dr. Gyaraki Réka r. őrnagy: A nyomozóhatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában

A kiberbűnözés az egyik leggyorsabban terjedő és talán az egyik legveszélyesebb bűncselekmény, amely komoly kihívásokat állít a nyomozóhatóságok és a kibervédelemmel és kiberbiztonsággal foglalkozó hatóság- így az Országos Katasztrófavédelmi Főigazgatóság- elé.
A tanulmány célja, hogy a két szervezet feladatai és hatásköre tekintetében bebizonyítsam, hogy a közös együttműködésük a kiberbűnözés a kiberfenyegetés ellen elengedhetetlen. A büntetőjogi tényállások – a terrorcselekmény valamint a közérdekű üzem megzavarása- esetében a nyomozóhatóság eljárásában elengedhetetlen szerepe van a katasztrófavédelmi hatóságnak, mint ahogyan egy bekövetkezett kibertámadás esetén a károk elhárítása nem kizárólag a katasztrófavédelem feladata, hanem a rendőrség segítsége és fellépése is szükséges lehet egy esetlegesen bekövetkező veszélyhelyzet elhárítása érdekében.

Kulcsszavak: rendőrség, katasztrófavédelem, kibertámadás, terrorcselekmény, közérdekű üzem, kiberbűncselekmény

One of today's fastest expanding and probably the most dangerous crime is cyber criminality which challenges the investigative and other authorities that handle cyber crimes – including the National Directorate General for Disaster Management.
The goal of this study is to prove that the collaboration and cooperation of these two authorities in successfully fighting cyber crime and cyber treats is a must.
In criminal provisions – such as terrorist offence or disturbance of works of public interest – in the proceedings of the investigative authorities disaster management's role is crucial, just as to deal with the aftermath of cybercrime is not only the task of disaster management, but the police's help and presence could be required in parrying emergencies.
Key words: police, disaster management, cyber attack, terrorist offence, works of public interest, cybercrime

Az informatika fejlődése magával hozta a bűnözés megváltozását és a hagyományos elkövetés mellett vagy sok esetben helyett az információs rendszerek felhasználásával elkövetett deliktumok elszaporodását, amelyekben a bűncselekmény elkövetésének célja nem kizárólag az anyagi haszonszerzés lett, hanem az elektronikus rendszerekben tárolt adatok megszerzése, azok hozzáférhetetlenné tétele, az azokkal történő visszaélés és károkozás. Ezen célok akár külön-külön vagy együttes megvalósulása miatt lassan kezd elmosódni a határ a kiberbűnözés, a kibertámadás és a kiberhadviselés között.
Ahogy a tanulmány címe is mutatja, azokat a szervezeteket kívánom bemutatni, amelyek feladataik szempontjából összefonódnak, ugyanakkor mégis az adott probléma felmerülése kapcsán más és más módszerrel történő végrehajtást vár el tőlük a jogalkotó és a felügyeleti szervük, a Belügyminisztérium. Ez a két hazai szervezet működését, a hatáskör, és illetékesség szempontjából úgy szeretném bemutatni, hogy kifejezetten az elektronikus információs rendszer elleni jogellenes cselekmény bekövetkezése esetén történő összefonódásukat és az együttműködésük szükségességét vizsgálom majd meg.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Látszólag a két szervezet – a rendőrség és a BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) között nincs igazi kapcsolat, különösen nem a kibertérben elkövetett jogellenes cselekményekkel összefüggésben. Mégis az elmúlt időszakban bekövetkezett kibertámadások miatt fontosnak éreztem, hogy a szervezetek közötti együttműködésüket – különösen a jogszabályban meghatározott kötelezettségeiket és feladataikat- megvizsgáljam és a közös kapcsolódási pontokat megkeressem.
A tanulmányban végig kívánom vezetni, hogy:
1. a kiberbűncselekmény és a kibertámadás között milyen összefüggés van
2. a kiberbűncselekmény elleni küzdelem során milyen feladata van a rendőrségnek valamint az OKF-nek
3. a katasztrófavédelem szerepe és helyzete, valamint együttműködése más hatóságokkal.

A tanulmány első részében ismertetem azokat a feladatokat, amelyek a nyomozószervekre- a rendőrségre és az Országos Katasztrófavédelemi hatóságra hárul napjaink kiberfenyegetései miatt, majd pedig a két szerv közös feladatai illetve szükséges kapcsolódási pontjainak ismertetése következik a kibertámadások és kiberbűncselekmények megelőzése, felderítése és bekövetkezését követően a károk, veszélyek elhárítása, enyhítése vonatkozásában.
A szervezetek feladatainak ismertetése előtt szükséges, annak meghatározása, hogy mit is értünk kiberbűncselekmény (cyber crime) alatt és milyen rendszer alapján lehet meghatározni a jogellenes deliktumot, egyáltalán lehetséges-e egységes fogalomban meghatározni azt?
Három csoportba sorolom a kibercselekményeket:

1. Amikor a hagyományosnak nevezhető bűncselekményt az internet segítségével követik el. Ilyenek a különböző hirdetési, illetve aukciós oldalakon a nem létező vagy nem a meghirdetett minőségű termékek, szolgáltatások kínálása eladásra vagy bérlésre. Ezáltal megvalósul a csalás vagy közokirathamisítás, piramisjáték szervezése stb, de akár az „okoseszközök" elterjedése révén a lopás vagy rablás bűncselekménye is megvalósul.
2. Amikor önmagát az információs rendszert használják fel deliktum elkövetésére, vagy az információs rendszerben tárolt adatok, illetve a rendszer integritását sértő vagy veszélyeztető jogellenes cselekménnyel valósul meg a bűncselekmény. Ilyenek az információs rendszer felhasználásával elkövetett csalás, az információs rendszerben tárolt adatok megsértése, felhasználása... stb.
3. Amikor az elkövető jogellenes cselekménye támadást valósít meg úgy, hogy azok a kritikus infrastruktúrák információs rendszerei ellen irányulnak és amelyek sokszor találomra, a leggyengébb védelemmel ellátott berendezések ellen történnek.

A (kiber)bűncselekmények

A jog meghatározza, hogy mit is értünk bűncselekmény alatt. A hatályos büntető törvénykönyv szerint az a szándékos vagy- ha a törvény a gondatlan elkövetést is büntetni-gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre a törvény büntetés kiszabását rendeli[1].
A 2012. évi C. törvény, a Büntető törvénykönyv valamennyi törvényi tényállást meghatároz, ugyanakkor az, hogy mit is ért számítástechnikai környezetben elkövetett bűncselekmény alatt, azt nem tette meg a jogalkotó. Persze felmerül a kérdés, hogy ennek van-e relevanciája?!

[1] 2012. évi C. törvény 4.§ (1) bekezdés

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

Álláspontom szerint, bizonyos mértékig szükséges, hogy rendelkezzen- ha más nem a nyomozóhatóság a felderíthetőség miatt egy olyan pontos fogalommal, ami a nyomozási taktika kiválasztását elősegíti.
Amennyiben megelégszünk azzal, hogy minden olyan jogellenes cselekmény, amelyben az elkövetés eszközekén információs rendszer szerepel, akkor szinte valamennyi bűnelkövető kiberbűnöző is egyben, hiszen majdnem mindenki rendelkezik valamilyen eszközzel, amelynek működése összefüggésben van az internettel.
A hazai jogi szabályozás a számítástechnikai bűncselekményeket a büntető kódexünkben nem egy fejezet alatt tárgyalja hanem sok esetben a törvényi tényálláson belül, mint elkövetési magatartást emeli ki az információs rendszerben alkalmazott kifejezésekkel illetve a törvény indoklásában utal a 2001-es Számítógépes Bűnözésről szóló Egyezményben vállalt kötelezettségünkre.

A kiberbűncselekmények kategóriái:

I. „Klasszikus cybercrime": adathalászat, kibertámadások, internetes csalások, online banking csalások
II. Gyermekek online szexuális kizsákmányolása: gyermekpornográfia, egyéb (szexuális zsarolás, beszervezés..) nemi élet szabadsága és nemi erkölcs elleni bcs
III. Bankkártyabűnözés

A kiberbűncselekmény fogalma valamennyi tényállásból és a fenti kategóriákból összegezve- a következők szerint határozható meg-: informatikai eszközök és/vagy rendszerek segítségével, vagy informatikai eszközök és hálózatok ellen elkövetett bűncselekmények, amelyek célja a rendszerben tárolt adatok megszerzése, hozzáférhetővé tétele vagy éppen a jogosultak számára hozzáférhetetlenné tétele, melynek célja lehet anyagi haszonszerzés vagy az informatikai rendszerbe vetett bizalom megszerzése. Külön kategóriát képeznek azok a számítógéphez kapcsolódó bűncselekmények, amelyeket a törvény más tényállás alapján büntet (például pedofília), de ebben a részben azzal külön nem kívánok foglalkozni.

A kibertámadás

A kibertámadás fogalmát egy HM utasítás határozza meg. Ez alapján *kibertámadásnak minősül a kibertéren keresztül történõ támadás, melynek célja egy információs környezet vagy infrastruktúra üzemelésének megszakítása, kikapcsolása, megsemmisítése, felügyeleti jogának megszerzése, a kezelt adat integritásának megsemmisítése, vagy a felügyelet alatt álló adat megszerzése*[2].

Ahogy az utasításból is kiolvasható, a kibertámadás valamilyen információs infrastruktúra elleni támadás, amelynek célja az abban tárolt adatok megszerzése, magának a rendszernek a megsemmisítése, kikapcsolása.

[2] 60/2013 (IX.30) HM utasítás A Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról (forrás:http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/10.pdf, letöltve: 2017. július 30)
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

A kiberbűncselekmények jellemzőit - és az általam meghatározott fogalomból valamint a kibertámadás jogszabályi fogalmát kielemezve megállapítható, hogy a két jogellenes tevékenység összefügg, azok sok helyen kapcsolódnak.
Egy általam felállított tézis, miszerint minden kibertámadás bűncselekmény, ugyanakkor nem minden kiberbűncselekmény kibertámadás, a fentiek alapján megállja a helyét.

Kibertámadások fajtái[3]:
- illetéktelen hozzáférés az információkhoz
- illetéktelen adatbevitel
- rosszindulatú szoftverek bevitele
- információs környezetszennyezés

1. A rendvédelmi feladatokat ellátó szervezetek

1.1. Rendőrség
Magyarország közbiztonságáért, a rendvédelmi, bűnüldözési és bűnmegelőzési feladatok ellátásáért a Belügyminisztériumhoz tartozó rendőrség felelős. A rendőrség feladatait elsősorban az 1994. évi XXXIV. törvény a Rendőrségről szabályozza, de munkájuk során tekintettel kell lenniük az 1998. évi XIX. törvényre, a 2012. évi C. törvény, büntetőtörvénykönyvre, illetve a 25/2013 (VI.24) BM rendelet a rendőrség hatásköréről és illetékességéről szóló rendeletre, amely a rendőrség szervezeti tagolódását szabályozza. Ezen jogszabályokon kívül a nyomozóhatóság a 23/2003 (VI.24) BM rendelet a belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól szóló rendelet és további belső utasítások alapján látja el feladatait.
A rendőrség a feladatait az Alaptörvényben meghatározott jogok és kötelezettségek szem előtt tartása és amellett végzi, mindeközben védik az állampolgárok biztonságát és a gondoskodnak a törvények betartásáról és betartatásáról. A rendőrség feladata talán az egyik legösszetettebb, hiszen a közrendvédelmi, bűnügyi és szabálysértési terület mellett ellát egyéb feladatokat is.

A rendőrség bűnügyi feladatai ellátása során az Alaptörvényen kívül az 1998. évi XIX. törvény a büntetőeljárásról szóló törvény, a 2012. évi C. törvény a Büntető Törvénykönyv, az 1994. évi XXXIV. törvény a Rendőrségről és a 25/2013 (IV.24) BM rendelet és további, az ügyek szempontjából szükséges jogszabályok szem előtt tartásával végzik. Minden büntetőeljárás megindításánál az első lépés a hatáskör és illetékesség vizsgálata, amely alapján az elkövetés helye, jellege, az elkövetett kár mértéke alapján folytatja le az arra jogosult szerv a vizsgálatot.

Mit értünk illetékesség alatt?
Az illetékesség kérdésében az elkövetés helyének megállapítása a fő szempont. Azaz, az illetékesség alatt a földrajzi, területi meghatározást értjük. A BM rendelet 3. § -a alapján *a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt - sorozat-bűncselekmények esetén a bűncselekmények többségét - elkövették.* Amennyiben az elkövetés helye nem állapítható meg, vagy pedig a cselekmény jellegéből adódóan a több hatóság lenne jogosult lefolytatni az eljárást, akkor a megelőzés elve érvényesül, vagyis ott fogják az ügyet kivizsgálni, ahol korábban intézkedtek.

---

[3] Haig Zsolt-Várhegyi István: Hadviselés az információs hadszíntéren (Zrínyi Kiadó Budapest 2005, 230. oldal)
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Az illetékesség esetében megkülönböztetünk általános, kiemelt és kivételes illetékességet, aminek meghatározása fontos.
Általános illetékességű nyomozó hatóságok a rendőrkapitányságok, a kiemelt illetékességű a megyei rendőrfőkapitányságok, a Budapesti Rendőr-főkapitányság valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda és a Reptéri Rendészeti Igazgatóság.

A hatáskör és illetékességgel különösen szükséges a kiberbűncselekmény esetében foglalkozni, mert az elmúlt időszakban több alkalommal is felmerült probléma, hogy a számítástechnikai környezetben elkövetett bűncselekmények esetében mi tekintendő az elkövetés helye?
Első gondolatra sokakban az a válasz fogalmazódik meg, hogy ott követik el a kiberbűncselekményeket, ahol maga az eszköz található. Ugyanakkor a válasz ennyire nem egyszerű ennél a deliktumnál, hiszen ma, amikor már az asztali számítógépek helyett laptopokat, tableteket és okostelefonokat használunk, amelyek mozgatása, helyváltoztatása egyszerű, akkor már ennyire nem evidens a válasz. Amennyiben valaki útközben (két település között vagy éppen két ország között utazva követi el egy vállalkozás ellen a jogellenes tevékenységét, akkor annak megállapítása, hogy ki jogosult megindítani a nyomozást már ennyire nem egyszerű).
Létezik az illetékesség megállapítására is olyan nézőpont, miszerint az elkövetés helye ott van, ahol maga a kibertérben elkövetett jogellenes cselekmény ténylegesen megvalósul (így fordulhatott elő az a probléma, amikor az elektronikus cégbejegyzés megjelent, hogy a cégbíróság székhelye szerinti kerületi kapitányságnál a közokirat-hamisítások miatt indított eljárások száma megsokszorozódott, mert valamennyi olyan ügyben, ahol cégbejegyzés, vagy cégváltozással kapcsolatban történt feljelentés vagy jogellenes cselekmény, azok a kerületi kapitányságra lettek továbbítva).

A fentiek értelmezése alapján azt gondolom, hogy a kibertér esetében- bár az nem egy egységesen meghatározott terület, tér- is megállapítható, hogy melyik nyomozószerv jogosult eljárni.
A nyomozó hatóság a hatáskörét és az illetékességét hivatalból vizsgálja[4], amennyiben valamelyik hiányát észleli, akkor *átteszi a hatáskörrel és illetékességgel rendelkező nyomozó hatósághoz vagy ügyészhez*[5].

1.2. Készenléti Rendőrség Nemzeti Nyomozóiroda
A 25/2013 BM rendelet 2. számú melléklete alapján a Készenléti Rendőrség Nemzeti Nyomozóiroda hatáskörébe tartoznak - teljesség igény nélkül- a következő számítástechnikai környezetben elkövetett bűncselekmények:
- a nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények
- Nukleáris létesítmény üzemeltetésével visszaélés bűntette[6]
- Atomenergia alkalmazásával visszaélés bűntette[7]
- az állam elleni bűncselekmények[8]
- az igazságszolgáltatás elleni bűncselekmények[9]

[4] 25/2013 (IV.24) BM rendelet BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről 4.§ (1) bekezdése
[5] 25/2013 (IV.24) BM rendelet 4.§ (2) bekezdése
[6] Btk. 251.§
[7] Btk.252.§
[8] Btk. XXIV. fejezet
[9] Btk. XXVI. Fejezet
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

- Háborús uszítás bűntette[10]
- Különösen jelentős kárt okozó csalás bűntette, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja[11]
- Különösen jelentős vagyoni hátrányt okozó gazdasági csalás bűntette, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja[12]
- Különösen jelentős kárt okozó információs rendszer felhasználásával elkövetett csalás, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja[13]
- Pénzhamisítás előkészülete, ha az a KR kizárólagos hatáskörébe tartozó bűncselekmény elkövetésére irányul[14]
- pénzmosás[15]
- tiltott adatszerzés és az információs rendszer elleni bűncselekmények[16]
- Fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából elkövetett tiltott adatszerzés bűntette[17]
- Közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése bűntette[18]
- Közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége, kivéve az RRI hatáskörébe tartozó eseteket[19].

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály- 2017. Január 01 óta- három osztályra tagolódik. Az egyik osztály végzi a hatáskörükbe tartozó vagy magukhoz vont bűncselekmények nyílt nyomozását- így a kihallgatásokat és az 1998. évi XIX. törvényben felsorolt eljárási cselekményeket.
A másik osztály a kiberbűncselekmények felderítését végzi a büntetőeljárásról szóló törvény valamint az Rtv. alapján.
A harmadik osztály a Forenzikus Osztály, feladata nemcsak a szervezetükön belüli, hanem más, hazai rendőri szervnek is a szakértői tevékenység elvégzése, támogatása, valamint egyéb bűncselekmény során keletkezett adatok, evidenciák mentése, értékelése, elemzése úgy, hogy azok alkalmasak legyenek a bíróság előtt a bizonyításra.

A KR Nemzeti Nyomozóiroda a fent említett BM rendelet alapján a következőkben lehet röviden a feladatait meghatározni:

- büntetőeljárás lefolytatása
- operatív felderítés
- forenzikus tevékenység
- OSINT jelentések, elemzések készítése
- Monitorozás
- Rendezvény biztosítás
- Hazai együttműködés
- Nemzetközi együttműködés

[10] Btk. 331. §
[11] Btk. 373. § (6) bekezdés *a)* pont
[12] Btk. 374. § (6) bekezdés *a)* pont
[13] Btk. 375. § (4) bekezdés *a)* pont
[14] Btk. 389. § (3) bekezdés
[15] Btk. XL. Fejezet
[16] Btk. XLIII. Fejezet
[17] Btk. 422. § (2) bekezdés
[18] Btk. 423. § (3) bekezdés
[19] Btk. 424. §

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

- Szakirányítás, segítségnyújtás
- a rendőri és igazságszolgáltatás egyéb területein dolgozók (ügyészek, bírók) oktatása

1.3.Budapesti Rendőrfőkapitányság

A Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztály foglalkozik a főváros területén elkövetett kiberbűncselekményekkel.
Az általános szabály szerint, minden olyan deliktum esetében, amelynek tárgya vagy eszköze informatikai berendezés vagy információs rendszer és amennyiben nem éri el az elkövetési érték az 50 millió forintot, vagy egyéb minősítő körülmény nem merül fel, úgy az illetékességgel rendelkező kerületi rendőrkapitányság jogosult eljárni Budapest területén elkövetett jogellenes cselekmények esetén.

1.4.Nemzeti Adó-és Vámhivatal (NAV)

A Nemzeti Adó-és Vámhivatal feladatai a klasszikus adó és illetékkiszabások mellett büntetőeljárások lefolytatása. A NAV Bűnügyi Főigazgatóság Központi Nyomozó Főosztály Információtechnológiai Osztály feladata a különböző informatikai eszköz felhasználásával elkövetet jogellenes cselekmény nyomozása . A Főigazgatóság hatáskörébe tartozik az egy milliárd forintot meghaladó értékre üzletszerűen, vagy bűnszövetségben elkövetett bűncselekmények, a bűnszervezetben elkövetett bűncselekmények, valamint az olyan bűncselekmények nyomozása, amelyeket az elkövető személye, vagy az elkövetés körülményei, illetve a bűncselekmény társadalomra való veszélyességének kiemelkedő foka miatt a Bűnügyi Főigazgatóság hatáskörbe vont, illetve utalt bűncselekmények nyomozása.
A NAV hatáskörébe a következő bűncselekmények nyomozása tartozik[20]:

- nemzetközi gazdasági tilalom megszegése (Btk. 327. §),
- nemzetközi gazdasági tilalom megszegése feljelentésének elmulasztása (Btk. 328. §),
- haditechnikai termékkel vagy szolgáltatással visszaélés (Btk. 329. §),
- kettős felhasználású termékkel visszaélés (Btk. 330. §),
- orgazdaság, ha vámellenőrzés alól elvont nem közösségi árura vagy jövedéki adózás alól elvont termékre követik el (Btk. 379. §),
- bitorlás (Btk. 384. §),
- szerzői vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §),
- védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §),
- jogkezelési adat meghamisítása (Btk. 387. §) és iparjogvédelmi jogok megsértése (Btk. 388. §),
- társadalombiztosítási, szociális vagy más jóléti juttatással visszaélés (Btk. 395. §),
- költségvetési csalás (Btk. 396. §),
- költségvetési csaláshoz kapcsolódó felügyeleti vagy ellenőrzési kötelezettség elmulasztása (Btk. 397. §), jövedékkel visszaélés elősegítése (Btk. 398. §),
- számvitel rendjének megsértése (Btk. 403. §),
- csődbűncselekmény (Btk. 404. §), engedély nélküli nemzetközi kereskedelmi tevékenység (Btk. 406. §),

[20] forrás: https://www.nav.gov.hu/nav/bunugy/buncselekmenyek/buncselekmenyek.html (letöltve: 2017. június 20)

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

- versenytárs utánzása (Btk. 419. §),

továbbá a felsorolt bűncselekményekkel összefüggésben elkövetett:

- közokirat-hamisítás (Btk. 342-343. §),
- hamis magánokirat felhasználása (Btk. 345. §),
- egyedi azonosító jellel visszaélés (Btk. 347. §),
- bélyeghamisítás (Btk. 391. §),
- pénzmosás (Btk. 399-400. §)
- és a pénzmosással kapcsolatos bejelentési kötelezettség elmulasztása (Btk. 401. §).

Az említett bűncselekmények közül a hagyományos kiberbűncselekmény a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye, amely csak 2011. január 01-je óta tartozik kizárólag a NAV hatáskörében- azt megelőzően a rendőrség is hatáskörrel rendelkezett ezen deliktum nyomozásában.

A szerzői vagy szerzői joghoz kapcsolódó jogok bűncselekménye során az IT osztály feladata internetes monitorozás, azon során a jogsértések feltárása a jogsértés módjának meghatározása, továbbá az okozott vagyoni hátrány meghatározása, a jogsértő azonosítása, a Btk.77.§-a alapján a jogsértő adat eltávolítására tett indítvány és annak ellenőrzése.

BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF)

Magyarországon a BM OKF feladatát a köztudatban a tűzesetekre, a balesetek esetén a mentésre, valamint az egyéb veszélyek elhárítására szűkítették. Pedig tevékenységük nemcsak a fizikai biztonságra, hanem a kibertérből érkező fenyegetések és támadások elhárítására és megelőzésére, a kritikus infrastruktúra (vagy ahogy a magyar jogi szabályozás is nevezi létfontosságú rendszerelemek) védelmére, az iparbiztonságra is kiterjed.
A BM OKF feladatai miatt leginkább a Kibervédelmi Intézettel történő kapcsolattartás, az létfontosságú rendszerelem elleni incidensek bejelentése, ezek által egy aktív együttműködés.
A kritikus infrastruktúrák azonosításáról és kijelölésükről illetve ezek védelmi fejlesztéseinek szükségességéről szóló 2008/114/EK tanácsi Irányelv 2008-ban jelent meg. Magyarországon a Zöld Könyv megjelenése (2007) után 2010-ben kapott új lendületet a hazai létfontosságú rendszerek és létesítmények védelmével kapcsolatos szabályozások kidolgozása. A Zöld Könyv szerint „*az infrastruktúrák folyamatos működése, kockázati tényezőkkel szembeni ellenálló képességének növelése a lakosság, az infrastruktúra tulajdonosok, üzemeltetők, valamint a gazdaság szereplőinek és az állam számára egyaránt kiemelt fontossággal bír, a biztonságos működést elősegítő környezet és intézkedések ezért értéket képviselnek.”*[21]
A kritikus infrastruktúrákkal kapcsolatos a 2013. március 1. napján hatályba lépett létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben, valamint a hozzá kapcsolódó 65/2013. (III. 8.) általános végrehajtási kormányrendeletben meghatározott védelmi feladatok. A jogszabály célja egyrészt a létfontosságú rendszerelemek azonosítása, másrészt a kijelölés megtörténte után a megfelelő szintű - humán, fizikai és informatikai - védelem biztosítása

A létfontosságú rendszerelemek fogalma alatt a hazai jogi szabályozás az alábbi definíciót adja meg: „*a.....meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer*

---

[21] 1249/2010. (XI.19) Korm.határozat 1. számú melléklete- a nemzeti kritikus infrastruktúrák védelmének célja és alkalmazási köre

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához -, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna",[22]...
A létfontosságú rendszerelem védelmének meghatározása, ami többek között az OKF feladata: *„ a létfontosságú rendszerelem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység."[23]*

A BM OKF Országos Iparbiztonsági Főfelügyelőség tevékenységi körén belül kiemelt helyet foglal el a kritikus infrastruktúra védelmi szakterület, melynek egyik fő tevékenysége a jogalkotási és szabályozási feladatok végrehajtása.

A létfontosságú rendszerelemeket érő fenyegetések:
- természeti csapások
- műszaki/technikai hibák, zavarok, amelyek a működésük közben lépne fel
- emberi mulasztások
- terrorizmus
- ipari kémkedés
- szabotázs

A fent felsoroltakon kívül, akár azokhoz kapcsolódóan a kiberbűnözés- így a zsarolóvírusok , a kiberterrorizmus és a különböző hackertámadások valamint a rendszereik nem megfelelő üzemeltetése, felügyelete, a belső szabályozás hiánya illetve azok kijátszása is veszélyezteti a kritikus információs infrastruktúrát.

A BM OKF feladata többek között, hogy koordinálja a kritikus infrastruktúrák védelmével kapcsolatos hálózatbiztonsági intézkedéseket, valamint végzi a hálózatbiztonsággal kapcsolatos események elemzését, és azok értékelését is.

Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK)
A BM Országos Katasztrófavédelmi Főigazgatóság szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja - az állam és önkormányzat által üzemeltetett létfontosságú rendszerek és létesítmények kivételével - ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet.
Az LRLIBEK feladat- és hatáskörét a 185/2015. (VII. 13.) Korm. rendelet 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, 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.
Ezen fenti szabályozás alapján a Hatóság az eseménykezeléssel kapcsolatban a következő feladatokat lát el a 2013. évi L. törvény (Ibtv.) alapján:

[22] 2012. évi CLXVI. törvény a létfontosságú rendszerelemek védelméről Értelmező rendelkezések 1.§ f) pontja
[23] Lrtv 1.§ e)pontja
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

• a szervezetekkel való kapcsolattartás a bejelentett biztonsági események fogadására, valamint azok kezeléséhez szükséges intézkedések megtétele és koordinációja (20. § c.),
• a magyar kibertér rendszeres biztonsági helyzetértékelésének elvégzése (20. § d.),
• folyamatosan elérhető 24 órás ügyelet működtetése (20. § e.),
• a biztonsági események kivizsgálásának támogatása, amely során elvégezheti a biztonsági események adatainak műszaki vizsgálatát, amelyhez adatokat és az adatokhoz elektronikus hozzáférést kérhet (20. § f.).
• azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági fenyegetettségekről, ezek magyar nyelvű megjelenítése (20. § i.),
• hazai információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt (20. § k.),
• nemzetközi információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt (20. § l.),
• együttműködik a hatósággal, továbbá szükség szerint a biztonsági esemény kezelése tekintetében érintett szervezetekkel (20. § m.).

A fentieken túl az eseménykezeléssel kapcsolatos feladataik a 185/2015. Korm. Rendelet szerint:
• a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítése (4.§ a.)
• biztonsági eseményekről nyilvántartás vezetése (személyes adatokat nem tartalmaz, megtett intézkedések és azok eredménye kerül rögzítésre) (4.§ b.)
• az érintettek számára a biztonsági események kezelése során szakmai támogatás nyújtása (4.§ c.)
• az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben az üzemeltetők, a hatóságok és az eseménykezelő központok tájékoztatása (5. § 2.) bek. b.)
• évente jelentés készítése a tevékenységéről az irányító miniszter részére (5. § 3.) bek. c.)
• (nem kötelező érvényű) állásfoglalások, ajánlások kiadása (5. § 4.) bek. a.)
• a biztonsági események kezelésére irányuló tájékoztató tartása (5. § 4.) bek. b.)
• részvétel az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában (5. § 4.) bek. b.)
• szakértői-oktatói tevékenység végzése (5. § 4.) bek. b.)
• információtechnológiai, hálózatbiztonsági, és biztonságiesemény-kezelési együttműködési fórum működtetése (5. § 4.) bek. c.)

Az előzőekben felsorolt feladatokra figyelemmel a következőkben a tanulmány címében kiemelt két szervezet, azaz a rendőrség és a katasztrófavédelem kapcsolatát vizsgálom, amelyet leginkább a felsorolt feladataik alapján a kritikus infrastruktúrákat érő kibertámadásokban lehet a legjobban érzékeltetni.
További kapcsolódási pont a két szervezet között, hogy a rendőrség, mint közbiztonságot ellátó szervezet nemcsak a létfontosságú infrastruktúrák védelméhez kapcsolódó feladatot lát el, hanem önmaga is beletartozik a kritikus infrastruktúra 10 ágazata közé. Így a 512/2013. (XII. 29.) Korm. rendelet alapján a BM OKF az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről szóló jogszabály alapján a rendvédelmi szervek kijelölt infrastruktúrájának védelmével kapcsolatban a katasztrófavédelem lát el feladatokat, illetve kijelölő hatóságként jár el.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

További vonatkozó jogszabályok[24]

Az információs rendszerek elleni támadások fogalmánál már megjelenik annak értelmezése, hogy a kiberbűncselekmények és a kibertámadások nem választhatók el egymástól, így ebben a fejezetben az egymással összekapcsolódó jogi szabályozást tekintem át, amelynek a legutolsó momentuma a kiberbűncselekményekre vonatkozó büntetőjogi jogszabályt is tartalmazó 2012. évi C. törvény a Büntető Törvénykönyv egyes tényállásainak ismertetése.

A 2012. évi C. törvény a Büntető Törvénykönyv alapján három tényállást vizsgáltam meg:
A Btk. 323.§-a a közérdekű üzem működésének megzavarása, valamint a Btk.314-316§§., terrorcselekmény és az információs rendszer védelmét biztosító technikai intézkedés kijátszása (Btk.424.§).

Közérdekű üzem működésének megzavarása
323. § (1) Aki közérdekű üzem működését jelentős mértékben megzavarja, bűntett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.

A közmű meghatározása: olyan termelő-vagy szolgáltató üzemek, amelyek a lakosság, továbbá az ipar, a mezőgazdaság, a szolgáltató tevékenység kiterjedt körét vízzel, elektromos, gáz-,gőz-, vagy hőenergiával látja el[25]. Továbbá a közösségi közlekedési üzem, amely a tömeges közlekedés lebonyolítására alkalmas, a használók széles köre által igénybe vehető közlekedési eszközök üzeme. A tényállást kell alkalmazni az elektronikus hírközlő hálózatokra is, továbbá az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemekre is.

A bűncselekmény nyitott törvényi tényállásnak lehet nevezni, hiszen a törvényalkotó nem határozza meg benne az elkövetési magatartást, így elkövethető szándékosan, tevéssel vagy éppen mulasztással is.
A deliktum a fent felsorolt közműhálózatba okozott bármilyen zavarral már bekövetkezett a az eredmény. A bűncselekmény elkövetője tettesként bárki lehet.

Terrorcselekmény
314. § (1) *Aki abból a célból, hogy*
a) állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűrjön,
b) a lakosságot megfélemlítse,
c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja,
a (4) bekezdésben meghatározott személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el, ...
(2) Az (1) bekezdés szerint büntetendő, aki az a) pontban meghatározott célból
a) jelentős anyagi javakat kerít hatalmába, és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé, vagy
b) terrorista csoportot szervez.

---

[24] Kizárólag a rendőrség hatáskörébe tartozó bűncselekményekkel foglalkozom, így a Nemzeti Adó-és Vámhivatalt érinti deliktumok ebben a tanulmányban nem szerepelnek. A továbbiakban ezért kizárólag a Rendőrség fogalma szerepel.
[25] Kereszty Béla-Maráz Vilmosné-Nagy Ferenc-Vida Mihály: A magyar büntetőjog –Különös része, (Korona Kiadó, Budapest, 2004. p. 457.oldal)
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

.....
(4) E § alkalmazásában személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekmény
....
c) a közlekedés biztonsága elleni bűncselekmény [232. § (1)-(2) bekezdés], a vasúti, légi vagy vízi közlekedés veszélyeztetése [233. § (1)-(2) bekezdés],
d) a radioaktív anyaggal visszaélés [250. § (1)-(2) bekezdés],
f) a jármű hatalomba kerítése [320. § (1)-(2) bekezdés], a közveszély okozása [322. § (1)-(3) bekezdés], a közérdekű üzem működésének megzavarása [323. § (1)-(3) bekezdés], a robbanóanyaggal vagy robbantószerrel visszaélés [324. § (1)-(2) bekezdés], a lőfegyverrel vagy lőszerrel visszaélés [325. § (1)-(3) bekezdés],
g) a nemzetközi szerződés által tiltott fegyverrel visszaélés [326. § (1)-(5) bekezdés], a haditechnikai termékkel vagy szolgáltatással visszaélés [329. § (1)-(3) bekezdés], a kettős felhasználású termékkel visszaélés [330. § (1)-(2) bekezdés],
h) a rablás és a rongálás,
i) az információs rendszer vagy adat megsértése
***315. §** (1) Aki a 314. § (1) vagy (2) bekezdésében meghatározott bűntett elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja...*[26]

A terrorcselekmény jogi tárgya az állami szervek, más államok, a nemzetközi szervezetek zavartalan, kényszertől mentes működéséhez, a lakosság megfélemlítéstől mentes életviteléhez fűződő társadalmi érdek.[27]
Az elkövetési magatartás a tényállás alapján a tűrésre kötelezés, megfélemlítés, alkotmányos rend megváltoztatása, nemzetközi szervezet működésének megzavarása, anyagi javak hatalomba kerítése és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé[28]. A szakirodalom ennél a bűncselekménynél meghatároz egy cél- illetve eszközcselekményt is. Az eszközcselekménye a jelentős anyagi javak hatalomba kerítése, amely nem feltétlenül jelenti a jogellenes birtokbavételt és a rendelkezési jog gyakorlását. A kibertérből érkező fenyegetések[29]- értve ezalatt a zsarolóvírus kritikus információs infrastruktúrához történő eljuttatását- már teljes mértékben kimeríti a terrorcselekmény fogalmát. Mivel a törvény az előkészületet is bünteti, így már akkor önmagában csak azzal elköveti valaki a cselekményt, hogy akár egy adott KI információs rendszerének sérülékenységét ismerve, arra célzottan elkészíti a programvírust, de ugyanúgy az is elköveti a jogellenes cselekményt, aki – bár nem tudva a sérülékenységekről- az általa megírt rosszindulatú programot megír ami egy adott, létfontosságú rendszerelem működését veszélyezteti vagy abban zavart okoz.

Rendőrség- BM OKF

---

[26] net.jogtar.hu

[27] Blaskó-Hautzinger-Madai-Pallagi-Polt-Schubauer: Büntetőjog különös rész II. (Rejtjel Kiadó, Budapest 2015) 16. oldal

[28] Btk. 314.§ (1) és (2) bekezdés

[29] Ibtv 1.§ 16. pontja meghatározza, hogy mit is jelent a fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemi védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

A BM OKF hatósági jogkörében eljárva ellenőrzi a biztonsági szintekre vonatkozó követelmények teljesülését[30], ellenőrzését, kockázatelemzését és a különböző biztonsági eseményekkel kapcsolatos bejelentéseket kivizsgálása, ennek megfelelően a hatóságokkal (többek között az eseménykezelő központtal, amely felé az incidens jelenti) történő együttműködés.
A bekövetkezett támadás esetén, szükséges mértékben- mind a két szervezetnek feladata is van. A kritikus információs infrastruktúrák működésével kapcsolatos szabályozás, biztonsági szintjének besorolása, az annak kezelésére jogosult személyek kijelölése stb. a BM OKF hatáskörébe tartozik. Éppen ezért egy információs rendszert érő támadás- súlyos biztonsági esemény bekövetkezése[31]- vagy akár „csak" annak kísérlete esetén az ő feladatuk többek között a további hatóságok- így a GovCert, Alkotmányvédelmi Hivatal, Rendőrség- értesítése és a szükséges intézkedés és tájékoztatás megtétele.
Súlyos biztonsági esemény „*olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek."*

Mivel az említett két bűncselekmény nyomozása (is), a további bűncselekmények megakadályozása, az elkövető kézre kerítése a rendőrség, ezen belül a hatáskörre vonatkozó utasítás alapján a Készenléti Rendőrség Nemzeti Nyomozóiroda hatáskörébe tartozik, így azok bekövetkezése esetén a rendszer működéséről, a kialakult veszélyhelyzetről a legteljesebb információval ők rendelkeznek.

Egyéb közös feladatok elvégzése

Egy bekövetkezett kibertámadás során a létfontosságú rendszerelemek információs rendszereiben keletkezett problémák befolyással lehetnek az adott rendszerelem más területét- a berendezések funkcióját- súlyos biztonsági esemény, amely ezáltal veszélyeztetik a működésének folytonosságát és a katasztrófához vezethetne.
A támadás következtében bekövetkezett zavar elhárítása ugyanakkor nem kizárólag a Katasztrófavédelem feladata. A lakosság létfenntartását, egészségét, biztonságát szolgáló ideiglenes intézkedések és cselekvések- így akár a vízművek elleni támadás, amely következtében nincs vagy nem megfelelő az ivóvízellátás, a napi adag pótlásának eljuttatása- mind a katasztrófavédelem, mind a rendőrség, mind pedig a honvédelem feladata.

Bibliográfiai hivatkozások jegyzéke:

1. HAIG Zs.-VÁRHEGYI I.: Hadviselés az információs hadszíntéren

[30] Ibtv. 9. § (1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

[31] A 2013. évi L. törvény (Ibtv.) 1.§ 41a. pontja határozza meg, hogy mit is értünk a súlyos biztonsági esemény alatt.
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült."

2. KERESZTY B.-MARÁZ V.-né-NAGY F.-VIDA M.: A magyar büntetőjog
3. BLASKÓ B.-HAUTZINGER Z.-MADAI-PALLAGI A.-POLT P.-SCHUBAUER L.: Büntetőjog különös rész II.
4. 2012. évi C. törvény a Büntető Törvénykönyv
5. 1998. évi XIX. törvény a büntetőeljárásról szóló törvény
6. 2013. évi L. törvény az állami és az önkormányzati szervek elektronikus információbiztonságáról
7. 2012. évi CLXVI. törvény a létfontosságú rendszerelemek védelméről
8. 25/2013 (IV. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
9. 60/2013 (IX.30) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának Kiadásáról

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”