fájlokban), messengereken vagy letöltött tartalmakon keresztül.

A rosszindulatú programok másik kategóriáját a **férgek** alkotják. A férgek a számítógépes vírushoz hasonló „önsokszorosító" programok, azonban, a vírusokkal ellentétben, a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A férgek gyakran a számítógép-hálózatokat használják fel terjedésükhöz. A kezdetben egy olyan e-mail melléklet, amely megnyitva megfertőzi a számítógépeket. A féreg olyan fájlokat, címtárakat vagy ideiglenes weblapokat kereshet a fertőzött számítógépen, amelyek e-mail címeket tartalmaznak. Ezt követően fertőzött e-mailekben üzeneteket küld a címlistában lévő címekre. Az e-mail üzenetekben a feladó címét gyakran álcázza, meghamisítja. majd a férgek automatikusan terjedni kezdenek különböző e-mailekben a hálózatokon és az operációs rendszerek biztonsági résein át. A férgek sem minden esetben tesznek kárt a számítógépben, viszont csökkenthetik a számítógép és a hálózat teljesítményét és stabilitását.

A rosszindulatú programok egy újabb kategóriáját képezi a **Botnet**[13]**, avagy zombi gépek hálózata.** A botnet célja, hogy nagy teljesítményű, gyors, ugyanakkor egy anonim infrastruktúrát nyújtson a levélszemét küldőnek (spammernek), amivel majd az könnyen és gyorsan lesz képes nagy mennyiségben kéretlen levelet küldeni, vagy egyéb törvénytelen cselekedetet folytatni. A botnetek általában otthoni, iskolai vagy vállalati számítógépek lesznek. Egy számítógép úgy is válhat botnetté, hogy arról a használója tudna, mivel egy speciális program feltelepül a számítógépre és az a háttérben fut anélkül, hogy azt a számítógép gazdája észrevenné. Nemcsak spammerek használnak botneteket, hanem más bűnözői csoportok is károkozás vagy megfélemlítési célzattal. A botnet tehát fertőzött, távolról irányított gépek hálózata, melynek irányítását a trójai típusú szoftverek és vírusok az elsődleges eszközei. Napról napra egyre többen használnak internetet A világháló az üzleti életben is megkerülhetetlen, így a potenciális áldozatok száma és a támadások által okozható kár egyre nő. Már régóta jelen vannak a támadások kivitelezéséhez infrastruktúrát (vagyis botneteket) biztosító "vállalkozók" is, akik bérbe adják az általuk uralt számítógépeket kéretlen levelek küldésére, illetve különféle támadások végrehajtására. A botnetek száma és mérete döbbenetes mértékben megnőtt. A technikai háttér tehát maximálisan biztosított ahhoz, hogy a világ bármely részén található informatikai rendszer ellen túlterheléses támadást indítsanak.

Bot-hálózatról akkor beszélünk, ha nagyon sok számítógépet (ez lehet akár több ezer is) távirányítással kapcsolnak össze. Ezeket nagyobb weboldalak megbénítására, illetve, kéretlen levelek felismerés veszélye nélküli küldésére használják. Előfordulhat az is, hogy pénzért továbbítanak bot-hálózatokat harmadik személyeknek. A bot-hálózatok mögött bűnözői érdekek vannak, de az ilyen hálózat-üzemeltető ugyanúgy lehet egyéni felhasználó is, mint a szervezett bűnözői-, vagy a terroristacsoportok. A támadók az operációs rendszerek

[13] A köztudatban a Botnetre a zombie-számítógép megnevezés terjedt el, mivel a számítógép úgy viselkedik, akár egy zombi, mint egy akarat nélküli eszköz, amely életre kel.

(elsősorban a Microsoft, de lehet más is) gyengéit használják ki. Naponta a világon több ezer számítógépet kaparintanak meg és használnak fel idegen célok megvalósítására.

Az interneten terjedő titok- és személyiségsértő számítógépes programok összességét **kémprogramo**knak (Spyware) nevezik. E programok célja, hogy a felhasználó tudta nélkül szerezzék meg a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait. Úgy működik, hogy az interneten történő böngészést rögzíti és arról jelentést küld a program írójának A megszerzett adatokat leginkább bűncselekmény elkövetéséhez használják fel. Ismert kémprogram a **billentyűzetfigyelő** (keylogger) program is. Ezek a programok a billentyű-leütéseket rögzítik és naplózzák a begépelt szöveg kifürkészése a cél. Kémprogram a **láng** (Flame) **vírus**, amely a billentyűhasználatot, a szöveges- és hangüzenetek (pl.: a Skype,) forgalmát rögzíti és továbbítja a szerverekre. Ebbe a kategóriába sorolható még a **betörés** (Hacking), amely jogosulatlan belépést (elektronikus betörést) és bennmaradást jelent a számítástechnikai rendszerbe, illetve egyéni számítógépekbe. Célja sokféle lehet, pl. vírus vagy más rosszindulatú program (malware) elhelyezése.

Végezetül szólni kell a **hátsó ajtó** (Backdoor) **programok**ról, amelyek a számítógép védelmi rendszerén keresztül nyitnak kiskaput Ezáltal a támadók hozzá tudnak férni a rendszer erőforrásaihoz. Célja lehet számítógépes és személyes adatok kifürkészése, tiltott tartalmak elhelyezése, szerver megbénítása stb. A Backdoor-nak lehet legális program funkciója is. Ilyen például a vállalati rendszerben a munkaállomások távmenedzseléséhez szükséges program, melynek segítségével az arra felhatalmazott rendszergazda távolból is elvégezhet bizonyos beállításokat és módosításokat.

7.3.2. Számítógéppel elkövetett bűncselekmények

A számítógépekkel elkövetett bűncselekmények csoportjába azokat a bűncselekményeket soroljuk, amelyeket magával a számítógép felhasználásával, informatikai eszközzel és/vagy internetes hálózat segítségével követnek el. Az információs rendszer felhasználásával elkövetett bűncselekményeknek (csalások vagy hamisítások) alapvetően két formájáról, a **számítógépes csalás**ról és az **adathalászat**ról beszélhetünk.

A **számítástechnikai csalás** olyan szándékos, vagyoni hátrány okozására irányuló elkövetés, amit adatok felvitelével, megváltoztatásával, vagy törlésével követnek el. Ide tarozik az olyan jogosulatlan adatbevitel, módosítás, vagy információtörlés által keletkezett adatok felhasználása is, amelynek célja, hogy az valamilyen előnyhöz jutassa a felhasználót.

Az **adathalászat** (phising) olyan tevékenység, amikor valaki úgy szerzi meg egy felhasználó titkos jelszavait, hogy végtére is azt ő maga adja meg neki. Az adathalászat egyik, gyakori formája az **eltérítéses adathalászat** (pharming), amikor az elkövetők az adatszerzéssel jogosulatlanul, a banki ügyfelektől szereznek pénzt. Ennek az elkövetése kíván némi informatikai ismeretet. A tettesek e-mailben arról értesítik az ügyfelet, hogy bankjuk honlapját az adott üzenetben megadott linken érhetik el és léphetnek be a különböző internetes pénzügyi tevékenységük lebonyolításához. Így az ügyfél a linken begépeli az azonosítóit, felhasználónevét és a sikeres belépés helyett azt látja, hogy a bank oldala továbbra sem elérhető. Az elkövetők viszont a megadott adatokat elmentik és felhasználják. A másik adathalászati módszer, amikor a bank nevében telefonon vagy e-mailen keresztül keresik meg az ügyfeleket és kérik el a belépéshez szükséges információkat.

7.3.3. Tartalom-jellegű bűncselekmények

Tartalom-jellegű bűncselekményeknek nevezzük azokat a bűncselekményeket, amelyek tartalmuknak jellege miatt valamilyen deliktumot valósítanak meg. A weboldalon található szöveg, kép, video jellege önmagában alkalmas a bűncselekmény megállapítására. Ilyenek például a gyermek pornográf tartalmak, a gyűlöletbeszéd, az interneten keresztül megvalósuló zaklatás, de tartalom-bűncselekmény a film-, zene,- szoftver illegális letöltése, a szerzői vagy szerzői joghoz kapcsolódó jogok megsértése is.

7.3.4. Egyéb jellegű bűncselekmények

Az **egyéb jellegű bűncselekmények** csoportjába szokás besorolni az alábbiakban felsorolt internetes bűncselekményeket, amelyekről meglehetősen gyakran lehet hallani, illetve olvasni.

A **nigériai levelek** (más néven 419-es átverés, illetve SCAM-419) lényege, hogy az elkövetők e-mailen keresztül keresik meg áldozatukat, amelyben nagy összeget helyeznek kilátásba bármilyen segítségnyújtás ellenszolgáltatásaként. Az e-mail általában külföldi ügyvédi irodától és/vagy valamelyik gazdag (de nem létező) afrikai királytól érkezik, és arra utal, hogy egy nagyobb vagyonhoz vagy örökséghez akkor tud hozzájutni, ha a címzett előre meghitelez neki egy kisebb összeget, amit majd visszafizet a pénzből. Természetesen a pénz átutalása után a sértett nem kapja vissza a pénzét.

A **Hoax** (átverés) valójában e-mailen keresztül terjedő álhír. Célja nem agyonszerzés, hanem a célszemély megtréfálása. Az álhírekkel szinte napi rendszerességgel találkozunk. Bár nem minden esetben, de jellemzője a vírus jelleg. Előfordulhat, hogy az üzenet kitalálójának célja, hogy a világban szétküldött e-mailekkel további e-mail címeket szerezzen meg, melyekre akár kéretlen leveleket (spameket) is lehet küldeni.

A meglehetősen nagy mennyiségben, az interneten terjedő **kéretlen levél vagy lánchír** (Spam) látszólag érdektelen információkat tartalmaz. Gyakori, hogy a levélben szereplő megszólítás ismeretlen, így első látásra téves címzésnek tűnik. A tartalma viszont valamilyen nyereményjátékra történő regisztrálás, piramisjáték, vagy egy-egy illegálisan működő szerencsejáték weboldal vagy film, illetve zene letöltését hirdető internetes honlapra reklámoz.

A **holland vagy spanyol lottó** a nigériai levelek egy újabb változata, amellyel pénzügyi csalásokat próbálnak végrehajtani. Az elkövetés módja, hogy a kiválasztott személyt elektronikus levélben értesítik arról, hogy egy nyereményjátékon a hatalmas összeget nyert. Csak egy dolga van az illetőnek, hogy válaszoljon. Amennyiben ez megvalósul újabb és újabb e-mailek érkeznek, amelyekben különböző jogcímeken (illetékek, adók, banki-átutalási költségek stb.) nagyobb összegeket kérnek egy megadott külföldi számlaszámra átutalni. A becsapottak természetesen hiába várják a nyereményüket, az soha nem érkezik meg. Ennek a csalásnak a komolyságát mutatja, hogy már 2004-ben az akkori Nemzetbiztonsági Hivatal (NBH) is vizsgálódott. Megállapították, hogy a „nyereményjátékos” elkövető ugyanazok, akiktől a nigériai levelek is származtak.

A **piramis- vagy pilótajáték** lényege, hogy a játék szervezői meglehetősen kis összegek befizetése esetén hatalmas összeget ígérnek a befektetőknek. Sőt magas jutalmat is látókörbe hoznak, ha további résztvevőket szerveznek be maguk alá. Azaz a korábban belépők a később

belépett személyek által befizetett pénzből is részesülnek. Persze előfordul, hogy utóbbiak már egyáltalán nem kapnak semmiféle részesedést. Dr. Nagy Zoltán szerint „*A piramisjáték büntetőjogi üldözendősége akkor jelentkezik, amikor kiderült, kiderül, hogy a játék szervezői a magas hozamot megtévesztésül ígéri, ígérte. A piramisjáték a csalás speciális esete.*[14] Ezért is a piramisjáték szervezése a Btk. 412.§ szerint jogellenes cselekmény.

Az utóbbi időben terjedtek el a **rendőrségi kártevők** (Police malware), amelyek valójában a rendőrség nevében küldött olyan tartalmú e-mailek, amelyek arra utalnak, hogy egy adott – általában felnőtt tartalmú – oldal letöltése bűncselekménybe ütközik és a felhasználónak emiatt büntetést kell fizetnie.

Az egyéb bűncselekmények közé tartoznak a **szerzői jogi jogsértések,** amelyek a szerző és/vagy más jogosultak vagyoni jogait sértik. Ilyen jogellenes cselekmény a különböző, szerzői joggal védett tartalmak (filmek, zenék, számítógépes-játékok, szoftverek) fel, illetve letöltése. Az elkövetők az ilyen típusú bűncselekménnyel hatalmas bevételhez jutnak.

A k**özösséget és egyéni becsületet sértő jogsértések** alatt a rasszista, idegengyűlöleti (xenophob) tartalmakat, közösség elleni izgatást, gyűlöletbeszédet, stb. jogsértéseket kell érteni.

Figyelemre méltók és veszélyesek a **pornográf, pedofil tartalmak**. Megjegyzendő, hogy a gyermekpornográfia bűncselekmény, amely a 18. életévet be nem töltött személyekről készült, a nemiséget nyíltan bemutató, erotikus tartalmú kép vagy videofelvételek. Magyarországon a Btk.[15] szerint ez zaklatásnak minősül.

Az egyéb bűncselekmények közé soroljuk még az **internetes zaklatást** (cyberbullying) is, amely legfőképp a tinédzserek között terjedő, az áldozat valamilyen külső-vagy belső tulajdonságát kiemelő cselekmény, amelyet nagy nyilvánosság előtt mutatnak be. Bár csekély jelentőségűnek tűnik, de nem az. Nagyszámú, mind magyarországi, mind külföldi példa ismeretes, amikor a zaklatott személy öngyilkosságot követett el.

Rendkívül veszélyesek a **kábítószerhez való jutásra, fogyasztására é forgalmazására szolgáló tartalmak** is. Ma már az interneten is elérhetőek olyan tartalmú weblapok, amelyek kábítószer alapanyagait és készítésének módját ismertetik, illetve a kábítószer előállításhoz alkalmas eszközöket is árulnak.

7.4. Az informatikai bűnözés elleni harc nemzeti szabályai és szervezetei.

Magyarországon az első és legfontosabb jogszabály ebben a témában is az **Alaptörvény**.

A számítógépes bűncselekmények meghatározása, jogszabályi keretek közötti szabályozásának szükségessége már a 2001-es **számítógépes bűnözésről szóló Egyezmény** (Convention on Cybercrime) aláírásakor megfogalmazódott. Magyarország, meglehetősen hosszú évek multán, csak 2004-ben hirdette[16] ki, illetve tett eleget az Egyezményben vállalt, a magyar jogrendbe való beemelési (implementálási) kötelezettségének.

---

[14] Dr. NAGY Zoltán András*: Bűncselekmények számítógépes környezetben*. Ad Librum, Budapest, 2009. 150-151.
[15] 2012. évi C. törvény a Büntető törvénykönyvről (Btk.)
[16] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

Fontos jogszabály a **2012 évi Btk.**,[17] amely már külön fejezetben foglalkozik a számítógépes környezetben elkövetett bűncselekményekkel

Magyarországon az első és legfontosabb jogszabály ebben a témában is az **Alaptörvény**.

A számítógépes bűncselekmények meghatározása, jogszabályi keretek közötti szabályozásának szükségessége már a 2001-es **számítógépes bűnözésről szóló Egyezmény** (Convention on Cybercrime) aláírásakor megfogalmazódott. Magyarország, meglehetősen hosszú évek multán, csak 2004-ben hirdette[18] ki, illetve tett eleget az Egyezményben vállalt, a magyar jogrendbe való beemelési (implementálási) kötelezettségének.

Fontos jogszabály a **2012 évi Btk.**,[19] amely már külön fejezetben tartalmazza az információs rendszer elleni bűncselekményeket. A korábban hatályban lévő Btk. a gazdálkodási kötelességeket és a gazdálkodás rendjét sértő bűncselekmények között helyezte el ezeket a cselekményeket, holott a jogi tárgya az információs bűncselekményeknek nem a gazdálkodás rendjének megsértése. Az információs bűncselekmények esetében a társadalmi érdek védelme az információs rendszerek megfelelő működtetéséhez és a rendszerben foglalt adatok megőrzéséhez fűződik.

A Btk XLIII. fejezet a „Tiltott adatszerzés és az információs rendszer elleni bűncselekmények" címet kapta. A fejezet különálló törvényi tényállásokban szabályozza az információs rendszereket érintő különböző elkövetési magatartásokat. A 422.- 424. §-ok a tiltott adatszerzés, az információs rendszer vagy adat megsértése, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszása elnevezéseket viseli. Ezek a bűncselekmények a Cybercrime Egyezmény, valamint az Európai Tanács információs rendszerek elleni támadásokról szóló 2005/222/IB kerethatározata rendelkezésein alapulnak.

A 422.§-ában szabályozott tiltott adatszerzésre lett változtatva a magántitok jogosulatlan megismerése bűncselekmény, kifejezőbbé téve a korábbiakban szabályozott, a magántitok megsértése bűncselekmény elkövetési magatartását. A tiltott adatszerzés a jogosulatlanul megszerezhető titokkört kibővíti, ezáltal a magántitkon túl a személyes adat, gazdasági titok vagy üzleti titok jogosulatlan megszerzése érdekében végzett, célzott magatartásokat is szankcionálja. Az elkövetési magatartások közül kiemelendő a technikai eszköz alkalmazásával történő megfigyelés vagy rögzítése a történteknek, valamint elektronikus hírközlő hálózat útján másnak továbbított vagy azon tárolt adat kifürkészése, és az észleltek technikai eszközzel rögzítése. A jogalkotó a rögzítés kifejezés alatt eseményeknek kép- és/vagy hangrögzítő eszközzel való felvételét érti (a felvétel digitális vagy analóg jeleket rögzítő eszközzel is történhet). A tényállásban új elem lett beépítve, amelynek szükségességét az teremtette meg, hogy a szervezett bűnözés titkos információgyűjtése során használt eszközei és szakértelme szinte megegyezik a bűnüldöző szervek által használt eszközökkel és szakértelemmel. Ezért szükségessé vált a fedett nyomozók és a bűnüldöző hatóságokkal titkosan együttműködő személyek életének és testi épségének bűntetőjogi védelmet biztosítani.

A 423.§ az Információs rendszer vagy adat megsértése bűncselekmény az információs rendszer jogosulatlan használata megvalósításának eseteit sorolja fel, emellé beemelve a „jogosultsága kereteit megsértve" történő elkövetést is. Ez utóbbi következik be, amennyiben

---

[17] 2012. évi C. törvény a Büntető Törvénykönyvről (Btk.)

[18] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

[19] 2012. évi C. törvény a Büntető törvénykönyvről (Btk.)

az elkövető jogosultsága kiterjed az adott magatartásra (pl. rendszergazda), azonban amennyiben a rendszergazda a jogosultsága kereteit túllépi, akkor már bűncselekményt követ el.

Kiemelést igényel, hogy az információs rendszerbe való jogosulatlan adatbevitel akkor tekinti ezen jogszabályhely szankcionálandónak, ha az további , nem kívánt következményekhez vezet, így ha a rendszer működését akadályozza. Feltétlenül hangsúlyozandó a szabályozásban, hogy a számítástechnikai rendszer kifejezés helyett – annak jelentés tartalmát megtartva – a törvény az információs rendszer fogalmát használja, itt kerül meghatározásra az információs rendszer vagy adat megsértése tényállással – a Cybercrime Egyezményben szereplő fogalommal azonosan – az adat fogalma: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

A 424. §-ban szabályozott, az Információs rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekmény értelmező rendelkezése megadja a jelszó fogalmát (az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.), büntetendővé nyilvánítja a jelszó egyszeri átadását is, mint elkövetési magatartást. A jelszó fogalma alatt bármely belépési kód, jelzés, azonosító stb. értendő, ha azok célja az információs rendszerbe – egészbe vagy részbe- történő bejutásának lehetővé tétele, illetőleg a rendszerbe való megakadályozása. A tényállásban megjelenő megszerzés kifejezés, amely a program, stb. sorsa feletti rendelkezést jelent, azonos tartalmú a Cybercrime Egyezményben meghatározott birtoklás szóval.

További informatikai vagy internetes környezetben elkövethető bűncselekmények:

- 204.§ Gyermekpornográfia
- 219.§ Személyes adattal visszaélés
- 220.§ Közérdekű adattal visszaélés
- 222.§ Zaklatás (Cyberbullying)
- 223.§ Magántitok megsértése
- 224.§ Levéltitok megsértése
- 226.§ Rágalmazás
- 226/A.§ Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése
- 226/B.§ Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala
- 227.§ Becsületsértés
- 265.§ Minősített adattal visszaélés
- 360.§ Tiltott szerencsejáték szervezése
- 375.§ Információs rendszer felhasználásával elkövetett csalás
- 385.§ Szerzői vagy szerzői joggal kapcsolódó jogok megsértése

A felsorolt bűncselekmények tekintetében ki kell emelni, hogy a korábbiakhoz képest megváltozott vagy szélesebb körben is értelmezhető az elkövetési magatartás.

Ilyen elkövetési magatartások a megszerzés, tartás, hozzáférhetővé tétel, nagy nyilvánosság számára hozzáférhetővé tétel, adatbevitel stb., amelyek az jogellenes cselekmények informatikai rendszeren történő megvalósulását jelentik.

Természetesen az anyagi jog szabályozása mellett szükség volt az eljárásjog új szabályozására is az informatikai bűncselekmények és a bűnözők elleni hatékony fellépéshez.

A számítástechnikai bűncselekmények felderítését és a bizonyítékok összegyűjtését, felhasználását a nyomozó szervek és az igazságszolgáltatás számára csak megfelelő eljárási cselekményekkel lehet elérni. Ezt tette meg **a büntetőeljárásról szóló 1998. évi törvény (Be).**[20]

A 2001-es Egyezménnyel összhangban alkották meg az információs rendszerben tárolt adatok megőrzésre kötelezésének és az elektronikus adat ideiglenes hozzáférhetetlenné tételének, mint kényszerintézkedéseknek, az új eljárásjogi szabályait. Az intézkedésekkel elérendő cél, hogy az informatikai rendszerben tárolt adatok, információk a büntetőeljárás megindulásától egészen a bírósági szakasz végéig felhasználhatóak legyenek bármikor, valamint az illegális tartalmakat blokkolják úgy, hogy azok ne semmisüljenek meg.

Fenti kényszerintézkedések végrehajtásához segítséget nyújt a belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól szóló **23/2003. (VI. 24.) BM-IM együttes rendelet (Nyor.)**, amely az elektronikus adat ideiglenes hozzáférhetetlenné tételének elrendeléséhez szükséges előterjesztéséhez nyújt segítséget.

Az előbbi törvények mellett természetesen fontos megemlíteni azokat az egyéb törvényeket, amelyek az internetet és az információs társadalmat hivatott szabályozni.

A következő jogszabály, bár a szó szoros értelmében nem kapcsolódik a számítástechnikai bűnözéshez az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló **2001. évi CVIII. Törvény (Elker.tv)**. E törvényben több olyan szabályozás, fogalom meghatározása található, amelynek ismerete az informatikai bűncselekmények nyomozása során elengedhetetlen. Ilyenek, többek között a szolgáltató (az információs társadalommal összefüggő szolgáltatást nyújtó természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet) és közvetítő szolgáltató. A törvény szabályozza a gyermekek védelmét, az elektronikus úton történő szerződéskötést, illetve elektronikus adat hozzáférhetetlenné tételének, valamint az elektronikus adat ideiglenes hozzáférhetetlenné tételének eljárására vonatkozó szabályokat is.

A fenti jogszabályokon kívül meg kell említeni az alant felsorolt további jogszabályokat, amelyek – bár nem tartalmaznak a jogellenes cselekmények elkövetése esetére szankciókat és csak egy-egy számítástechnikai bűncselekményhez alkalmazhatóak – ismerete mégis szükséges. Ilyenek például:

- az 1994.évi XXXIV. törvény a Rendőrségről szóló törvény (Rtv.);
- az 1995.évi CXXV. törvény, a nemzetbiztonsági szolgálatokról (Nbtv.);
- az 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről;
- az 1997. évi XXXI. Törvény a gyermekek védelméről és a gyámügyi igazgatásról;
- a 1999.évi LXXIV. törvény a szerzői jogról;

[20] 1998. évi XIX. Törvény a büntetőeljárásról (Be.)

- a 2001.évi XXXV. törvény az elektronikus aláírásról;
- a 2002. évi LIV. törvény a bűnüldöző szervek nemzetközi együttműködéséről;
- a 2003. évi C. törvény az elektronikus hírközlésről;
- a 2010. évi CXXII. törvény a Nemzeti Adó-és Vámhivatalról;
- a 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről;
- a 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.).

Felsorolt jogszabályok nem kimerítőek a számítógépes környezetben elkövetett bűncselekmények esetében. Nem is igazán lehet teljes a felsorolása, hiszen ez az egyik olyan bűncselekmény típus, amely a leggyorsabban fejlődik, és ami a törvényhozóknak is a legnagyobb gondot okoz épp a folyamatos változása miatt.

7.5. Az informatikai bűnözés elleni harc szövetségi és nemzetközi szabályai, valamint szervezetei.

A számítógépes bűnözés veszélyét mi sem jelzi jobban, mint az, hogy az nemzetek nemcsak a saját jogrendszerükön belül kívánják szabályozni az informatikai biztonságra és kibertérre vonatkozó szabályokat. A súlyosságot mutatja az, hogy nemzetközi összefogás keretében is fel kívánják venni a harcot a számítógépes bűnözéssel kapcsolatban.

A szabályalkotásból és a számítógépes bűncselekmények elleni harcból természetesen kivették a részüket az alábbiakban részletesen tárgyalt interkontinentális, kontinentális és régiós szervezetek (ENSZ, OECD, ET, EU, EBESZ, és mások) is.

Az **Egyesült Nemzetek Szervezete** (ENSZ) 1994-ben adott ki egy tanulmányt, amely az informatikai bűnözéssel szembeni védekezés kérdéseivel foglalkozik. Ez a tanulmány jelentős mértékben támaszkodik az ET ajánlásra.[21] Ebben felismerték, hogy a számítógépes környezetben elkövetett bűncselekményekkel szemben nem elegendő a területi védekezés, mivel az a deliktum jellege miatt egy kiterjedtebb kört veszélyeztet. Ugyanakkor, a már említett gyermekpornográfia bűncselekménye vagy az elektronikus zaklatás (cyberbullying) kiemelést érdemel, hiszen már az 1989-es gyermekek jogairól szóló New York-i egyezmény több szabályt is tartalmazott a gyermeknek a káros tartalmakkal szembeni védelméről.

A **Gazdasági Együttműködési és Fejlesztési Szervezet** (OECD) 1983 és 1985 között vizsgálta a számítógépes bűncselekményekkel kapcsolatos európai helyzetet és összegezte a tapasztalatokat. Megállapításaikkal iránymutatást kívántak adni a számítógépes környezetben elkövetett bűncselekmények megismeréséhez és kodifikálásához. Az OECD kimondta, hogy véleménye szerint számítógépes bűncselekménynek minősül:

- a számítógépes adatok és/vagy programok bevitele, elmentése, módosítása vagy törlése jogtalan vagyoni eszközök vagy más értékek megszerzése céljából;
- a számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elmentése hamisítás céljából;
- a számítógépes adatok és/vagy programok bevitele, módosítása, törlése vagy elmentése, vagy a számítógépbe történő bármely más beavatkozás a számítógépes

[21] Tanulmány a számítógépes bűnözés megelőzéséről és szabályozásáról (UN Manual on the Prevention and Control of Computer-Related Crime)

vagy telekommunikációs rendszerek funkcióinak megakadályozása céljából;

- a védett számítógépes programok tulajdonosai exkluzív jogainak megsértése a program jogosulatlan hasznosítása vagy forgalomba hozatala révén;
- a számítógépes vagy telekommunikációs rendszerbe az arra jogosult engedélye nélkül vagy a biztonsági intézkedések megsértésével, illetve más, tisztességtelen, netán, bűnös szándékkal történő belépés, vagy annak lehallgatása.

Az **Európa Tanács** (ET) által már az 1989. szeptember 13-án kibocsátott, ET 9(89). számú ajánlásában, ahogy ezt a 6.2.2 szakaszban is bemutattuk, egy minimum és egy fakultatív listát is összeállított a számítógépes-környezetben elkövetett bűncselekményekről. Ez követően, 2001-ben, éppen Budapesten fogadták el a „**Számítástechnikai bűnözésről szóló Egyezményt**.[22] Az Egyezmény 2004. július 1-jén lépett életbe, miután az ET 5 tagállama – így Magyarország is – ratifikálta a konvenciót. 2011. október 1-ig az ET 31 tagja, valamint az Amerikai Egyesült Államok is elfogadta, majd törvénybe iktatatta azt. Az Egyezmény védeni kívánja a számítástechnikai rendszerek, a hálózatok, az adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát. Biztosítani kívánja a rendszerek, a hálózatok, az adatok visszaélésszerű használatának megelőzését és bűncselekménnyé nyilvánítását is. Meghatározza továbbá a számítógépes bűnözés elleni hatékony fellépést lehetővé tévő felderítést, a nyomozást és bűnüldözést a nemzeti és nemzetközi szinten.

Az **Európai Unió Tanácsa** megbízásából is készült, 1994-ben, az információs társadalommal szemben tanúsított alábbi elvárásokat (célkitűzéseket) megfogalmazott lista, amelyben kimondta:

- Az informatikai eszközöket szabványosítani kell (bár az üzleti élet, a versenyszféra ebben nem érdekelt), ellenkező esetben elveszik a lényeg, az információáramlás.
- A monopolhelyzeteket, különösen a telekommunikációban meg kell szüntetni.
- A szellemi alkotásokat (szöveg, kép, zene, film, stb.) megfelelő szinten szabályozott, megfelelő szintű védelemben kell részesíteni.
- Biztosítani kell a veszélynek legjobban kitett magánszféra jogi védelmét.
- Ki kell dolgozni az adatbiztonság szabályait, az informatikai bűncselekmények megelőzésének megbízható rendszerét.

Az **Európai Unió Belső Biztonsági Állandó Bizottsága** (COSI) meghatározta a számítógépes bűncselekmények elleni védelem stratégiai céljait annak érdekében, hogy megkönnyítse a tagállamok közötti operatív tevékenységek koordinálását. Ez a belső biztonsággal kapcsolatos, operatív együttműködés érinti a rendőrségi, a határvédelmi, az igazságügyi, a vámügyi, a büntetés végrehajtási és egyéb területeket, valamint és szerveket és szervezeteket. A COSI-ban Magyarországot a Belügyminisztérium (BM) képviseli.

A 2014-2017 közötti időszakban a COSI hatékony lépéseket kíván tenni:

- a nagy károkozással járó, on-line és bankkártyás fizetéssel összefüggő bűncselekmények megelőzésében;
- az áldozatok részére komoly hátránnyal járó – különös tekintettel a gyermekek sérelmére elkövetett – számítógépes bűncselekmények megelőzésében;

[22] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

- a kritikus infrastruktúrát és számítógépes rendszereket érintő informatikai bűncselekmények elleni védekezés érdekében.

A COSI stratégiája kitér a lehetséges informatikai rendszerek sebezhetőségeinek és beazonosításának problematikájára is. Meghatározta az informatikai támadások elleni védelem legfontosabb problémáit. Kimondta, hogy:

- kevés, illetve nem elegendő az információ a bűnözői hálózatokról;
- hiányzik, illetve nem kellő szintű a kockázatokhoz kapcsolódó tudatosság;
- esetenként és helyenként jogi akadályok is fennállnak az információcserében;
- az elégtelen, illetve nem kellő színvonalú a bűnfelderítői együttműködés;
- elégtelen, illetve alacsony színvonalú az állam jogalkalmazó és igazságszolgáltató szerveinek felkészültsége;
- országonként eltérő formájúak az incidensek azonosítása és besorolása;
- alacsony szintű a civilszféra bevonása a bűnüldözésbe;
- jelentős hatással bírnak az Európai Unión kívüli cselekmények;
- az alacsony mértékű a felderítés;
- nem kellően hatékony a bűnelkövetők elfogása.[23]

Az **Európai Parlament** (EP) és az Európai Tanács 460/2004/EK számú rendeletében létrehozta a független státuszú **Európai Hálózat-és Információbiztonsági Ügynökséget** (ENISA). Az EU ezt azért tartotta szükségesnek, mert úgy ítélte meg, hogy az informatikai támadások, a számítógépes rendszerek elleni bűncselekmények komolyan veszélyeztetik a tagállamok állampolgárainak biztonságát, illetve évről évre egyre jelentősebb és nagyobb anyagi kárt okoznak a nemzetgazdaságoknak.

Az Ügynökség legfőbb célkitűzése, hogy „*…az EU-tagállamok és az üzleti szféra fokozottabb mértékben legyen képes a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra.”*[24]

Az Ügynökség feladatai:

- jogi és technikai segítségnyújtás és tanácsadás a tagállamok, az EP, Európai Bizottság (EB) részére;
- információk gyűjtése, kockázatelemzés és értékelés, valamint az ET, az EP, az EB és a tagállamok kijelölt szerveinek és szervezeteinek tájékoztatása;
- az együttműködésre kijelölt szervek és szervezetek közötti együttműködés elősegítése és fokozása;
- részvétel a biztonsági problémák megelőzésére szolgáló közös módszerek kidolgozásában;
- hozzájárulás a tudatosság növeléséhez;
- hozzájárulás ahhoz, hogy a hálózat- és információbiztonsággal kapcsolatos kérdésekre vonatkozóan naprakész, tárgyilagos és átfogó információk legyenek elérhetők valamennyi felhasználó számára;
- segítségnyújtás minden érintett részére az iparral folytatott, hardver- és szoftvertermékek biztonságával kapcsolatos problémákról szóló párbeszédben;
- a biztonsági termékek és szolgáltatások szabványai kialakításának nyomon követése;

[23] http://www.cert-hungary.hu/node/212 (letöltve: 2014. 09.26.)
[24] http://europa.eu/legislation_summaries/information_society/internet/l24153_hu.htm (letöltve:2014.09.26.)

- a kockázatértékelési és kockázatkezelési tevékenység előmozdítása;
- hozzájárulás az EU-n kívüli országokkal és nemzetközi szervezetekkel folytatott együttműködést célzó, uniós szintű erőfeszítésekhez;
- a biztonsági kérdésekre vonatkozó globális szemlélet terjedésének elősegítése;
- következtetések és iránymutatások megfogalmazása.[25].

Fontos szerepe van az EU bűnüldöző hatóságának, a 2010-ben ügynökséggé lett, az EU kormányközi, koordinációs és jogi végrehajtó szervezetének. az **EUROPOL**-nak, amelynek fő feladata az EU biztonságosabbá tételének segítése.

Feladatai közé tartozik:

- az EU tagállamok hatóságainak támogatása;
- a kölcsönös információ-megosztás a nemzeti rendőrségekkel;
- a különböző bűnügyi adatok szakszerű elemzése;
- a terrorizmus, a kábítószer-kereskedelem, a nemzetközi szervezett bűnözés, az ipari jog megsértése és termékhamisítás, az illegális bevándorlás, továbbá a lopott autók csempészése, a pénzmosás és az euró hamisítása elleni fellépés és megelőzés;
- a számítógépes bűnözés elleni harc.

A számítógépes bűnözés elleni harc hatékonyabbá tétele érdekében hozták létre az EUROPOL fennhatósága alatt a **Csúcstechnológiai Bűnözés Elleni Központot**.

A Központ három területen – munkacsoportokban – fejti ki tevékenységét:

- a gyermekek szexuális kizsákmányolása ellen;
- a bankkártya csalások ellen;
- a számítástechnikai bűnözés ellen.

A Csúcstechnológiai Bűnözés Elleni Központ harmadik munkacsoportjának bázisán, az EB 2012. március 28-án benyújtott javaslatára hozták létre a **Számítástechnikai Bűnözés Elleni Központot (European Cybercrime Centre, EC3).**

A számítástechnikai európai központ Hágában, az Európai Rendőrségi Hivatalon belül 2013. január 11-én kezdte meg működését. Hatásköre kiterjed a számítógépek és a hálózati infrastruktúrák ellen végrehajtott bűncselekmény kivizsgálására, beleértve a különböző internetes bűncselekmények, a gyermekek szexuális kizsákmányolásának, a bankkártyákkal történő csalások és a személyes adatokkal történő visszaélések kivizsgálását is. Létszáma 45 fő, amellyel képes a tagállamoknál folytatott nyomozások támogatására is. Önálló nyomozati jogkörrel nem rendelkezik.

A **Központ feladatai:**

- kapcsolattartó pontként a számítástechnikai bűnözés elleni küzdelemben való tevékenység;
- részvétel az unión belüli rendészeti koordinációban;
- operatív támogatással az EU tagállami rendészeti szerveinek segítése a konkrét nyomozások során;
- a számítógépes bűnözés elleni harc koordinálása, különös hangsúlyt fektetve a nagy nyereséggel járó bűnözés elleni tevékenységre;
- a személyazonosság-lopás elleni küzdelem;
- az elektronikus bankszolgáltatásokat érintő bűncselekmények elleni harc;

[25] http://europa.eu/legislation_summaries/information_society/internet/l24153_hu.htm

- a gyermekek szexuális kizsákmányolása elleni harc;
- az EU kritikus infrastruktúráinak és informatikai rendszereinek korlátozott védelme;
- a tagállamok figyelmeztetése az esetleges fenyegetettségek;
- az online szervezett bűnözői csoportok felkutatásának és azonosításának koordinálása és támogatása.

A Számítástechnikai Bűnözés Elleni Központ mellett a NATO létrehozta a **Számítógépes Védelmi Irányító Hatóságot** (Cyber Defence Management Authority – CDMA) is, amely a Brüsszel székhelyű **Számítógépes Védelmi Irányító Tanács** (Cyber Defence Management Board – CDMB) alárendeltségében látja el a szövetségi szintű, centralizált, számítógépes védelem megteremtésének és irányításának feladatait.

A **CDMA alapvető feladatai:**

- közreműködés informatikai rendszerek sérülékenységi vizsgálatainak végrehajtásában, illetve a feltárt hálózati sérülékenységek elhárításában;
- a hatáskörébe tartozó kormányzati, állami, valamint állami háttérintézmények rendelkezésre álló naplóállományainak elemzése, valamint azok hiánya esetén a szükséges munkafolyamatok kialakítása;
- közreműködés a hatáskörébe tartozó kormányzati, állami, valamint állami háttérintézmények elektronikus incidenseinek kezelésében, illetve azok rendszerein történt elektronikus visszaélések kivizsgálásában;
- az állami rendszerek üzemeltetésével összefüggésben szakértői, minőségbiztosítási tevékenység végzése;
- gondoskodás elektronikus információbiztonsági és tudatossági programok szervezéséről;
- stratégiai és taktikai együttműködés az EU és a NATO társszervezetivel, valamint a tagállamok CDMA szervezeteivel.

A Számítógépes Védelmi Irányító Hatósághoz kapcsolódva alakították ki az ún. **gyorsreagálású csoportokat** (Rapid Reaction Teams – RRT), amelyek gyorsan települve az adott országba nemzeti szinten nyújtanak segítséget a számítógépes támadások ellen.

A számítógépes szükséghelyzeteket elhárító csoportok (Computer Emergency Response Team – CERT) rendszerét a CDMA mellett alakították ki. A CERT koncepciója 1988-ban jelent meg – függetlenül a NATO-tól – a Carnegie Mellon Egyetemen, az Egyesült Államokban. A CERT tulajdonképpen egy szakértőkből álló „testület", amely a nemzeti számítógépes hálózatok felügyeletét, illetve, adott esetben védelmének kidolgozását és – a lehető leggyorsabb reagálással – annak végrehajtását végzi. Ma több mint 250 ilyen CERT létezik, beleértve a magyarországiakat is. Bevett gyakorlattá vált, hogy az államok pénzügyi támogatásával ezek a csoportok látják el a nemzeti kibervédelmi felügyeletet, ezzel is erősítve a CDMA munkáját.

A NATO Norfolkban székelő és a szövetség katonai reformjaiért felelős **Szövetséges Átalakítási Parancsnokság** (Allied Command Transformation – ACT) irányítása alatt (bár nem szervezeti eleme és nem a NATO költségvetéséből finanszírozott) működik a **Kibervédelmi Kiválósági Központot** (Cooperative Cyber Defence Centre of Excellence-CCD COE).

A kiemelt számítógépes védelmi és együttműködési központ 2008. május 14-én, az észtországi Tallinban jött létre azzal a céllal, hogy a NATO-tagállamok és partnereik

számítógépes védelmi kapacitásait erősítse a tapasztalatcsere, az oktatás és kutatás-fejlesztés eszközeivel. A világ egyik legfejlettebb számítógépes védelmi központja, amely számos tag- és más országi szervezetekkel működik együtt, olyan közös centrum, amely összegyűjti és partnereivel megosztja mindazt a nemzetközi tapasztatot és tudást, ami a 21. század informatikai biztonságának fenntartásához szükséges. Magyarország 2010-ben csatlakozott a Központhoz. Az Amerikai Egyesült Államok megfigyelő státuszban van jelenleg, de vannak olyan országok is, mint pl. Törökország, akik bejelentették csatlakozási igényüket, mint támogató államok.[26] A **Központ feladatai** közé tartozik többek között:

- jogi és kibervédelmi politika (háttértanulmányok, nemzeti és szervezeti szabályozások, átültetési és felülvizsgálati gyakorlatok, stb.) végzése és a tapasztalatok, eredmények megosztása;
- segítségnyújtás a kibervédelmi koncepciók és kíberképességek kidolgozásához és fejlesztéshez;
- stratégiai trendek és különböző típusú kiberműveletek (támadó, védekező, stb.) elemzése;
- elméleti és gyakorlati információbiztonsági oktatás, ki-, át-, és továbbképzés;
- információs és technikai infrastrukturális védelmi kutatások végzése.

[26] http://www.biztonsagpolitika.hu/?id=16&aid=1125&title=A_NATO_kiberv%C3%A9delmi_politik%C3%A1j%C3%A1nak_%C3%A1ttekint%C3%A9se 2014. Szeptember 27.