Nemzeti Közszolgálati Egyetem
Rendészetelméleti Kutatóműhely

Országos tudományos pályázat

A kiberbűnözés

Készítette: Kovács Csilla
Széchenyi István Egyetem
Deák Ferenc Állam- és Jogtudományi Kar
Jogász szak

Pápa, 2014. március

Előszó

Napjainkban szinte az életünk minden területét uralja az információtechnológiai eszközök sokasága. Már a korábban analóg jelközvetítéssel működő médiumok is digitális műsorszórással működnek. Az újabb technikai vívmányoknak köszönhetően már nemcsak a telefonjaink, de már a televízióink is „okosnak” nevezhetők.

A globális teret behálózó digitális és számítástechnikai világ nem kizárólag pozitív változásokat hozott az emberek számára. Kétségtelen tény, hogy könnyebbé és egyszerűbbé teszik mindennapjainkat, de használatuk során kiszolgáltatottá is válhatunk. A kibertérben való biztonságos munkavégzés valamint szórakozás elsősorban tudatos és körültekintő használatot követel meg tőlünk felhasználóktól.

Elsőként a dolgozat témájaként a kiberbűnözés nyomozástaktikai ajánlásait szerettem volna feldolgozni, de sajnos az eredeti elképzelésemet nemzetbiztonsági érdekből át kell gondolnom, ugyanis a taktikai ajánlások jellemzően belső utasítások, így azok titkos információnak számítanak.

Pályamunkámban elsősorban a jogi szabályozottságot, a hazai szervezetrendszert, nemzetközi viszonylatban a joghatósági és a jogalkalmazási kihívásokat próbálom felvázolni. Az elmúlt hetekben számos nemzetközi jogszabályt, irányelvet és kutatási anyagot tanulmányoztam, hogy átfogó képet kaphassak a témáról. Ahogy az eljáró hatóságok részéről elengedhetetlen a nagyfokú szakmai tudás, úgy a téma kutatójának is nehéz dolga van, ha ismeretei csupán felhasználói szintűek.

A kutatás során nagyon sok hasznos információ és tudás birtokába jutottam, melynek egy része kimaradt a dolgozatból, mert nem illett annak struktúrájába.

1. A kiberbűnözés vett védett jogi tárgya

A kiberbűnözés esetében a védett jogi tárgy az információ vagy az adat.

Az adat fogalmát a 2012. évi C. törvény a 2001-es Budapesten aláírt Cybercrime egyezménnyel összhangban határozza meg. Vagyis adat az „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."[1]

A 2013. évi L. törvény értelmezésében az adat nem más, mint „az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas"[2].

Az információtársadalom alapját az információs infrastruktúra biztosítja. Ez alatt értendő az információ előállítását, szállítását és felhasználását biztosító, szolgáló rendszerek és hálózatok, de ide kell érteni a szakszemélyzetet is, amely e rendszerek, eszközök működtetésére alkalmas.

A Cybercrime Egyezmény a számítástechnikai rendszert eképpen definiálja „minden olyan eszköz, illetőleg egymással kapcsolatban lévő vagy összekötött eszközök összessége, amelyek, illetőleg amelyeknek egy vagy több eleme egy adott programnak megfelelően adatok automatikus feldolgozását végzi".[3]

Az információs infrastruktúrát feloszthatjuk a felhasználás jellege szerint. E csoportosítás alapján beszélhetünk globális, nemzeti és védelmi jellegű információs infrastruktúráról. A globális információs infrastruktúra részét képezi minden olyan információtechnológiai eszköz, rendszer, amely globális szinten biztosítja az információ megszerzését, tárolását, feldolgozását és továbbítását. Minden nemzeti, regionális intézmény és működési rendszer, így a nemzeti információs infrastruktúra is a globális architektúra részét képezi és annak tulajdonképpen egy kicsinyített mása. A védelmi információs infrastruktúra a nemzeti rendszer részét képezi, de szervesen kapcsolódik a szövetséges védelmi struktúrákhoz is. Külön kategorizálásának szükségességét az adatok, információk specifikuma indokolja, ugyanis a védelmi célú információk megszerzését, tárolását, feldolgozását és továbbítását, megjelenítését szolgáló eszközösszesség. Ezek egy egymással összekapcsolt komplex

[1] 2012. évi C. törvény 423. § (4) bek.
[2] 2013. évi L. törvény 1. § (1) bek. 1. pont
[3] Számítástechnikai Bűnözésről Szóló Egyezmény 1. Cikk b) pont

rendszert alkotnak, melyben az információkommunikációs eszközök is fontos szerepet játszanak.

Feladat szerint funkcionális és támogató információs infrastruktúrákról beszélhetünk. A funkcionális értelemben vett osztály az ellátandó feladat jellege szerint további csoportokra osztható, ilyen például – a teljesség igénye nélkül – számítógép hálózatok, műsorszóró és lakossági tájékoztató hálózatok, nyílt előfizetői távközlési hálózat, közszolgáltató, közüzemi és közellátási érdekből üzemeltetett távközlési zárt hálózat.

A támogató információs infrastruktúra döntően a feladatok megvalósításához szükséges ellátó rendszerek halmaza.

Nemzetbiztonsági szempontból beszélhetünk kritikus és sebezhető rendszerekről. Kritikus infrastruktúraként kell értékelni minden olyan fizikai vagy információtechnológiai eszközt, hálózatot vagy szolgáltatást, amely működésének összeomlásával, illetve korlátozásával a polgárok egészsége, gazdasági jóléte, biztonsága és védelme szempontjából súlyos következményekkel járhat, továbbá veszélyezteti a kormány hatékony működését.

A kiberbűnözés jellemzően e rendszerek ellen vagy által elkövetett jogellenes magatartásformák összessége.

A szűkebb értelemben vett jogi tárgy minden esetben az adott bűncselekmény jellegétől függ.

2. Különös részi megközelítés

A nemzetközi jogalkotás által fontosnak tartott pönizálás a bűncselekmény jellegéből és az információtechnológiai eszközök gyors fejlődéséből adódóan folyamatos és inkább követő, mint prevencionális, azaz megelőző jellegű. A dolgozat terjedelmére tekintettel néhány, tipikus tényállást szeretnék bemutatni.

Az Európai Unió által készített felmérés szerinti hat leggyakoribb deliktumcsoport:

- online identitás-lopás
- számítógépes csalás
- bankkártyaadatok eltulajdonítása
- gyermekek szexuális kizsákmányolása
- online felhasználói fiókokba történő illetéktelen belépés
- köz- vagy magántulajdonú informatikai rendszerek elleni támadások[4]

[4] http://ec.europa.eu/news/justice/120328_hu.htm

A Cybercrime Egyezmény az alábbi bűncselekményeket tipizálta.

1. Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sérthetetlensége és titkossága elleni bűncselekmények
   1.1. Jogosulatlan belépés
   1.2. Jogosulatlan kifürkészés
   1.3. Számítástechnikai adat megsértése
   1.4. Számítástechnikai rendszer megsértése
   1.5. Eszközökkel való visszaélés
2. Számítógéppel kapcsolatos bűncselekmények
   2.1 Számítógéppel kapcsolatos hamisítás
   2.2 Számítógéppel kapcsolatos csalás
3. Számítástechnikai adatok tartamával kapcsolatos bűncselekmények
   3.1. Gyermekpornográfiával kapcsolatos bűncselekmény
4. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

A magyar büntetőjog öt bűncselekményt kriminalizál önálló deliktumként ugyanakkor számos bűncselekmény esetében lehetséges elkövetési formaként megemlíti a számítástechnikai eszközzel történő elkövetést. A büntetőjogi kódex kommentárja kiemeli, hogy egyes kiberbűnözés körébe tartozó elkövetői magatartások ugyan a törvény más fejezetében kerültek elhelyezésre, de a védett jogi tárgy ennek ellenére is az „információs rendszerek megfelelő működtetéséhez és az abban foglalt adatok megőrzéséhez fűződő társadalmi érdek védelme”[5]. Így e bűncselekményeknek az adott fejezetből történő kiemelése és önállóan való kezelése különösen indokolt.

2.1 Gyerekpornográfia

A 2012. évi C. törvény (Btk.) megfogalmazása alapján a „aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt megszerez vagy tart, készít, kínál, átad, hozzáférhetővé tesz, forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz bűntettet követ el.[6]

[5] 2012. évi C. törvény kommentárja
[6] 2012. évi C. törvény 204. §

Kiberbűnözés szempontjából releváns tényállási elem, hogy a pornográf felvétel információtechnológiai eszközzel készüljön, jellemzően a világhálón történő terjesztés és továbbítás, illetve az itt történő elérés, megtekintés céljából.
A Gyermekjogi Fakultatív Jegyzőkönyv, a 2011/93/EU irányelv, valamint a Lanzarote Egyezmény által meghatározott elkövetési magatartások:

Nemzetközi dokumentumok	**2012. évi C. törvény**
megszerzés (acquisition)	megszerez
- birtoklás (possession)	birtokol
- információs és kommunikációs technológia segítségével történő tudatos hozzáférés (knowingly obtaining access by means of information and communication technology)	
- felajánlás (offering)	- kínál
- továbbítás (transmission)	- átad
- terjesztés (dissemination)	
- hozzáférhetővé tétel (making available)	- hozzáférhetővé tesz, nagy nyilvánosság számára hozzáférhetővé tesz
- készítés (production)	- készít
- forgalmazás (distribution)	- forgalomba hoz, kereskedik
- biztosítás (supply)	- készítéshez, forgalomba hozatalhoz, kereskedéshez, nagy nyilvánosság számára hozzáférhetővé tételhez anyagi eszközöket szolgáltat

A 2011/93/EU irányelv büntetni rendeli a „szexuális kizsákmányolás elkövetése céljából történő találkozásra gyermeknek tett internetes ajánlat, valamint a gyermek ugyanilyen úton való késztetése őt bemutató pornográf anyag szolgáltatására” [7] irányuló kapcsolatfelvételt. A magyar jog nem önálló bűncselekményként, hanem bűncselekmény előkészületeként szankcionálja az információtechnológiai eszköz útján történő felhívást.

2.2 Információs rendszer felhasználásával elkövetett csalás

A hatályos Btk. szabályozásában, „aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi,

[7] 2011/93/EU irányelv a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről

illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő". Büntetendő az is, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt.[8]

A csalás elkövetési magatartásánál elengedhetetlen a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás, az információs rendszer felhasználásával elkövetett jogellenes magatartás esetében ez hiányzik. Mindkét cselekmény jellemzően vagyoni érdekeket sértő károkozás, azonban az információs rendszer felhasználásával elkövetett csalást e struktúra jogtalan befolyásolása eredményezi. Ebből kifolyólag az információs rendszer vagy adat megsértése szükségszerű eszközcselekménye a rendszer felhasználásával elkövetett bűncselekménynek.

2.3 Tiltott adatszerzés

Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, bűntettet követ el. A törvény büntetni rendeli az így megszerzett adat továbbítását és felhasználását is.[9]

Fontos és ezért kiemelendő, hogy a tiltott adatszerzés hasonlóságot mutat a magántitkok jogosulatlan megismerésének azon tényállásához, amikor a bűncselekményt speciális eszköz használatával valósítják meg. Az elhatárolás alapja, hogy tiltott adatszerzés 422. § (1) bekezdés d) pontja esetén maga az információ melynek megszerzésére a cselekmény realizálódik számítástechnikai rendszer ellen valósul meg, így a Számítástechnikai Bűnözésről Szóló Egyezmény rendelkezéseibe ütközik.

A tényállás elkövetési magatartásai célzatosak, ugyanis személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából történnek, erre figyelemmel kizárólag egyenes szándékkal valósíthatók meg.[10]

[8] 2012. évi C. törvény 375. §
[9] 2012. évi C törvény 422. §
[10] 2012. évi C. törvény kommentárja

A törvény a számítástechnikai rendszer kifejezés helyett az információs rendszert használja, és a 2003. évi C. törvény fogalmi meghatározását átvéve a hírközlő hálózat kifejezést építi be a hírközlő berendezés helyett.
A bűncselekmény alanya általános, azt bárki elkövetheti.

2.4 Információs rendszer vagy adat megsértése

Aki, információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad, az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz, vétséget követ el. A bűncselekmény bűntetti alakzata esetén, ezen cselekmények jelentős számú információs rendszert érintenek, illetve, közérdekű üzem ellen követik el.[11]

A jogszabály nem határozza meg az akadályozás konkrét módját, a technika gyors fejlődésére és az elkövetési módok széles spektrumára tekintettel nyitva hagyja a törvényi tényállást, így bármely cselekmény, amely a számítástechnikai rendszer működését akadályozza jogellenesnek minősül.

2.5 Információs rendszer védelmét biztosító technikai intézkedés kijátszása

Az elkövető magatartása akkor minősül jogellenesnek, ha információs rendszer vagy adat megsértéséhez, továbbá az információs rendszer felhasználásával elkövetett csaláshoz szükséges, vagy a belépést könnyítő „jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz” [12] vagy az ezek készítésére vonatkozó ismereteit rendelkezésre bocsátja.

[11] 2012. évi C. törvény 423. §
[12] 2012. évi C. törvény 424. §

Jelszó alatt „az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító”[13] értendő.

A Számítástechnikai Bűnözésről Szóló Egyezmény szövege szerint az ilyen jellegű eszköz birtoklása - ha azt bűncselekmény felhasználása érdekében tartja magánál az elkövető - önálló tényállás, ugyanakkor a Btk. a birtoklást nem szabályozza, hiszen a megszerzés már magában foglalja a dolog feletti rendelkezési jogot, amely feltételezi a birtoklást is.

3. Internet terrorizmus és kiberhadviselés

3.1 Internet terrorizmus

A kiberbűnözés e két nagy csoportját azért láttam indokoltnak önálló fejezetben tárgyalni, mert ezen cselekmények elsősorban egy állam alkotmányos rendjének, társadalmának illetve gazdaságának megzavarására irányulnak.

Az internet terrorizmus alatt az információtechnológia terrorista célú felhasználását értem. Véleményem szerint fontos megkülönböztetni a kiberterrorizmustól, illetve a hacktivizmustól. Utóbbi kettő esetében ugyan a terrorcselekményekhez hasonlóan egy ideológiai cél a motiváció, de jellemzően jelentős imázs- illetve presztízsveszteséget okozó magatartás, melyhez gazdasági kár is társulhat, azonban nem ennek elérése az elsődleges cél. Rendszerszinten vizsgálva a támadás kiterjedését sem beszélhetünk jelentős nagyságú károkozásról, hiszen az érintett rendszerek száma viszonylag alacsony.

Ezzel szemben az internet terrorizmus viszonylatában az elkövetési magatartásokat további két csoportba lehet sorolni. Az információtechnológia úgynevezett „soft” típusú használatára és ezen eszközök „hard” típusú alkalmazására.

A „soft” típusú igénybevételnél a terrorista szervezetek jellemzően történetüket írják meg, véleményüket fejtik ki, a tevékenységük népszerűsítésére és a közvélemény formálására, adománygyűjtésre, mozgósításra és még számos ehhez hasonló tevékenységre használják fel. Például az Al-Kaidának van gyermekek számára oktatási célból létrehozott oldala is, melyen ideológiai irányvonalakat, gyilkolástechnikát, erőszakot és brutalitást jelenítenek meg. Ma körülbelül 40 terrorszervezet több mint 5000 oldalt üzemeltet.

[13] 2012. évi C. törvény 424. § (3) bek.

Az információtechnológia „hard” típusú alkalmazása a szűkebb értelemben vett kiberbűncselekmények elkövetése. Itt az internetet elsősorban adathalászatra, információk eltulajdonítására, hamis információk elhelyezésére, illetve információs infrastruktúrák blokkolására használják fel.

A terrorista szervezetek viszonylag hamar felismerték az internet nyújtotta lehetőségeket és képesek a saját céljaik elérése érdekében felhasználni. A világháló tulajdonságaiból fakadó anonimitás lehetősége, az információáramlás szinte teljes lekövethetetlensége, a centralizáltság hiánya és a technika gyors fejlődése egy teljesen új harcteret nyitott a terrorizmusnak.

3.2 Kiberhadviselés

A jelenség alatt egy állam által egy másik állam ellen irányuló olyan magatartása, amelynek célja az adott ország gazdasági vagy társadalmi ellehetetlenítése, illetve korlátozása. Jellemzően hidegháborús cselekmény, de nem kizárt, hogy fegyveres támadás kísérőjeként jelenjen meg. A kibertérben elkövetett offenzíva rendszerbeli kiterjedése és az okozott kár mértéke is jelentős.

A célpont általában valamely kritikus információs infrastruktúra. A legismertebb példa a kiberhadviselésre a Stuxnet vírus, az iráni nukleáris program ellen irányuló amerikai kibernetikai támadás. A kártevő szabotálta az ipari számítógépes rendszerek működését, nem az adathalászat vagy az adatlopás, hanem az ipari rendszerben történő károkozás volt az elsődleges cél. A támadás okozta károk nagyságának – az urándúsító centrifugák jelentős része megsemmisült- eredményeként Irán leállította az urándúsítóit. Bebizonyosodott, hogy kiberbűnözés eszközei oly mértékben fejlődtek, hogy „féreg programokkal” mára a valóságban megjelenő fizikai károk okozására is alkalmassá váltak.

A fenti példából is jól látható, hogy a kiberhadviselés a modern háború kezdete lehet. Egy olyan érdekérvényesítő eszközzé nőheti ki magát, amely a kiberbűnözők által kifejlesztett, illetve alkalmazott technikákat állami, nemzeti szintre emeli. A kiberhadviselés egyik korlátját az adott nemzeti kormány morálja határozza meg, vagyis az, hogy mit képes megtenni a céljainak elérése érdekében. A másik tényező, amely befolyásolja az ország kibernetikai értelemben vett hadseregének erejét, az a rendelkezésre álló anyagi erőforrás, az infrastruktúra és a megfelelő tudással és lojalitással rendelkező informatikai szakemberek mennyisége.

A fegyveres hadviselés tipikus eszköztárát felhasználó offenzíva, mely csak abban tér el a klasszikus értelemben vett háborútól, hogy a kibertérben folyik. Így beszélhetünk hálózati-felderítésről, támadásról és védelemről is.

Magyarországon - bár nemzetbiztonsági ismereteim e szempontból a titkosságuk miatt hiányosak- a felderítés és a védelem az elsődleges. Míg az interneten elérhető anyagokból az USA vonatkozásában arra a következtetésre jutottam, hogy elsődleges eszköz a támadás volt, majd az utóbbi években megszaporodó információtechnológiai eszközzel elkövetett kritikus információs infrastruktúrát – elsősorban pénzügyi intézeteket és energetikai rendszereket-érintő támadások hatására a prioritás a védelemi eszközöké lett.

4. A bűncselekmény alanya

A bűncselekmény elkövetője és sértettje bárki lehet. Mindkét oldalon állhat természetes és jogi személy is. A Cybercire Egyezmény kifejezett célként rögzíti, hogy törekedni kell a jogi személyek által elkövetett deliktumok esetében is a felelősségre vonhatóság megteremtésére.

Potenciális elkövető bárki lehet, aki a kiberteret használja és az ismeretei valamint a technikai háttere adott hozzá. Az elkövetők csoportjainak egyik felosztása szerint az alábbi kategóriákról beszélhetünk:

- Hackerek: olyan számítástechnikában jártas emberek, akik egy adott rendszer gyenge pontjait keresve az internet használatával védett adatokhoz, információkhoz férhetnek hozzá. A klasszikus hacker kerüli a rendszer működésében, illetve az adatban való károkozás lehetőségét.
- Crackerek: A rendszerekbe történő bejutás haszonszerzési céllal történik és az információhoz, adathoz való hozzáférés során nem foglalkoztatja a rendszer működőképességének megőrzése.
- Vírusírók: Tevékenységük során olyan kódokat állítanak elő, amelyek adott rendszerbe történő behatolásukat segíti elő, a vírus negatív, kártékony hatásával kifejezetten számolnak.
- Kalózok: A crackerekből kivált csoport, mely kifejezetten szoftverek biztonsági rendszerek feltörésére specializálódott
- Cypherpunkok: Programjaik használatával jelentősen megnő az adatok titkosításának, rendszerekben történő adatbújtatásoknak a lehetősége. Az ilyen jelszavakkal védett adatokhoz sok esetben lehetetlen a hozzáférés

- Anarchisták
- Terroristák

Az ENSZ kriminológiai kutató szerve az UNICRI (United Nations Interregional Crime and Justice Research Institute) egy 1200 kérdőíves kutatást végzett, melynek fő célja a hacker-típusok profiljainak megalkotása volt. A kapott válaszok alapján kilenc profilt alkottak.

- wannabe lamer: A csoport ismérve, hogy más hackerek által megírt programokat töltenek le és a felhasználáshoz kapott utasításokat követik tevékenységük során. Képzettségüket tekintve még nem magasan kvalifikáltak, elsődleges motivációjuk sem más, minthogy egyszer hackerek lehessenek. Sok esetben internetes fórumszobákban kérnek segítséget tapasztaltabb társuktól a tanuláshoz, fejlődéshez. Célpontjaikat általában nem tudatosan választják
- script kiddie: Szintén hacker programok letöltése, felhasználása és nem saját programok készítése jellemző rájuk. Az előző csoport tagjaival ellentétben a „script kiddie”-t nem érdekli a tanulás, az ehhez szükséges technikai készség és kifinomultság a legtöbbször hiányzik. Legfőbb motivációjuk a rombolás.
- cracker: Főtevékenységi körük az adathalászat az információszerzés, melyet gazdasági előnyszerzés céljából, tudatosan választott célpontok sérelmére követnek el. Közepesen képzett, de jó technikai készséggel rendelkező fiatalokból és idősebbekből álló társulat. Tagjai közepes technikai és gazdasági háttérrel rendelkeznek.
- etikus hacker: Megítélésük az informatikabiztonsági piacon és az illegális informatikai világban nem egyértelmű, számtalan vitát generál a felhasználhatóságuk, hiszen előéletüket tekintve nagy vaslószínűséggel „rosszfiúk” voltak. Kiváló szaktudással rendelkező informatikusok csoportja, akik arra vállalkoznak, hogy megbízójuk rendszerének gyenge pontjait keresve próbáljanak az infrastruktúra sebezhetőségéről átfogó képet adni. Tipikusan saját programokat írnak, alkotó hackerek. Kivételes estekben javítanak fel korábban más által alkotott szoftvereket. Támadásuk kivitelezése során a prioritás a kézi behatolásé az automatizált rendszereket nem szívesen használják, hiszen minden rendszerbe alapos körültekintéssel törnek be. Az etikus hackerek rendkívül bonyolult és specializált különböző operációs rendszerek használnak. Magas technikai és gazdasági háttérrel rendelkeznek.
- képzett csendes-paranoid hacker: Kvalifikáltsága és képessége hasonló az etikus hackeréhez. A támadók e csoportja általában IT rendszereket támad, de nem

információt keresnek, inkább a kihívás motiválja őket, hogy bejuthatnak a rendszerbe. Ha a támadások során a legapróbb jelét is észlelik annak, hogy figyelik és elkaphatják őket, eltűnnek. Saját maguk által írt szoftvereket használnak.

- kiberharcos: Ez az egyik olyan kategória, amelyet meg az elmúlt években, az internet globalizációja és a hacktivisták megjelenése hívott életre. A kiberharcosok hősök a saját környezetükben, azaz egy szélsőséges politikai vagy vallási háttérrel rendelkező csoporthoz tartoznak. Informatikai készségeik lényegesen eltérhetnek egymástól, a csupán alapképzettséggel rendelkező és a kiválóan képzett hackerekig szinte minden típus megtalálható. Jutalék ellenében is dolgozik és a pénz fejében konkrét célokat támad.
- ipari kém: A gyakorlat és a tapasztalat is azt mutatta, hogy ipari kémek mindig is léteztek, míg korábban papíron, mikrofilmen szerezték meg a kívánt információt, úgy az információtechnológiai fejlődés hatására, ma már új lehetőségek nyíltak meg. Magasan képzettek, jó technikai és anyagi háttérrel rendelkeznek.
- kormányügynök: Napjainkban a meglévő informatikai rendszer, az internet és annak tagoltsága, felépítése teszi lehetővé a kormányok számára, hogy rendkívül kifinomult támadásokat hajtsanak végre, melyek konkrét nemzetek, illetve a "know-how” üzleti piacok szereplői ellen irányulnak. A technikai és gazdasági háttér az adott ország pénzügyi helyzetétől függ.
- katonai hacker: Az "államilag támogatott támadás", vagyis a kiberhadviselés logikája szerint támadások mögött katonai hackerek állnak, egyes feltevések szerint akár a kormányügynökökkel közösen.

Raoul Chiesa az UNICRI a kiberbűnőzés vezető tanácsadója szerint az elkészült profilok nem alkalmasak arra, hogy vakon követhessük őket, de egy esetleges nyomozás során profilalkotási alapnak, vagy saját információs infrastruktúránk kialakításánál nagy segítséget nyújthat. Alapul véve, hogy a tanulmány kérdőíves felmérése 2004-ben kezdődött és 2010-ben fejeződött be, lehetséges, hogy egy ma készülő felmérés újabb profilokat is létrehozna, mely az információtechnológia gyors fejlődésének és egyre szélesebb körű használatának lenne köszönhető.

A bűncselekmény elkövetésének célja szerinti elkövetők 3 kategóriáját tartja kiemelkedően fontosnak Nemzetközi Kiberbűnözés Nyomozási Képzési Központ elnöke.

- Azon elkövetők csoportját, akik gazdasági előnyszerzés céljából tevékenykednek. A kategória legismertebb csoportosulása a román Râmnicu Vâlcea városához köthető, bár

a kibertérben csak Hackerville-ként emlegetik. Az online csalásra és a cégek ellen irányuló káros szoftver támadásokra specializálódott bűnözök több 10 millió dollárral károsították áldozataikat.

- A hacktivisták körébe azon elkövetők tartoznak, akiknek elsődleges célja nem gazdasági előnyszerzés, hanem mozgalmak szervezése és az ideológiájukkal összhangban megvalósított számítógépes offenzívák megvalósítása, rendszerek működésének blokkolása. Legismertebb hacktivista csoport az Anonymus, mely a működéseihez és a weboldalának üzemeltetéséhez szükséges anyagi forrás jelentős részét is a világhálón, adományokból gyűjti össze.
- Harmadik kategória a korábban már kifejtett kiberhadviselés, bár jelen kategória az általam értelmezettnél kissé tágabb körben értelmezendő, hiszen nem csak a nemzeti kormányok egymás elleni viszonyában, hanem a szervezetek egymás közötti, illetve szervezetek és államok viszonylatában is értékelendő információtechnológiai eszközökkel megvalósított támadás is minősülhet kiberhadviselésnek, amennyiben a cél az „ellenség” gazdasági-, társadalmi rendjének a veszélyeztetése.

A bűncselekmény sértettje is bárki lehet, aki információtechnológiai eszközt használ. A használat alatt értendő számos tevékenység, magatartás, amellyel könnyen áldozatokká válhatunk. Például online bankolás, adatainak nem biztosítunk kellő védelmet a kibertérben, meghatározott rendszerek helytelen használata stb.
Kiemelendő, hogy a biztonság kialakítása a kiberterünkben az elsődleges feladat ahhoz, hogy ne válhassunk sértetté.

5. Szabályozás és intézményrendszer a hazai jogban

5.1 Jogszabályi háttér

Az Alaptörvényben rögzített alapjogokat a kibertér használata közben sem lehet megsérteni, így nem jogszabályként, de jogforrásként ez az egyik legfontosabb dokumentum.
Természetesen a nemzetközi egyezményeket sem lehet figyelmen kívül hagyni, de ezt egy külön részben a nemzetközi szabályozás ismeretetésének keretében mutatnám be. A hazai jogi szabályozás esetében a számomra legfontosabbnak tartott rendeletet mutatnám be, míg az

Információbiztonságról szóló törvényt a szervezetrendszer bemutatásával összekötve ismertetném.

Az 1139/2013. (III.21.) Kormányrendelet Magyarország nemzeti kiberbiztonsági stratégiája, melynek elsődleges célja, hogy Magyarország érvényesíteni tudja a nemzet érdekét a globális kibertérben, különös tekintettel az ennek részét képező magyar kibertérben. Továbbá fontos, hogy a szabad és biztonságos környezetet alakítson ki az állam, melynek keretében együttműködik más államokkal és nemzetközi szervezetekkel is, úgy, hogy közben figyelemmel van a nemzeti szuverenitásra és a magyar érdekekre.

A rendelet megalkotásánál a nemzetbiztonsági stratégiáról szóló 1035./2012. (II.2.) Korm. rendeletet vonatkozó részeinek, az Európai Parlament 2012. november 22-én elfogadott kiberbiztonságról és védelméről szóló állásfoglalásának és az Európai Unió kiberbiztonsági stratégiájának elveit és előírásait is figyelembe vették. A jogszabály összhangban a nemzetközi irányelvekkel a fontosabb területeken követelményeket állított fel azért, hogy a világháló megbízható és biztonságos lehessen.

- az egyének és a közösségek személyes adatainak védelme, ezzel is segítve az integrációt
- az innovativitás lehetőségének megteremtése a gazdasági szereplők számára, melyhez szükséges az adatok és üzleti titkok, technológiák megfelelő védelme
- a jövő generációi számára a kibertér akkor biztonságos, ha nem hat károsan a lelki fejlődésükre és sérülésmentesen gyűjthetnek tapasztalatokat és tudást az interneten
- kardinális pont az állami szolgáltatások fejlesztése, vagyis a közigazgatásban megjelenő elektronikus ügyintés során és az adatbázisokban tárolt adatok védelme
- nemzetbiztonsági érdek, hogy a válsághelyzet hatékony kezelése és a felhasználás a védelem szempontjából a megfelelő összhangban legyen.

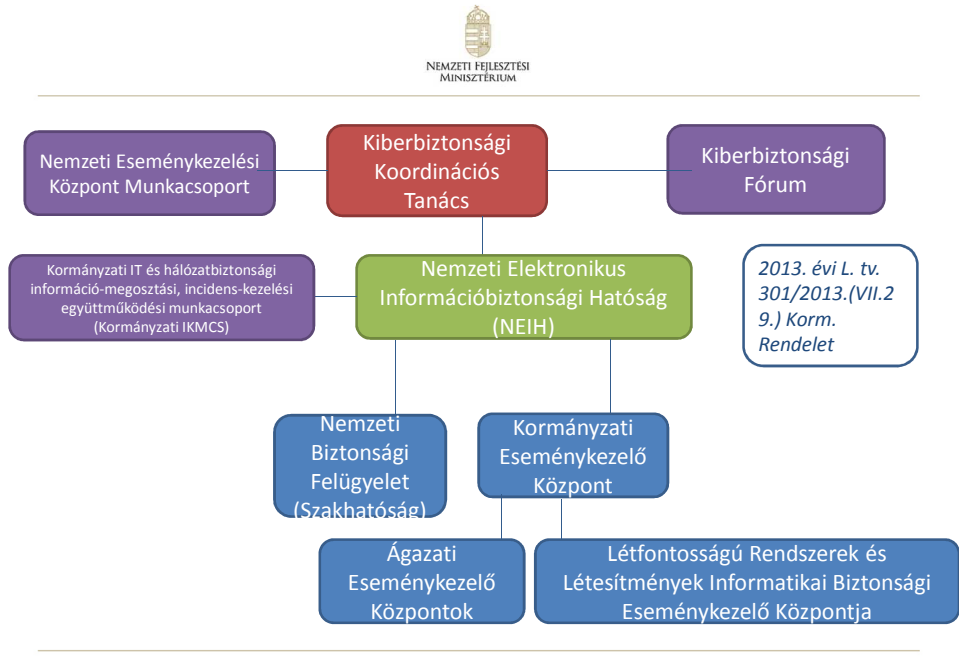
Szükséges feladatként meghatározott állami feladatok:

- kormányzati koordináció, ennek eleget téve létrejött a Nemzeti Kiberbiztonsági Koordinációs Tanács
- együttműködés a kormányzati és nem kormányzati szervekkel, legfőbb célja a hatékony és gyors információcsere
- szakosított intézmények létrehozása, melyben specifikus szakértelemmel rendelkező személyek a megfelelő határkörrel rendelkező szervnél úgy dolgozhatnak, hogy a nem kizárólag egymással, hanem az adat- és titokvédelmi területek hatósági feladatot ellátó szervekkel is együttműködnek
- a jogi háttér megteremtése

- nemzetközi együttműködés
- tudatosság kialakítása, ennek érdekében fórumok megszervezése és a gyakorlati tudás megszerzése
- oktatás, kutatás, fejlesztés
- gyerekvédelemi feladat keretében a Gyerekbarát Internet Európai Unió Stratégiájának célkitűzésit valósította meg, amikor létrehozta a Gyermekvédelmi Internet-kerekasztalt
- a gazdasági szereplők motiválása, hogy a hazai és nemzetközi biztonsági követelményeknek megfeleljen

5.2 Szervezetrendszer

Az jobb áttekinthetőség érdekében a nemzeti szervezetrendszert az alábbi ábrával szemléltetném.



[14]

A Kiberbiztonsági Koordinációs Tanácsot feladatai végrehajtásában ágazati és funkcionális kiberbiztonsági munkacsoportok segítik a jogszabályban előírt kötelező területeken, melyek az eseménykezelés, belbiztonság, e-közigazgatás, energetika és a gyermekvédelem. A felmerülő problémák jellegétől függően további munkacsoportokat is

[14] http://www.kurt.hu/wp-content/uploads/2013/11/NEIH_szerepe.pdf

létrehozhat a Tanács. A Tanács feladata a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken a kormányzati tevékenység koordinációját elősegítése és annak végrehajtását ellenőrizze és felügyelje. A cselekvési területekhez kormányzati intézkedéseket tartalmazó akcióterv kidolgozásának elkészítése és annak évenkénti felülvizsgálata is a Tanács szerveinek hatáskörébe tartozik.

A Kiberbiztonsági Fórum dolgozza ki az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját, ezek követelményrendszerét. Gondoskodik arról, hogy a vezetők és az elektronikus információs rendszer biztonságáért felelős személyek és a szervezeti egységek munkatársai a képzéseken évente részt vegyenek. Kibervédelmi gyakorlatokat szervez és azok lebonyolításában aktív szerepet vállal.

Nemzeti Eseménykezelési Központ Munkacsoport legfontosabb feladata az ágazati kiberbiztonsági szabályok megtervezése, az ágazatok között kialakult konfliktusok kezelése és felelősségviselési szabályainak megállapítása. Az ügyfelek és a hatóságok tekintetében is pontos és naprakész nyilvántartások vezetése. Prevencionális tevékenysége keretében állásfoglalások, ajánlások, publikációk kiadása valamint védelmi gyakorlatok szervezése és az ügyfelek számára sérülékenység kockázati besorolást végez.

Eseménykezelési tevékenységének ellátásához 24 órás ügyeletet működtet. Incidens bejelentése esetén annak kezelését koordinálja, ha szükséges beavatkozik és a gyanús eseteket minden esetben kivizsgálja.

Nemzeti Elektronikus Információbiztonsági Hatóság feladatai:

- az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala
- az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése
- az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése
- a rendelkezésre álló információk alapján kockázatelemzés elvégzése
- a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása
- javaslattétel a létfontosságú rendszerek és létesítmények védelmi szabályozását biztosító, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére,

- az információs társadalom biztonságtudatosságának elősegítése és támogatása,
- együttműködés a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvényben meghatározott elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,
- kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,
- kapcsolattartás a Nemzeti Média- és Hírközlési Hatósággal, továbbá a kormányzati eseménykezelő központtal és az ágazati eseménykezelő központokkal, a kormányzati incidens-kezelő munkacsoport irányítása,
- véleményezési jog gyakorlása a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,
- együttműködés a kormányzati eseménykezelő központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal,
- együttműködés a Nemzeti Média- és Hírközlési Hatósággal és a Nemzeti Biztonsági Felügyelettel, ha a biztonsági esemény vagy fenyegetés a hatáskörük alá tartozó szervet vagy szolgáltatót érinti
- éves és egyedi jelentések készítése a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban
- feladatának ellátása során a Nemzeti Biztonsági Felügyelet szakhatóságként jár el[15]
- nyilvántartást vezet
- folyamatos kapcsolattartás más hatóságokkal

A NEIH véleményezési jogkörrel rendelkezik a Kormányzati Eseménykezelő Központ azon tervezete tekintetében, amely az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szól.

A Gyermekvédelmi Internet-kerekasztal piaci, állami és civil delegáltakból álló munkacsoport. Általános és egyedi ügyekben is állásfoglalásokat kidolgozó hatóságként működik. Elsődleges célja, hogy a gyermekek védelme a világhálón, a piaci szereplők ez irányú ösztönzése elsősorban a szűrőprogramokat kifejlesztő szoftvergyártóké, valamint a szülőkben és a gyermekekben a tudatos, biztonságos használat kialakítása.

[15] 2013. évi L. törvény 15.§ (2) bek.

6. Nemzetközi szabályozás

6.1 Nemzetközi jogszabályok

Az Európai Parlament által 2012. november 22-én elfogadott, a kiberbiztonságról és védelemről szóló, 2012/2096 (INI) számú határozata, mely megállapítja, hogy Uniós szintű szabályozásra és koordinációra van szükség a kibertér biztonsága érdekében, mivel egyre gyakoribbak a támadások és ezek nem kizárólag a piaci szereplőket, hanem állami és honvédelmi, nemzetbiztonsági szerveket is érintenek. A hatékony védelemhez globális szinten elfogadott irányelvekre, szabályozásra és fogalom meghatározásra van szükség. Felhívja a figyelmet, hogy fontos az Európai Védelmi Ügynökséggel, a NATO-val és az Amerikai Egyesült Államokkal való együttműködés a bűnüldözés és a bűnmegelőzés hatékonyságának növelése érdekében. Ösztönzi a tagállamokat, hogy katonai, nemzetbiztonsági struktúrájukon belül hozzanak létre külön kiberbiztonsági és kibervédelmi egységeket. Az így létrejött szervek nemzetközi szinten is működjenek együtt. A köz- és magánszféra együttműködésének fontosságára is kitér a határozat a kritikus információs infrastruktúrák biztonságos működtetésének kapcsán.

Az Európai Bizottság és az Európai Unió közös kül-és biztonságpolitikájának főképviselője által 2013. február 7-én "Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleménye. A hálózat- és információbiztonsági irányelvjavaslat – melynek számos rendelkezését a 2012. évi C. törvény megalkotásakor már figyelembe vettek- az Európai Unió szabályozási szintjén átfogó stratégia a kiberbűnözés visszaszorítása érdekében. Az irányelvjavaslat néhány intézkedési javaslata

- a tagállamoknak el kell fogadniuk a hálózat- és információbiztonsági stratégiát, ki kell jelölnie minden tagállamnak a biztonságért felelős hatóságot és az ehhez szükséges anyagi, humán és szervezeti struktúrát biztosítania kell
- a tagállamok és a Bizottság közötti együttműködési mechanizmus kidolgozása elengedhetetlen, továbbá amelynek célja, hogy megfelelő szakértelemmel és szervezetrendszerrel rendelkező hálózatot építsenek ki a hatékony előrejelzés érdekében
- a néhány ágazatban – jellemzően a kulcsfontosságú infrastruktúrák- és a közigazgatási hivataloknak kockázatkezelési képzésen és gyakorlatokon kell részt vennie. Ha akad olyan kockázati tényező, amelyre nincs kidolgozott akcióterv, akkor azt jelezniük kell.

Az Európa Tanács számítástechnikai bűnözéssel szembeni, 2001. november 23-i budapesti egyezmény (Cybercrime Convention), döntően anyagi és eljárásjogi szabályokat tartalmaz, kvázi számítástechnikai büntetőtörvénykönyv. A jogszabály rendelkezéseiről már a korábbi fejezetekben is szót ejtettem, így nem fejteném ki részletesen. Ugyanakkor hangsúlyozni szeretném, hogy anyagi és eljárásjogi szabályai lévén nagyon fontos dokumentum a világhálón elkövetett bűncselekményekkel kapcsolatos tényállások meghatározásánál eljárások lebonyolításában és nem utolsó sorban a nemzeti büntetőkódexek megalkotásánál.
Számos további dokumentum segíti a harcot az információtechnológiai a teljesség igénye nélkül ilyen még:

- A kritikus információs infrastruktúrák védelméről szóló, 2011. május 27-i tanácsi következtetésekre és a kiberbiztonságról szóló korábbi tanácsi következtetése,
- A Bizottság Közleményéhez az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és Szociális bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről
- Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása

6.2 Néhány fontosabb nemzetközi szervezet

A European Cybercrime Centre (EC3 - Európai Kiberbűnözés Elleni Központ) az EUROPOL keretein belül állították fel, és 2013 januárjában kezdte meg tényleges működését. A Központ a elsősorban a bűnszervezetek, bűnszövetségek által megvalósított kibertámadásokra fókuszál. Különösen tekintettel, a kiemelkedően nagy kárt okozó online csalásokra, illetve a gyermekek szexuális kizsákmányolására, és amelyek célpontjai az EU-n belüli kritikus infrastruktúrák illetve információs rendszerek. A szervezet együttműködik a kiberbűnözésben eljáró hatóságokkal, a tagállamok nyomozati szerveivel, nemzetközi bűnüldöző hatóságokkal és a civil szférával is. Feladatkörébe tartozik egy olyan információs infrastruktúra kialakítása, melyben a vele együttműködő szervezetektől származó minden adat rögzítésre kerül és visszakereshető a kiberbűnözésre vonatkozóan. Az információs központ biztosítása mellett műveleti támogatást és a szakértői bizonyítás területén kutatási-fejlesztési támogatást nyújt.

Az ENSZ kriminológiai kutató szerve az UNICRI (United Nations Interregional Crime and Justice Research Institute) ugyan nem kizárólag a kibertérrel és az abban elkövetett bűncselekményekkel foglalkozik, de számos kutatásában foglalkozik a kérdéssel. A korábban

már kifejtett profilalkotási tevékenysége nagyban megkönnyíti a bűnüldöző hatóságok munkáját.

7. A bűnüldözés problematikája és kihívásai

Elsőként említeném a digitális bizonyítékok problémáját, melyek egyrészről könnyen manipulálhatóak, másrészről beszerzésük komoly nehézségekbe ütközik. Az IP címről, mely az interneten való közlekedés rendszámtáblája. A szolgáltató által kiosztott IP cím tárolja az internetre csatlakozás helyét, idejét, a használt operációs rendszer és böngésző típusát. Elsődleges célja az ellenőrzés lehetőségének megteremtése volt, azonban egy egyszerű proxy szerver használatával viszonylag könnyen kijátszható. A láthatóság ilyen formán történő kijátszásra egy többmilliós felhasználóbázissal rendelkező ingyenes szolgáltatás is épül, melyet Onion network-nek (Tor) neveznek. Ez az internet sötét oldalának is nevezett tárhely, ahol szinte csak titkosított weboldalak találhatóak, továbbá a forrásai és a látogatói is visszakereshetetlenek.

Második kihívásként a titkosítás lehetősége. A különböző biztonsági szintű jelszavak feltöréséhez hol több, hol kevesebb idő szükséges. A titkosítással védett adatokhoz történő hozzáférés azonban nagyon sok esetben lehetetlen.

A szteganográfia az adatelrejtés és titkosítás egyik bevált módszere a világhálón. Sztereogrammok esetén első ránézésre ismétlődő mintákat látunk, amennyiben megfelelő technikával nézzük háromdimenziós képet láthatunk. A módszer alkalmazása során képekbe mentik el az adatokat. Az emberi szem számára a nem érzékelhető részeket kivéve extra információ tárolására alkalmas helyhez jutnak a felhasználók, így a kép eredeti méretének megtartása mellett, úgy képesek elrejteni az információt, hogy a kép első ránézésre eredetinek tűnik. E technológia felfedésére külön technikai megoldások léteznek.

Jelentős kihívás az is, hogy az irányítás lehetősége csökken, hiszen a világháló egy decentralizált rendszer és rendszerhálók összessége. Az információcsere éppen erre a technológiára épül. A működése során az üzeneteket, információkat adatdarabokra bontja, melyek külön szervereken jutnak el a címzetthez, ahol ismét egy egésszé állnak össze. Jelentősége ennek, hogy ha egy-egy adatdarab elveszik, az üzenet rekonstruálható marad ugyanakkor maga a törzsszöveg követhetetlenné válik.

Az Internet-szolgáltatók és a bűnüldöző hatóságok együttműködésének problémája. A nagy cégek közül a Microsoft, a Google és a Facebook következetesen segítik a hatóságok munkáját. A Yahoo! ellenben következetesen elzárkózik az együttműködéstől.

Adatszolgáltatási kötelezettségének teljesítésére kötelezés esetén az eljárás abban az országban is megindítható, ahol a szolgáltató nem rendelkezik telephellyel, fiókteleppel vagy székhellyel. Ilyen eljárások joghatóságát megalapozza, ha az adott országban szolgáltatást nyújt.

A probléma másik oldalát az jelenti, hogy a megkereső hatóságok nem megfelelően nyújtják be adatszolgáltatási kérelmüket. Ilyen hibák lehetnek:

- nem világos, hogy mi indokolja az adatkérést
- nincs megjelölve a jogszabályi háttér
- a fentiek tisztázására irányuló viszont-megkeresésre sem egyértelmű a válasz vagy nincs is válasz

8. Joghatósági, jogalkalmazási kérdések

A joghatóság kérdése a felhő-alapú (clouding) szolgáltatások kapcsán merül fel a leggyakrabban . A joghatóság megállapításának egyik logikája az, hogy „A felhő ott van, ahol én vagyok.” E szerint ahonnan a hatóság hozzá tud férni a távoli szervereken (felhőben) tárolt adatokhoz, ott joghatósággal is rendelkezik. A gyakorlatban ez azt eredményezheti, hogy ha valamely más ország joghatóság hiányára hivatkozik, akkor azt ennek az országnak kell bizonyítania. Ezen logika egyetlen korlátja az, hogy az így megszerzett bizonyítékokat nem lehet az eredeti szerverről eltávolítani.

A másik logikai megközelítés szerint a joghatóság alapja a szerver helye, ez azonban a felhő-alapú szolgáltatásoknál nem egyértelmű, hiszen az szerverek összekapcsolt rendszere.

A Budapesti Egyezmény alapján a joghatóságot meghatározza

- ha az elkövetés helye az államterülete, vagy kvázi állami területnek minősül,
- ha az állam polgára követi el a cselekményt, amennyiben az az elkövetés helye szerinti büntető törvénybe ütközik
- vagy a cselekményt bármely állam területén kívül esően követték el.[16]

E konkrét szabályokkal szemben az EUROJUST kisegítő elvei szerint a joghatóságot megalapozhatja a terhelt tartózkodási helye, a bizonyítékok rendelkezésre állásának a helye, a sértettek érdekei, költségek stb.

[16] Számítástechnikai Bűnözésről Szóló Egyezmény III. Fejezet 22.cikk

Vitathatatlan tény, hogy közvetlen, határokon átnyúló hozzáférésre van szükség ahhoz, hogy a kiberbűnüldözés sikeres legyen különösen a felhő alapú rendszerek és a bűnözői számítástechnikai rendszerek esetén nincs idő joghatósági viták lefolytatására. Az univerzális, területi hatályra vonatkozó alapelvek nemzeti jogrendszerekbe történő beültetése elkerülhetetlen.

Jogalkalmazási szempontból kimondottan előnytelen, hogy nincs egzakt fogalma az internetnek, továbbá nem elhanyagolható az a hátrány sem, amely abból származik, hogy az adattovábbítás az adatok másolásával történik, és annak áramlása nem irányítható vagy ellenőrizhető pusztán a nemzeti szabályozások alkalmazásával.

A gyermekpornográfiával kapcsolatban felmerülő kérdés, hogy mely csatorna, vagy felület lehet a pornográf felvétel hordozója. Fényképek, filmek tekintetében egyértelműen meghatározható, azonban a hanganyag és a számítógéppel generált képek esetében már nem olyan egyértelmű. Felmerülő probléma, hogy ezek az oldalak jellemzően az internet sötét oldalán találhatóak megnehezítve, ellehetetlenítve a visszakövethetőséget és az azonosíthatóságot. A gyermekek internetes szexuális kizsákmányolása esetén magas a látencia, a feljelentés szinte minden esetben elmarad. Az elkövetők kilétének felfedése általában fedett nyomozók titkos chatszobákban történő beszélgetései során „rajtaütéssel” történik.

A tradicionális területek mellett, egy negyedik is megjelent ez a kibertér. A világháló területi hatályára vonatkozó jogalkotásnál figyelemmel kell lenni arra, hogy a bűnüldözés során a hatóságok ne ütközzenek a nemzeti jogok által fenntartott, elavult szabályokba.

Konklúzió

Napjainkban az információtechnológia gyorsütemű fejlődése miatt folyamatosan változó elkövetői magatartás mellett új bűncselekmények jelennek meg. A legnagyobb problémát mégis a jogalkotás lassú reakciója és a cselekmények kriminalizálása elhúzódik.

Újabb megoldásként előbb regionális, majd globális stratégia kidolgozása és az akciótervek kivitelezésének összehangolása lehet a kulcs. Ennek érdekében az Európai Unió már megalkotta kiberbiztonsági stratégiáját és a tagállamokat is kötelezte a nemzeti stratégiák megalkotására, melyben a nemzetközi taktikai elemek is megjelennek.

A joghatósági és a jogalkalmazási elvek egységesítése elengedhetetlen. Míg a brit büntetőeljárásban az elkövető köteles a saját email fiókjának és közösségi oldalakon használt felhasználónevének és jelszavának átadására, addig például a magyar eljárásban nem kötelezhető az eljárás alá vont személy, hogy saját maga ellen terhelő bizonyítékot szolgáltasson. Felmerülhet az a kérdés, hogy más nemzetiségű elkövetők esetén kötelezhető e a terhelt saját magára nézve terhelő bizonyítékot szolgáltatni, ha a nemzeti joga kimondja, hogy nem kötelezhető rá.

Személy szerint egyetértek Stein Schjolberg bíró véleményével, hogy az anomáliák elkerülése végett egy új jogalkalmazói szervet a Kibertér Nemzetközi Büntető Törvényszékét kellene létrehozni az ENSZ égisze alatt. A nemzetközi vonatkozású kibertámadások esetére, egy egységes vádhatóság a nemzetközi nyomozó illetve ügyészi szerv felállítása, illetve a kibertérre hatályos nemzetközi büntetőjogi normák megalkotása egységesíthetné az eljárásokat. A Törvényszék mellett működő ügyészi hatóság független szerv lenne, nem emelhetne kifogást a nyomozások megindítása miatt, azonban fellebbezési joga lenne az ítéletek ellen.

Az adatok, információk titkosításának megoldására jogszabályi korlát felállítása, illetve a szolgáltatók olyan irányú kötelezése jöhet szóba, hogy az ilyen védelemmel ellátott rendszerekbe egy kiskaput építsenek.

A legérzékenyebb pont a felügyeleti, nyomozati és jogalkalmazói szervek nem megfelelő szakmai képzettsége. A kiberbűnözés felderítése és az eljárás is nagyfokú információtechnológiai tudást követel meg. Bár az Európai Unió irányelvei és a magyar jogalkotás is célként tűzte ki hatóságok megfelelő ismereteinek biztosítását és ezek gyakorlati alkalmazásának képességét, jelenleg azonban még akadnak problémák ezen a területen.

Tartalomjegyzék

Felhasznált irodalom

1035./2012. (II.2.) Korm.

1139/2013. (III.21.) Kormányhatározat

2003. évi C. törvény

2011/92/EU irányelv

2011/93/EU irányelv

2012 évi C. törvény

2013. évi L törvény

484/2013. (XII. 17.) Korm. rendelet

Európai Parlament 2012/2096 (INI) számú határozata

Gyermekjogi Fakultatív Jegyzőkönyv

http://ec.europa.eu/home-affairs/doc_centre/crime/docs/Communication%20-%20European%20Cybercrime%20Centre.pdf

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

http://europa.eu/rapid/press-release_IP-13-94_hu.htm

http://hadmernok.hu/2013_1_szentgalig.pdf

http://hadmernok.hu/archivum/2008/2/2008_2_kovacsl.pdf

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/12/09/2013%20-%200376/p7_ta-prov%282013%290376_hu.pdf

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-489.358+01+DOC+PDF+V0//HU&language=HU

http://www.hadmernok.hu/2010_2_szegedine1.pdf

http://www.kurt.hu/wp-content/uploads/2013/11/NEIH_szerepe.pdf

http://www.unicri.it/special_topics/cyber_threats/cyber_crime/

http://www.unicri.it/special_topics/cyber_threats/hackers_profiling/

http://www.zmne.hu/dokisk/hadtud/terror/lekt_Haig_Zsolt.pdf

Lanzarote Egyezmény

Nagy Zoltán Attila CISM: A NEIH (Nemzeti Elektronikus Információbiztonsági Hatóság) megalakulása, ISCD 2013 Balatonöszöd

Számítástechnikai Bűnözésről Szóló Egyezmény