A rendészeti szervek együttműködése a kiberbűnözés ellen[1]

Simon Béla[2]

Absztrakt:

A szerző célja annak vizsgálata, hogy a magyar rendészeti szervek milyen kapcsolatban állnak egymással a kiberbűnözés elleni fellépés során. A vizsgálathoz áttekintette a törvényi rendelkezéseket és egyéb szabályozókat, megvizsgálta az elérhető statisztikai adatokat, illetve interjúkat folytatott az érintett szervezetek munkatársaival, vezetőivel. A kutatás megállapítása, hogy a rendészeti szervek számára az Alaptörvény és a Kiberbiztonsági Stratégia elvi iránymutatásai, és a Büntető Törvénykönyv tényállásain kívül nincsenek szabályozók, akciótervek, feladatszabások, módszertani utasítások, melyek a feladatokat, felelősöket és esetlegesen határidőket rögzítenének.

Kulcsszavak: magyar rendészeti szervek, kiberbűnözés, együttműködés

Abstract:

The author's aim is to investigate the relationship between the Hungarian law enforcement agencies and their counterparts in countering cybercrime. Legal provisions and other regulatoions has been reviewed, available statistical data was exemined, and the staff and leaders of the organizations concerned has been interviewed. The findig is that the law enforcement agencies have no regulations, action plans, task rules, methodological instructions - outside of the basic principles of the Basic Law and the Cyber Security Strategy and the Criminal Code - which would set the roles, responsibilities and eventually deadlines.

Keywords: Hungarian law enforcement agencies, cybercrime, cooperation

[1] A mű, a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű, kiemelt projekt keretében működtetett, Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

[2] Dr. Simon Béla r. őrnagy. a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési és Gazdaságvédelmi Tanszék tanársegédje ORCID:0000-0002-1555-3690

Bevezetés

Jelen cikk célja annak megvizsgálása, hogy az állami szerveknek és kiemelten a rendészeti szerveknek pontos, körülhatárolt feladatai vannak-e a kiberbűnözés elleni fellépésre és ezen feladatok közül megfelelő szabályozást kaptak-e az együttműködési kérdések, vagy azok csak ad-hoc jelleggel mindig az aktuális problémák felvetődése esetén kapnak rendezést.

A szabályozásnak mind a pozitív, mind a negatív hatásköri összeütközéseket ki kell zárnia, hiszen amíg egy adott rendészeti szerven belüli egységek közti vitát a felettes szerv eldönti, addig a rendészeti szervek és más szervek közti összeütközésre a jogszabályok hivatottak a döntést megadni. A szabályozási problémák lehetnek:

- nem pontosan körülhatárolt hatáskörök – azaz a feladatok nem egyértelműen tartoznak egy hatáskörbe
  - o több szerv is hatáskörébe tartozónak véli
  - o egy szerv sem véli hatáskörébe tartozónak
- az egyes feladatok egyáltalán nem kerültek hatáskörbe utalásra, mert pl: korábban nem látható új problémakörök keletkeztek
- kapcsolódó problémaként jelentkezhet, hogy az egyik szerv túlterheltsége okán tesz kísérletet hatásköre hiányának megállapítására,3 azaz a szabályozás nem éri el célját és a címzettek ellenállása miatt nem érvényesül.

A szabályzók megalkotásával a NATO Kooperatív Kibervédelmi Kiválósági Központjának (Cooperative Cyber Defense Center of Excellence (CCDCOE)) javaslatai iránymutatást adnak:

1. ábra: CCDCoE négy szintű javaslata[4]

[3] Túlterhelt rendőrkapitányságok esetében már teljesen elfogadott gondolatmenet az, hogy ügyirat, vagy feljelentés érkezésekor a hatáskör és illetékesség vizsgálatának egyetlen célja, hogy miként lehet megszabadulni az ügyirattól, holott ilyen kodifikált feladatokat nem találunk.

Azt javasolják, hogy a négyszintű konstrukció olyan eszközként alkalmazható, amely a szervezeti döntéshozatali struktúrák sokkal szélesebb körű kontextusát vizsgálja a kormányzat számára. Mint ilyen, a négy szint egy általánosabb elemző- eszközzé alakulhat. Beleértve olyan politikai szintet, ahol hosszú távú politikai célkitűzéseket definiálnak (például egy „fehér könyv",[5] amely kiemelt nemzeti prioritásként jelenti a számítógépes biztonságot). Egy olyan stratégiai szint, ahol a szervezeteket az előre meghatározott célok elérésére hozták létre, például egy irányelv, amely létrehoz egy konkrét testületet a számítógépes biztonság elérése érdekében. Egy olyan operatív szint, ahol az egyes szervezetek különböző feladatait összehangolják (pl. egy szervezet szegmentálása különböző szervezeti egységekbe), és taktikai szinten, ahol az adott feladatokat végre hajtják (például a konkrét taktikákat, technikákat és eljárásokat, amelyeket alkalmaznak minden feladathoz).

Megítélésem szerint a rendészeti szervek számára kiemelten fontos a feladatszabás és jogszabályok általi felhatalmazottság. Megkísérlem megvizsgálni, hogy a teljes szervezetektől a végrehajtó állomány szolgálatot teljesítő tagjáig mindenhol megtalálhatóak-e a feladatok elosztására vonatkozó rendelkezések és a feladatok végrehajtását meghatározó szakmai előírások, szabályok.

Természetesen nem lehet minden élethelyzetre vonatkozó előírásokat kimunkálni, és a túlszabályozottság semmiképpen nem célravezető különösen egy ilyen dinamikusan változó viszonyrendszerben, mint a kiber-bűncselekmények. Az azonban fontos, hogy megvizsgáljuk, hogy egy esetlegesen bekövetkező létfontosságú informatikai rendszerelemet ért támadás esetén milyen döntési és irányítási folyamatoknak kell megindulniuk, és úgyszintén fontos annak vizsgálata, hogy például egy bűncselekmény elkövetésével összefüggésben felkutatott informatikai eszközön keresztül milyen szabályok szerint rögzíthet bizonyítékokat a nyomozóhatóság eljáró tagja egy felhő alapú tárhelyről.

Cél beazonosítani, hogy

- a kiberbűnözésnek milyen területei vannak
- az adott területen mely szerveknek van tennivalójuk
- milyen jogforrások, előírások vannak az egyes szervek feladatainak meghatározására
- melyek azok a szabályozók, amelyek hiányosak? – kell-e egy ilyen gyorsan változó rendszerben jogszabályi szintre emelni a szabályzókat, vagy

[4] *Alexander KLIMBURG (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012 p. 111.*
https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
(Letöltve: 2017.09.01.)

[5] *Leíró dokumentum*

egyes esetekben a folyamatok akár önszabályozó módon a leghatékonyabbak?

Jogi felhatalmazottság, kötelezés[6]

Az Alaptörvény szintjén a feladatszabás megjelenik, amikor a közbiztonság védelme elsősorban az állam szerveinek az Alkotmányban meghatározott (40/A. §) vagy az Alkotmányból levezethető kötelezettsége (35. §, 50. §, 51. §). A közbiztonság a jogállam intézményrendszerének és a demokratikus társadalom működésének nélkülözhetetlen feltétele, és így általánosságban alkotmányos érték és alkotmányos cél.[7]

A közbiztonság és a belső rend védelme az Alkotmány 40/A. § (2) bekezdése szerint a rendőrség alapvető feladata. A közbiztonságnak, közrendnek alkotóeleme a köznyugalom, amely veszélyeztetésének a büntetőjog eszközeivel történő megelőzése, illetve megtorlása nyomós közérdek.[8]

A közrend és közbiztonság védelmének feladatát tehát az Alaptörvény a Rendőrséghez delegálja,[9] míg a törvényes rend védelme megjelenik a nemzetbiztonsági szolgálatok alapvető feladatai közt.[10] A bűnözés elleni fellépés alaptörvényi szinten e két címzettet érinti.

Ha azonban elfogadjuk, hogy a rendészeti szervek alkotmányos feladata a közrend és közbiztonság fenntartása Magyarország területén, akkor azonnal felvetődik a kérdés, hogy ez a feladat érvényes-e a kibertérre vonatkozóan is?

Ha a jogi felhatalmazást, feladatszabást keressük a rendészeti szervek irányában, akkor az Alaptörvény után a következő lépésként a Nemzeti Kiberbiztonsági Stratégiát[11] találjuk.

A stratégia nem rendészeti szerveket nevesít, hanem bűnüldöző szerveket.[12] Bár a stratégia nem kívánt szűkítő meghatározást adni az egyes szervezeteknek, de sajnos nem született ez alapján a bűnüldözést koordináló, feladatszabó ágazati stratégia, mely konkrét feladatokat és határidőket írna elő.

Cél volt az uniós és NATO stratégiákkal való összhang, de ha csak az EU kiberbiztonsági stratégiáját vesszük alapul, akkor is jól látszik, hogy indokolt volna a konkrétabb feladatszabás:

---

[6] Jelen tanulmányban, a nemzetközi és bilaterális szabályzók ismertetésére, terjedelmi korlátokra tekintettel nem kerülhetett sor.

[7] 13/2001. (V. 14.) AB határozat.

[8] 44/2004. (XI. 23.) AB határozat, III.1.1.

[9] Magyarország Alaptörvénye 46. cikk (1)bekezdés

[10] Magyarország Alaptörvénye 46. cikk (3)bekezdés

[11] 1139/2013. (III.21.) Kormányhatározat

[12] 1139/2013. (III. 21.) Korm. határozat III/10.pont, c./ alpont

„A stratégiában ismertetett uniós jövőképet öt stratégiai prioritásban foglaltuk össze, amelyek a fent kiemelt kihívásokra adnak választ:

- kibertámadásokkal szembeni ellenálló képesség elérése;
- a számítástechnikai bűnözés drasztikus csökkentése;
- kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása. (…)”[13]

„*Minden tagállamnak hatékony számítástechnikai bűnözés elleni egységekre van szüksége*.” Ezen túlmenően a finanszírozási, együttműködési és a hatékony működést célzó konkrét feladatokat is meghatároz a stratégia címzettek megjelölésével.

A közel azonos időben elkészült stratégiák közt jelentős különbségek vannak a címzettek, a feladatok és a célok meghatározásában.[14]

A már korábban hivatkozott NATO kiválósági központ tanulmánya az egyes állami feladatok szerint szemlélteti a kibervédelem életciklus modelljét,[15] melyből jól látható, hogy a kiberbűnözés elleni fellépés megköveteli:

- a proaktivitást (bűnelkövetőkre vonatkozó kiterjedt adatgyűjtést, operatív műveleteket),
- a bűnmegelőzést,
- felkészülést az egyes illegális cselekményekre (anyagi és emberi erőforrások dedikálása),
- a válaszadás és visszaállítás ebben az értelemben tulajdonképpen legfőképp a büntetőeljárás szakasza, valamint az
- utógondozás, követés (ami egyrész jelölheti az elkövetői csoportok későbbi ellenőrzését, de akár szignalizációt és visszacsatolást az életciklus elejére.

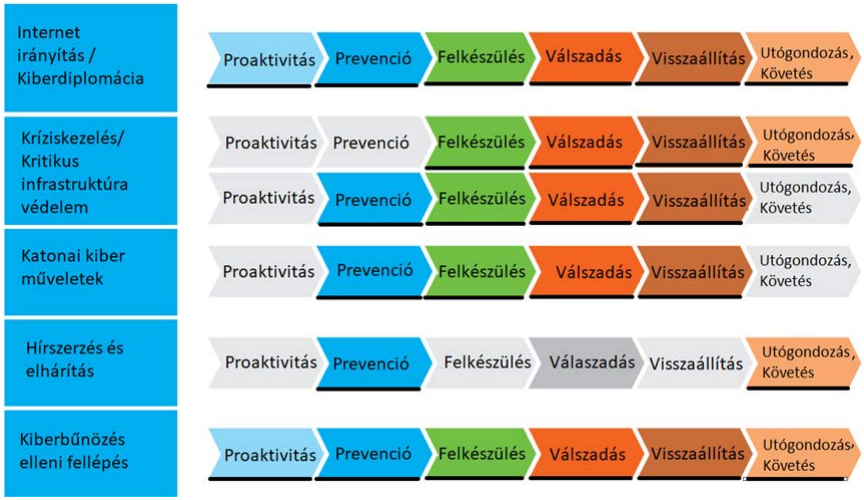
---

[13] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001 (Letöltve: 2017.09.02.)

[14] Az összevetés indokolt lehet az Európai Unió kibervédelemmel foglalkozó szervezete, az ENISA 2012-es nemzeti kiberbiztonsági stratégiák létrehozását támogató National Cyber Security Strategies – Practical Guide on Development and Execution című kiadványában foglaltakkal is.

[15] Alexander KLIMBURG (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012 – p. 118. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Letöltve: 2017.09.01.)

Mint látható az állami szervezetek és feladatok közül az egyik legösszetettebb folyamat hárul a közrend és közbiztonság fenntartására hivatott szervezetekre.



2. ábra: kibervédelem életciklus modellje

Ezt az összehangolt munkát csak megfelelő orientációval lehet megvalósítani. Szükséges egy kiberbűnözés elleni stratégia megalkotása, de ha ettől el is tekintünk, és a CCDCoE négy színtű modelljét alapul véve kijelentjük, hogy:

- a kiberbiztonsági stratégia megalkotásával a politikai szint valósult meg
- stratégiai szint céljai a testületek és szervezetek megalkotásával szintén teljesedésre jutottak.
- Azonban az operatív szint, ahol az egyes szervezetek különböző feladatainak összehangolása megtörténik és
- és taktikai szinten, ahol az adott feladatokat végre hajtása folyik – tehát az alsó két szinten a normák, szakmai szabályok megalkotása továbbra is szükséges.

Az operatív szint működtetése a kiberbiztonsági stratégiával összhangban a nemzeti kiberkoordinátor és a különféle munkacsoportok, munkabizottságok szintjén megvalósul, de a bűnüldözés folyamatainak összehangolása a problémák felmerüléséhez és ad-hoc megoldásokhoz kötődik.

A stratégia felülvizsgálata a NIS irányelv,[16] valamint a GDPR[17] rendelet elfogadásával halaszthatatlanná vált és a kiberbűnözés elleni feladatok, célok és felelősök meghatározására ez a megfelelő alkalom.

A párhuzam nemzetközi szint és a belföldi szint között jól látható. A NIS irányelvet megelőzően a tagállamok közti együttműködés sokszor bilaterális egyezmények segítségével, vagy szívességi alapon, ad-hoc jelleggel működött. Jelenleg a kiberbűnözéssel összefüggésben a belföldi helyzet a rendvédelmi szervek egymás közti és piaci szereplőkkel való kapcsolattartására is ez jellemző: az érintettek a legtöbb esetben nem előre definiált protokollok szerint működnek együtt, hanem mindig célhoz kötötten – szintén ad-hoc jelleggel. Megítélésem szerint egy megalkotandó a kiberbűnözés elleni stratégiának, vagy akciótervnek ezt is rendeznie kellene.

A fenyegetettségek és a célkitűzések megalapozottságának érdekében az új stratégia kidolgozása előtt országos kiberbiztonsági kockázatelemzés és értékelés elvégzése szükséges. Az új stratégiához nyilvános végrehajtási terv kidolgozása, valamint a végrehajtás ellenőrzését szolgáló mérőszámok és indikátorok meghatározása kell, hogy kapcsolódjon – csak ezáltal válik eredményesen végrehajthatóvá.[18] Hiszen csak azt lehet hatékonyan menedzselni, amit számokban ki tudunk fejezni. A mérőszámokhoz felelősöket és erőforrásokat is szükséges kapcsolni.

Az alkotmányos felhatalmazottságtól indulva a stratégiai feladatszabást követően vizsgálatunkat folytatni volna szükséges, hogy a rendészeti szervek számára melyek azok a törvények, rendeletek, amelyek a kiberbűnözés elleni fellépést meghatározzák.

Jelenleg ilyen jogforrás nincs. A következő lépés a Büntető Törvénykönyvünk, mely meghatározza, hogy melyek azok a cselekmények, amelyek a jogalkotó véleménye szerint veszélyesek a társadalomra és büntetendők.

Az élet számos területén valóban nem szükséges a feladatok jogszabályba foglalása az alkotmány és a Büntető Törvénykönyv közt. Példaként az emberi élet, a közrend és közbiztonság védelme alkotmányos gyökerekkel bír, az pedig

---

[16] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről - http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC (Letöltve: 2017.09.01.)

[17] Európai általános adatvédelmi rendelet – bővebben: http://www.adatvedelmirendelet.hu/a-rendelet-szovege/ (Letöltve: 2017.09.01.)

[18] BELÁZ Annamária, BERZSENYI Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései, STRATÉGIAI VÉDELMI KUTATÓKÖZPONT ELEMZÉSEK, Budapest 2017/3 - http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-3-kiberbiztonsagi-strategia-2-0-belaz-a-berzsenyi-d.original.pdf (Letöltve: 2017.04.01.)

nyilvánvaló, hogy az emberölést a BTK pönalizálja. Ebben az esetben azonban a védendő társadalmi érdek nyilvánvaló, és a feladat címzettje is egyértelmű – az ilyen büntetőeljárásokat a rendőrségnek[19] kell lefolytatni. A kiberbűncselekmények esetében azonban ez nem így van. Nem egyértelműen körülhatárolt a védendő társadalmi érdek és nem csak a bűnüldöző szervek a címzettje ezen feladatoknak, hanem számos állami szerv, és fontos szerep kell jusson a piaci szereplőknek is.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény az alkotmányos célok és a hatáskörök lehatárolása tekintetében nagyon fontos alapköve a kibervédelemnek, de a kiberbűnözés elleni fellépést nem segíti. A bűnelkövetői oldalról érkező inputok – a bejelentett incidensek – megjelennek az információs folyamatokban, de nincs rögzített kivezetésük a bűnüldöző szervek

A kiber bűncselekmények kategóriái

Ha a vizsgálat célja a meglévő működési folyamatok feltárása, akkor a csoportosítást is a rendvédelmi szervek számára meghatározott feladatcsoportok irányából célszerű megközelíteni. E szervek közti feladatmegosztás alapelve, hogy úgy kerüljenek létrehozásra szervek és szervezetek, hogy az adott feladatcsoporthoz szükséges anyagi, technikai valamint emberi erőforrás rendelkezésre álljon és optimális módon ki legyen használva. A létrehozott szervezeti egységek számára akkora szeletet indokolt dedikálni a teljes szervezet hatásköréből, amekkora háttértudás felhalmozható egy-egy szervezeti egységen belül.

A rendészeti szervek organogramjának kialakításában két egymás ellen ható tényező munkálkodik: az egyik, hogy a végrehajtó állomány a lehető legkisebb ügycsoportra specializálódjon, a másik tényező a földrajzi távolságok csökkentésének igénye.

A szükséges háttér ismeretek differenciálódásának fokozódásával azonban felülíródik a földrajzi közelség igénye. Ez hívta életre a területi nyomozóhatóságokat, illetve a Nemzeti Nyomozó Irodát.[20]

A kiberbűncselekmények esetében hasonló differenciálódás figyelhető meg: az elvégzendő feladatok szofisztikált jellege és a szükséges gyakorlati és elméleti ismeretek magas szintje miatt létrehoztak központi szervezeti egységeket. Jelenleg két ilyen szervezeti egység működik: a Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya, valamint Budapesti Rendőr-főkapitányság Korrupciós és Gazda-

[19] *Természetesen a büntetőeljárás rendelkezései szerint itt is érvényesek az ügyészségre vonatkozó hatásköri szabályok a speciális passzív alanyokra és sértettekre tekintettel. (rendőrök, ügyészek, bírók, stb) Be. 29.§.*

[20] *Bár szintén területi jogállású, de országos hatáskörű szerv.*

sági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztályán működő Csúcstechnológiai Bűnözés Elleni Alosztály.

Európai uniós kitekintésben a kiberbűnözés elleni fellépés letéteményese az Európai Bizottság által 2012. évben létrehozott Európai Kiberbűnözési Központ (European Cybercrime Centre – EC3), melyet a „Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása”[21] című közlemény hívott életre.

Az Europol bűnügyi elemzői korábban úgynevezett elemzési munkafájlok keretrendszerében dolgoztak,[22] amelyet később fókusz pontoknak, majd elemzési projekteknek neveztek el. Jelenleg 28 ilyen projekt működik,[23] melyek karbantartását, üzemeltetését külön-külön dedikált szakemberek végzik.

Az EC3 ezekből a projektekből 3-at gondoz. Ezek:

- AP Cyborg - támogatja az EU-ban a kritikus számítógépes és hálózati infrastruktúrákat érintő számítógépes bűnözés elleni vizsgálatokat. Különös figyelmet fordít a szervezett bűnözői csoportok által elkövetett jelentős súlyú bűncselekményekre. Ez a projekt magában foglalja a high-tech bűncselekmények széles körét, például a rosszindulatú programokat (kód létrehozása és terjesztése), az zsarolóvírusok, a hackelés, az adathalászat, a behatolás, a személyazonosság-lopás és az internethez kapcsolódó csalások.
- AP Terminal - a nemzetközi elektronikus és online fizetési csalások felderítésén dolgoznak.
- AP Twins elemzési projekt támogatja a gyermekek szexuális kizsákmányolásával és visszaélésekkel járó bűnözés minden formájának megelőzését és leküzdését.[24]

Fentieken túlmenően a kibertérhez szorosan kapcsolódó további elemző projektek is működnek, mint például az

- AP Copy, amely támogatja a szellemi tulajdonjogokkal (Intellectual property rights - IPR) kapcsolatos bűncselekmények megelőzését és az azok elleni küzdelmet.

---

[21] *elérhető: http://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52012DC0140 (Letöltve: 2017.09.02.)*

[22] *Analysis Work File- AWF*

[23] *Bővebben: https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects (Letöltve: 2017.09.03.)*

[24] *Az elmúlt időszakban nagy számban valósítottak meg olyan módon gyermekbántalmazásokat, hogy annak végrehajtását élő videoközvetítést megtekintő személy utasításait követve hajtják végre. A végrehajtás helyszíne jellemzően a Föld nagyon elmaradott régióira jellemző, míg a megrendelő tipikusan fejlett országok lakója.*

- AP Check-the-Web[25] az "Ellenőrzés a weben" 2007-ben indult és célja az együttműködés erősítése és a nyílt internetforrások figyelemmel kísérése és értékelése az iszlamista terrorizmus ellen. A témakör folyamatos jelentőségét jelzi, hogy a 2017. szeptemberi Europol által 550 rendőri vezető részvételével zajlott konferencia egyik fő témája volt a terrorista és az erőszakos szélsőséges propaganda online terjesztése és a bűnüldöző szervek válasza.[26]
- AP Apate különös hangsúlyt fektet az ügyvezetői csalások[27] elleni küzdelemre, valamint támogatást nyújt többek között tömeges csalárd emailekkel, nagyszámú marketing üzenetekkel, társkereséssel28 elkövetett csalások, piramisjáték, befektetési csalás és hamiszámla csalással elkövetett ügyekben is.

Természetesen majdnem minden elemzői projekt kapcsolatban áll a kibertérrel,[29] de a felsorolt AP-ken kívül nem szükséges folyamatosan speciális informatikai ismeret.

A fenti felsorolásnak nem célja a nemzetközi bűnügyi együttműködés bemutatása, csupán azt hivatott szemléltetni, hogy európai szinten milyen logika szerint osztották fel azokat a jogellenes cselekményeket, melyek a kibertérhez szorosan köthetők. A felosztás alapját az adja, hogy milyen speciális ismeretekre van szüksége az abban tevékeny munkatársnak, illetve az is, hogy milyen szervezetekkel kell kapcsolatot tartania. Ezáltal a munkavégzés és a munkatársak képzettsége is speciális és így professzionálisabbá válhat.

---

[25] Bővebben: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (Letöltve: 2017.09.07.)

[26] Bővebben:https://www.europol.europa.eu/newsroom/news/2017-european-police-chiefs-convention-largest-ever-gathering-of-global-police-chiefs-europol (Letöltve: 2017.09.07.)

[27] CEO fraud/ Manager fraud, melyet Magyarországon átutalásos csalásként is neveznek. Alapja a social engineering és a legtöbb esetben előzetes informatikai eszközökön illegálisan beszerzett információk. Bővebben: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees (Letöltve: 2017.09.07.)

[28] romance scams – bővebben: https://www.fbi.gov/news/stories/romance-scams (Letöltve: 2017.09.07.)

[29] Pl: a vagyonvisszaszerzéshez (AP Asset Recovery), az ÁFA csalásokhoz (AP MTIC - Missing Trader Intra Community Fraud) pénzmosáshoz (AP Sustrans) stb elengedhetetlen az informatikai eszközökből kinyert adat az eredményes nyomozás lefolytatásához,

A magyarországi szervezeti berendezkedést (pl: NAV-rendőrség) illetve a feladatok optimális szétosztását illetően az alábbi feladatközpontú felosztás indokolt megítélésem szerint:

- klasszikus kiber bűncselekmények (rendszerek elleni támadások, malware, ransomware, DDOS, botnet, stb)
- bankkártyás visszaélések
- gyermekek online szexuális kizsákmányolása
- szellemi tulajdont sértő online bűncselekmények
- V. online felületen elkövetett csalások

Az egyes területek azonban nem határolhatók el élesen egymástól. Számos olyan bűncselekmény van, ami átnyúlik a határokon. Példaképpen:

- a darknetet használó bűnelkövetők elleni fellépés speciális ismereteket tesz szükségessé, de szorosan kapcsolódik a gyermekek online szexuális kizsákmányolásához, az online kalózkodáshoz, bankkártya adatokkal, kábítószerrel való kereskedelemhez,
- A darknet piacokon az adásvételek többsége kábítószerhez kapcsolódik. Egy friss tanulmány 16 nagyobb darknet piacon vizsgálta az értékesítéseket 2011 és 2015 között, és ez alapján úgy becsülte, hogy a globális darknet piacok bevételének több mint 90%-át a kábítószerek árusítása teszi ki. A jelentések szerint a darkneten folyó összes kábítószer-értékesítés közel fele (46%) európai székhelyű eladóktól származott, és ennek becsült összege a vizsgálat ideje alatt 80 millió EUR-nak felelt meg. A legfontosabb európai forrásország az értékesített mennyiség sorrendjében Németország, Hollandia és az Egyesült Királyság volt, az értékesítésből származó bevétel legnagyobb részét pedig a stimulánsok, különösen az MDMA és a kokain tették ki.[30]
- a különféle kriptovaluták (pl: Bitcoin, Litecoin, Ethereum, Ripple, stb) szintén számos bűncselekményi kategóriához kötődnek.
- a terrorizmus számos formájában szorosan kapcsolódik a kibertérhez. Lehet a támadások célpontja is a létfontosságú informatikai rendszerelem, de a műveletei megszervezéséhez, finanszírozáshoz, pénzmosáshoz is infokommunikációs eszközöket használnak.

[30] *Európai kábítószer-jelentés-Tendenciák és fejlemények 2017* http://www.emcdda.europa.eu/system/files/publications/4541/TDAT17001HUN.pdf_en *(Letöltve: 2017.09.02.)*

Vizsgáljuk meg az egyes kategóriákat:

I. Klasszikus kiber bűncselekmények:

Ide tartozó büntető törvénykönyvi tényállások:

Személyes adattal visszaélés

Btk. 219. §
Statisztikai adatok:
2013 – 2635
2014 – 1059
2015 – 975
2016 – 487
2017 (I.-IX. hó) – 224

Ezen tényállás nem szükségszerűen kapcsolódik a kibertérhez, de a személyes adatok tárolása, feldolgozása, továbbítása jellemzően infokommunikációs eszközök igénybevételét teszi szükségessé.
Jellemző egy nagyon erős csökkenő trend, amely a GDPR rendelet bevezetésével összefüggésben – a felszínre kerülő bűncselekmények megjelenésével – vélelmezhetően emelkedni fog.

A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény

Btk. 267. §
2013. óta az ENYÜBS szerint ilyen bűncselekmény elkövetésére nem került sor

Jogosulatlan titkos információgyűjtés vagy adatszerzés

Btk. 307. § (1)
A 2013. évtől kezdődő időszakban 2db ilyen bűncselekmény elkövetését mutatja a statisztika azonban az adatsorokból nem vizsgálható ez esetben sem, hogy a kibertérhez köthetők-e a cselekmények.

Terrorcselekmény

Btk. 314. §
A 2013. évtől 17db e tényállás szerinti bűncselekmény elkövetésére került sor, melyből szintén nem célszerű következtetéseket levonni, mert ebben sincs elkülönítve a kibertérrel kapcsolatban megvalósított elkövetés.

Közérdekű üzem működésének megzavarása

Btk. 323. §
Statisztikai adatok
2013 – 73
2014 – 66
2015 – 34
2016 – 40
2017 (I-IX. hó) - 24
Szintén nem gyűjthetők ki a kibertérhez köthető cselekmények

Információs rendszer felhasználásával elkövetett csalás

Btk. 375. §
2013 – 250
2014 – 1398
2015 – 2176
2016 – 3409
2017 (I-IX. hó) - 3149
Amint látható a cselekmény elszaporodottsága fokozatos emelkedő tendenciát mutat.

Tiltott adatszerzés

Btk. 422. §
Statisztikai adatok:
2013 – 20
2014 – 31
2015 – 23
2016 – 20
2017 (I-IX. hó) - 11
Az ügyszám éves szinten nem jelentős és egy sávban marad.

Információs rendszer vagy adat megsértése

Btk. 423. §
Statisztikai adatok:
2013 – 823
2014 – 565
2015 – 520
2016 – 702
2017 (I-IX. hó) - 356

A bűncselekmények száma e tényállás esetében nem elhanyagolható és a 2016. évtől eltekintve csökkenő trendet mutat.

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

Btk. 424. §
Statisztikai adatok:
2013 – 580
2014 – 31
2015 – 15
2016 – 44
2017 (I-IX. hó) - 4
E tényállás elkövetését igazolja az interneten megosztott számos tartalom, de a statisztikai adatok tanúsága szerint ezek nem jutnak a nyomozóhatóságok és az ügyészség tudomására.

Hatásköri – együttműködési vonatkozások:

Rendőrség
Magyarországon a fent felsorolt büntető törvénykönyvi tényállások a Be. 36.§ (1) bekezdése alapján a rendőrség hatáskörébe tartoznak.[31]

A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet megyei (fővárosi) rendőr-főkapitányságok hatáskörébe tartozó bűncselekmények közé sorolja:
- Jogosulatlan titkos információgyűjtés vagy adatszerzés 307. §
- Közérdekű üzem működésének megzavarása 323. §[32]
- Különösen nagy, különösen jelentős kárt okozó, jelentős kárt bűnszövetségben okozó, információs rendszer felhasználásával elkövetett csalás bűntette - Btk. 375. § (3) bekezdés a), b) pont

A Készenléti Rendőrség hatáskörébe tartozó bűncselekmények közt jelenik meg:
- Terrorcselekmény 314. §
- Fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából elkövetett tiltott adatszerzés bűntette - Btk. 422. § (2) bekezdés

[31] Ahogy a későbbiekben tárgyalt tényállásokra is érvényes, úgy e tényállásoknál is, hogy az ügyészségnek is hatásköre van ezekre a nyomozásokra a Be. 28.§ (3) bekezdése alapján lehetőségként, vagy a 29.§ rendelkezései alapján kötelezően. Továbbá nyomozást folytathatnak nemzetközi közös nyomozócsoportok is.
[32] Kivéve, az Repülőtéri Rendőr Igazgatóság hatáskörébe tartozó esetet.

- Közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése bűntette - Btk. 423. § (3) bekezdés
- Közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége, kivéve az RRI hatáskörébe tartozó eseteket- Btk. 424. §

A fel nem sorolt ügyekben a hatásköri szabályok értelmében helyi – azaz városi és kerületi – nyomozóhatóságok kötelesek eljárni.

A jelenlegi gyakorlat azonban azt mutatja, hogy a jelentős nemzetközi vonatkozásokkal érintett, vagy nagy közérdeklődésre számot tartó ügyeket a BRFK Csúcstechnológiai Bűnözés Elleni Alosztálya, illetve az NNI Kiberbűnözés Elleni Főosztálya hatáskörébe utalja a felettes rendőri szerv, vagy a szervek előzetes egyeztetés alapján átteszik, vagy ha a központi szerveknél került elrendelésre a nyomozás, akkor azt lefolytatják, és nem határoznak áttételről.

Együttműködés a rendőrség és más rendészeti szervekkel:

Katonai Nemzetbiztonsági Szolgálattal való együttműködés ügyekhez kapcsolódóan eseti jelleggel titkos információgyűjtéssel összefüggésben jelentkezhet, melyre vonatkozó információ jelen tanulmányban nem szerepeltethető.

A Nemzetbiztonsági Szakszolgálat tevékenysége négy felületen jelenik meg.

- Egyrészt az Ibtv., illetve annak az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelete alapján kormányzati eseménykezelő központként működik. Az NBSZ keretein belül működő Kormányzati Eseménykezelő Központ (GovCERT-Hungary) nyílt büntetőeljárásokban nyújthat segítséget. Ezt sok esetben informatikai elemzésekkel, LOG elemzéssel, informatikai szakmai tanácsokkal valósul meg. Jellemzően megkeresésre adott válaszokban jelenik meg a büntetőeljárásokban. Bár a GovCERT információval bír az állami és önkormányzati szerveket ért incidensekről, de a jelenlegi gyakorlat szerint maga nem tesz feljelentést, mivel egyrészt nem sértettje az ügynek másrészt azon a véleményen van, hogy a GovCERT Incedenskezelő Osztály nem lép fel hatóságként, mivel azt a szerepet a Nemzeti Kibervédelmi Intézeten belül alapvetően a Nemzeti Elektronikus Információbiztonsági Hatóság látja el. Ez a gyakorlat a jelenlegi[33] és a 2018. július 01-től hatályba lépő büntetőeljárási törvény rendelkezése[34]

[33] *1998. évi XIX. törvény 171.§ (2) bekezdés*

[34] *2017. évi XC. törvény 376. § (2) bekezdése*

szerint is aggályos, mivel bűncselekmény észlelése esetén a hivatalos személyeknek[35] feljelentési kötelezettségük van. A jelenlegi gyakorlat alapján a feljelentést az ügy sértettje tehetné meg, de a valóságban ez csak elenyésző számban valósul meg.[36] Ezt a problémakört érintettük a jogszabályi felhatalmazottságot vázoló alcímben is.

- Másrészt a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról szóló 36/2013. (VII. 17.) BM rendelet ezt a szervezetet jelölte ki a belügyi szervek vonatkozásában a sérülékenységvizsgálattal összefüggő feladatok ellátására.[37] Ez előbbi két funkció a kibervédelemhez kapcsolódik, míg a fennmaradó két funkció már a bűnüldözést segíti.
- A harmadik vetület a szolgáltató jellegű titkosszolgálati működésével van összefüggésben, amikor a rendőrség, mint megrendelő számára végez bírói engedélyhez kötött és bírói engedélyhez nem kötött titkos információgyűjtési feladatokat, műveleteket.
- A negyedik funkció pedig az NBSZ szervezetén belül működő Szakértői Intézet informatikai szakértői tevékenysége, amely kiválóan felszerelt laborjával és magas szintű szakértői tevékenységével kirendeléseken keresztül működik közre az digitális bizonyítékok felkutatásában, rögzítésében és értékelésében.

A Terrorelhárítási Központ és a rendőrség bűnügyi szervei közti együttműködés a kiberbűncselekményekkel összefüggésben elenyésző. A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól szóló 295/2010. (XII. 22.) Korm. rendelet nem rendelkezik informatikai, vagy kiberbűncselekményekről, de a TEK rendelkezik a terrorizmussal összefüggésben internet monitorozó egységgel.

A rendőrség és a TEK együttműködését a korlátozott terjesztésű 247/2010. Tük. számú (OT22/2010) Országos Rendőr-főkapitányság és a Terrorelhárítási Központ között kötött együttműködési megállapodás szabályozza, melyet a 29000-129/20/2016. emü. számú „Együttműködési megállapodás módosítása”[38] újra szabályoz. Utóbbiban a kibervédelem és a létfontosságú informatikai rendszerelemek védelme nem jelenik meg.

---

[35] A Büntető Törvénykönyvről szóló 2012. évi C. törvény 459. § (1) bek.11.pont

[36] SIMON Béla: Hacktivism and its status in Hungary, MAGYAR RENDÉSZET 16:(2) 2016 pp. 161–174.

[37] Dr. KRASZNAY Csaba: A rendvédelmi szervek helye a kibervédelemben, MAGYAR RENDÉSZET, XIII. Évfolyam, 2013. Különszám 2013. szeptember p. 114.

[38] ORFK Tájékoztató (OT) 2016/21. szám

Katasztrófavédelmi szervezet

Az Országos Katasztrófavédelmi Főigazgatóság a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján felelős számos kritikus információs infrastruktúra védelmének felügyeletéért. Az Ibtv. ennek a feladatnak a kibervédelmi aspektusait nem részletezi, de több helyen is megerősíti azt, hogy a létfontosságú rendszerelemeket informatikai szempontból is védeni szükséges, ezért az OKF-et és a törvényben nevesített szervezeteket együttműködésre utasítja.[39]

Az OKF emellett eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK) elnevezéssel. Feladat- és hatáskörét a GovCERT-tel egységesen a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet, valamint az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII.13.) Korm. rendelet szabályozza.

Amint a GovCERT-nél kifogásként jelentkezett, hogy a kiberbűnözés elleni fellépés folyamatába nem illeszkedik, úgy ezt az LRLIBEK esetében is kijelenthetjük. A rendészeti szervek együttműködése a klasszikus kiber-bűncselekmények vonatkozásában a piaci szereplőkkel stratégiai szinten a Kibervédelmi Munkacsoport.

Végrehajtási, operatív szinten a bűnüldözésben intézményesített együttműködés nincs.

A létező kooperációk eseti jellegűek, ügyekhez, ügycsoportokhoz kötődnek. Büntető eljárásokban a létfontosságú informatikai infrastruktúrák üzemeltetői sértettként, megkereséssel érintett adatközlőként, munkatársaik eseti szakértőként, tanúként vonhatók jellemzően az eljárásokba.

Időszakonként visszatérő jellegű együttműködés jó példája az országos választások lefolytatása, amikor állami szervek, piaci szereplők, bűnüldöző szervek és titkosszolgálatok szoros együttműködése szükséges. 2017 nyarán a Nemzeti Választási Iroda is megkezdte az informatikai felkészülést, melynek egyik kiemelt területe az informatikai biztonság fokozása. Az információbiztonsági intézkedések fókuszában a bizalmasság, sértetlenség, rendelkezésre állás biztosítása áll. Az internet irányából esetlegesen érkező támadások elleni védekezés kapcsán az

[39] *Dr. Krasznay Csaba: A rendvédelmi szervek helye a kibervédelemben, Magyar Rendészet, XIII. Évfolyam 2013. Különszám, 2013. szeptember p. 114.*

NVI vizsgálja egy választási informatikai biztonsági műveleti központ létrehozásának lehetőségét.[40] Az NVI elnöke megjegyezte, hogy Magyarországon a szavazás és a szavazás eredményének összesítése papíralapon történik, a választási honlapon mindössze a gyorsabb tájékoztatás érdekében hozzák nyilvánosságra a papíralapú jegyzőkönyvek eredményét.

Összességében tehát kijelenthető, hogy intézményesített együttműködés a klasszikus kiberbűnözés területén a rendészeti szervek, állami szervek, piaci szereplők között nincs.

A tanulmány a magyar nemzetbiztonsági szféra egyes 1990 és 2012 (2016) közötti szervezeti és működési kérdésivel foglalkozott. A magyar nemzetbiztonsági szektor szervezeti változásait történeti kontextusában, adott környezetbe ágyazva, a szervezetrendszer egészeként és a rendvédelmi szektor más szereplőivel párhuzamosan érdemes vizsgálni. Egy alkotmányos demokráciában a döntéshozó és az irányítása alá tartozó nemzetbiztonsági szolgálatok szigorú jogszabályi keretek között, de a munkájukhoz szükséges szabad mozgástér biztosítása mellett szuverén szervezetként teljesítik az ország biztonság- és védelempolitikából rájuk háruló feladatokat.

Minden változás során figyelembe kell venni, hogy az intézményi változtatásokhoz több hónap, a széleskörű és stabil jogszabályi háttér megteremtéséhez több év, egy teljesen új szolgálati kultúra meghonosodásához még ennél is több idő szükséges. Két-három évtized tapasztalata már önmagában is vizsgálatra érdemes, korszakokon átnyúló viszonyítási alap. Két letűnt évtized fordulójának transzformációs időszaka, elmélyült gazdasági-politikai változás átformálta államról és biztonságról alkotott képzetünket, érezhető paradigmaváltást eredményezve a nemzetbiztonsági szférában. A konszolidáció nevében, és a folyamatos változás ellenére egyes kérdések napirenden maradtak, mások szakmai-történeti kontextusba ágyazva ismét előtérbe kerültek, így biztosítva lehetőséget további kutatásokhoz.

További kiber-bűncselekmény kategóriák:

II. Bankkártyás visszaélések, ahova az
- Információs rendszer felhasználásával elkövetett csalás
- Készpénz-helyettesítő fizetési eszköz hamisítása
- Készpénz-helyettesítő fizetési eszközzel visszaélés
- Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése

[40] *http://www.valasztas.hu/hu/ovi/content/kozlemeny20170615ogyvalfelkeszules.pdf (Letöltve 2017. július 15.)*

III. Gyermekek online szexuális kizsákmányolása ahova a
- Gyermekpornográfia

IV. Szellemi tulajdont sértő online bűncselekmények, ahova a
- Bitorlás
- Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése
- Védelmet biztosító műszaki intézkedés kijátszása

V. Online felületen elkövetett csalások tartoznak.

Ezen csoportok vonatkozásában is vizsgálta a szerző a tényállások bűnügyi fertőzöttségének szintjét, jelenleg feladattal érintett rendészeti szervek hatáskörét, az egyes szervek közti együttműködés szabályozását, és megvalósulását, de azok terjedelmi okoknál fogva nem kerülhettek be jelen cikkbe.

Összefoglalás

Alapvetésként elfogadhatjuk, hogy a nyomozóhatóságok szervezeti tagozódásának kialakítását, azaz a területi hatáskörök meghatározását az alábbi tényezők befolyásolják:
- a földrajzi távolság csökkentése ez elvégzendő nyomozati cselekményekhez (szűkítő hatás)
- a tevékenység végzéséhez szükséges speciális ismeretek megléte a végrehajtó állomány részéről (tágító hatás, mivel korlátozott számban áll rendelkezésre)
- az adott bűncselekmény típus általi fertőzöttség, veszélyeztetettség (lehet szűkítő és tágító hatású is)

Nem valósítható meg, hogy az állampolgárokhoz legközelebb eső nyomozó szervnél rendelkezésre álljon minden speciális ismeret és eszköz, de az sem helyes, ha ezek a készségek, csak országos szinten egy helyen állnak rendelkezésre.

Ennek megfelelően kell prognosztizálni, hogy területi, illetve helyi szinten milyen ügyteher várható, ahhoz mekkora személyi állomány szükséges és annak a személyi állománynak milyen szintű ismeretekkel kell rendelkeznie, azaz mennyire kell specialistának lennie. Milyen szintű specializáció szükséges a helyi és a területi munkatársak számára.

A távoli prognózisok kialakítása azért kiemelten fontos, mert ha felsőoktatáson keresztül kívánjuk a személyi állomány pótlását megvalósítani, akkor a képzés akkreditációját (1-2 év), a felvételi eljárás lefolytatását (1év), majd a képzés (3-4év) időtartamát is figyelembe kell venni.

Számos olyan állam működik, ahol:
- a digitalizáció magasabb szinten áll,
- az állampolgárok és piaci szereplők számára nagyobb értéket képvisel az online identitásuk
- egy-egy informatikai incidens jelentősebb reputációs veszteséget okoz
- a mindennapi élet szorosabban kapcsolódik az internethez.

Ezekben az államokban már napjainkban is jelentőseb erőforrás allokáció valósul meg a rendészeti szervek kiberbűnözés elleni egységei irányába, de ezt egy másik tanulmányában részletezi a szerző.

A fent leírtakból látható, hogy a rendészeti szervek számára a kiberbűncselekmények elleni fellépés vonatkozásában nincsen körülhatárolt feladatrendszer. Az alkotmány és a Nemzeti Kiberbiztonsági Stratégia általános feljogosításától a szabályozás következő lépcsője jelenleg a Büntető Törvénykönyv tényállásainak rögzítése. Ezen jogforrások közt sem ágazati stratégiát, sem akciótervet, sem az egyes szervek közti együttműködést szabályozó jogforrás nem áll rendelkezésre.

A jelenlegi viszonyrendszerben az egyes szervek, szervezetek közti együttműködés csak alapvető jogelveken nyugszik és azon, hogy a kibervédelemben és a kiberbűnözés elleni fellépésben részes állami szereplők majdnem mindegyike a Belügyminisztérium alá tartozik, így lehetőség van egyedi utasításokkal működtetni a rendszert.

A rendészeti szervek vezetői számára a személyi állomány kiképzése, a várható feladatokra való felkészülés érdekében szükséges ismerni, hogy meddig terjed feladatkörük és annak a középtávú tervek szerint milyen változása várható.

Szintén hiányzik a végrehajtó állomány számára egy egységes módszertani utasítás, mely a kiberbűncselekményekkel kapcsolatos intézkedéseik során iránymutatást ad és az esetleges diszfunkciók bekövetkezésekor az elszámoltatás alapját adja.

A kiberbűnözés elleni fellépés hatékonnyá tétele érdekében szükséges a legjobb nemzetközi gyakorlatok összegyűjtése és azok adoptálása. Ezt szolgálná, hogy az egyes kiküldetések, tanulmányutak, nemzetközi konferenciák során beszerzett információk, úti jelentések katalogizált formában, megismerhetők, kutathatók legyenek minden feljogosított érdeklő számára. Szintén javítaná a szervek közti együttműködést, ha nem csak kibervédelmi gyakorlatok kerülnének megrendezésre, hanem ezek a kiberbűncselekmények irányában a bűnüldöző szervek számára is feladatokat szolgáltatnának. Szükséges az ágazati stratégiák, akciótervek elkészítését megelőzően adatokat, mérőszámokat gyűjteni a szabályozandó terület vonatkozásában a CERT-ek, nyomozóhatóságok és bíróságok adatbázisaiból is.

Jelenleg a GovCERT és az LRLIBEK is számos esetben értesül olyan informatikai incidensekről, melyek bűncselekmény elkövetését valószínűsítik. Mivel megítélésük szerint nem látják indokoltnak sértetti jogállás hiányában a feljelentés

megtételét, ezért a nyomozóhatóságok nem szereznek tudomást a bűncselekményekről. Amint a GovCERT esetében részletezésre került: ez az álláspont a büntető eljárási törvény rendelkezéseivel nehezen összeegyeztethető.

Nem járna pozitív eredménnyel, ha minden incidenshez büntető feljelentés kapcsolódna, de jelenleg nem érvényesül a büntetőjog e területen és így generálprevenciós funkcióját sem töltheti be.

Szükséges volna az incidensekre vonatkozó információk becsatornázása a nyomozóhatóságok számára, hogy az azokból létrehozott adatbázisok segíthessék későbbi bűntetőeljárásokat.

Felhasznált irodalom:

- 1139/2013. (III.21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- 13/2001. (V. 14.) AB határozat
- 1998. évi XIX. törvény a büntetőeljárásról
- 2017. évi XC. törvény a büntetőeljárásról (új)
- 44/2004. (XI. 23.) AB határozat, III.1.1.
- A Bizottság közleménye a Tanácsnak és az Európai Parlamentnek - Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása http://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52012DC0140 (Letöltve: 2017.09.02.)
- Alexander KLIMBURG (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012, 111-118. p. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (Letöltve: 2017.09.01.)
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről - http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.HUN&toc=OJ:L:2016:194:TOC (Letöltve: 2017.09.01.)
- Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001 (Letöltve: 2017.09.02.)
- BELÁZ Annamária, BERZSENYI Dániel: Kiberbiztonsági Stratégia 2.0 A kiberbiztonság stratégiai irányításának kérdései, Stratégiai Védelmi Kutatóközpont Elemzések, Budapest 2017/3 - http://netk.uni-nke.hu/ uploads/media_items/svkk-elemzesek-2017-3-kiberbiztonsagi-strategia-2-0-belaz-a-berzsenyi-d.original.pdf (Letöltve: 2017.04.01.)
- BÁNYÁSZ Péter: Kiberbűnözés és közösségi média, In. Nemzetbiztonsági Szemle, 2017/4., pp. 55-74., 2017.
- Büntető Törvénykönyvről szóló 2012. évi C. törvény 459. § (1) bek11.pont
- Dr. KRASZNAY Csaba: A rendvédelmi szervek helye a kibervédelemben, Magyar Rendészet, XIII. Évfolyam 2013. Különszám - 2013. szeptember p. 114.
- Európai Általános Adatvédelmi Rendelet http://www.adatvedelmirendelet.hu/a-rendelet-szovege/ (Letöltve: 2017.09.01.)

- Európai kábítószer-jelentés - Tendenciák és fejlemények 2017 http://www.emcdda.europa.eu/system/files/publications/4541/TDAT17001HUN.pdf_en (Letöltve: 2017.09.02.)
- GIRHINY Kornél: The roblem of the investigation of computer criminality, Studia Universitatis Babes-Bolyai Iurisprudentia Cluj-Napoca Románia 2015/ 2 218-230 o.
- http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208457%202007%20REV%202 (Letöltve: 2017.09.07.)
- http://www.valasztas.hu/hu/ovi/content/kozlemeny20170615ogyvalfelkeszules.pdf (Letöltve 2017. július 15.)
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/infographic-fraud-scams-targeting-employees (Letöltve: 2017.09.07.)
- https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects (Letöltve: 2017.09.03.)
- https://www.europol.europa.eu/newsroom/news/2017-european-police-chiefs-convention-largest-ever-gathering-of-global-police-chiefs-europol (Letöltve: 2017.09.07.)
- https://www.fbi.gov/news/stories/romance-scams (Letöltve: 2017.09.07.)
- KISS Tibor, PARTI Katalin: Informatikai bűnözés In: Borbíró Andrea, Gönczöl Katalin, Kerezsi Klára, Lévay Miklós (szerk.) Kriminológia. 1031 p. Budapest: Wolters Kluwer, 2016. pp. 491-517.
- Magyarország Alaptörvénye
- NYITRAI Endre: Civilnyilvántartások a nyomozásban, In: Gaál Gyula, Hautzinger Zoltán (szerk.), Tanulmányok a "Biztonsági kockázatok - rendészeti válaszok" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XV., Pécs, 2014, 224. o.
- NYESTE Péter: A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépésre, Felderítő Szemle 2013/1. szám.
- ORFK Tájékoztató (OT) 2016/21. szám
- Simon Béla: Hacktivism and its status in Hungary, Magyar Rendészet 16:(2) 2016 p. 161-174.