VII. évfolyam 1. szám

R E N D V É D E L E M

2018/1. SZÁM

B U D A P E S T

– 2018 –

A BELÜGYI TUDOMÁNYOS TANÁCS

ONLINE FOLYÓIRATA

Felelős szerkesztő:

Dr. Dános Valér CSc/PhD
ny. r. vőrgy.
ügyvezető alelnök

TARTALOM

Szerkesztői előszó

A Belügyi Tudományos Tanács 2017. májusában pályázatot hirdetett meg *Az új évezred kihívása – digitális infokommunikációs képességek* címmel, *E-közigazgatás*, valamint a *Kritikus információs infrastruktúra* témákban.
Jelen számunkban a hat beérkezett pályamunka válik elérhetővé a téma iránt érdeklődők számára.

Az értékes tanulmányokhoz hasznos olvasást kívánunk!

A Bíráló Bizottság döntés szerinti pályázati eredmények:

„E-közigazgatás" témakörben

II. DÍJ

Dr. Szabó Csaba, Nagy Bence, Horváth Alexandra és Galambosi Barbara szerzőcsoport

KÜLÖNDÍJ

Érces Gergő

„Kritikus információs infrastruktúra" témakörben

II. DÍJ

Almási Csaba Sándor, Bártfai Fanni, Dr. Bonnyai Tünde, Dr. Gyaraki Réka Eszter, Kiss Sándor és Margitics József szerzőcsoport

III. DÍJ

Tóth Tamás

ELISMERŐ OKLEVÉL

Dr. Kovács István

Déri Attila

DR. SZABÓ CSABA – NAGY BENCE – HORVÁTH ALEXANDRA – GALAMBOSI BARBARA

A RENDŐRSÉG ELEKTRONIKUS FORMÁBAN VÉGZETT ÜGYINTÉZÉSÉNEK, MINT ÚJ KÉPESSÉG KIHÍVÁSAINAK KUTATÁSA

Bevezetés

A közigazgatás napjainkban egy modernizációs folyamaton megy keresztül. Ennek a folyamatnak a kikényszerítését elsősorban a változó társadalmi igények, másodsorban az Európai Unió közigazgatási reformokra vonatkozó törekvései, még harmadsorban a kormányzatnak a közigazgatás modernizációjára és költséghatékonyságára vonatkozó jogalkotói iránycéljai határozzák meg. A közigazgatás átalakítása során olyan kihívásokat kell figyelembe venni, mint az *ügyfélközpontú és bürokráciacsökkentő szolgáltatások kibővítésének lehetőségei, az Ügyfélkapu közigazgatási portál szolgáltatási rendszerének átstruktúrálása, a közigazgatási és hatósági ügyintézési folyamatok gyorsítása, a mobilplatformok fejlesztési irányvonalának kijelölése, vagy az elektronikus ügyintézés egyes rendszereinek integrálása a speciális hatósági feladatokat ellátó állami szervek feladatrendszerébe*. A közigazgatás átalakítása során figyelemmel kell lenni a tudomány által nyújtandó eredmények integrációjának lehetőségeire is. Jelen kutatás elsősorban azokra a tudományos eredményekre fokuszál, amelyek a közigazgatás azon kihívásait vizsgálja, amelyek összevetik a hagyományos ügyintézési formát (ügyfél és ügyintéző) az elektronikus formában végzett ügyintézéssel.

A kutatás első szakaszában felvázolja az e-közigazgatás általános elméletét, kibővítve és magyarázva azokkal a megállapításokkal, amelyek egy konkrét közigazgatási szakterület vonatkozásában vizsgálja a felvázolt hipotéziseket. Mivel az e-közigazgatás egy meglehetősen új interdiszciplináris szakterület, ezért a következtetések és javaslatok értelmezéséhez (a kutatás második szakasza) szükséges felvázolni olyan releváns nemzetközi közigazgatási modelleket, amelyek részeiben, vagy egészében új megvilágításba helyezik a kutatás eredményeit. A kutatás harmadik szakasza képviseli a bemutatásra kerülő szakterület hatékonysága és megújítása szempontjából fontos új álláspontokat, amelyek elemzésével felvázolásra kerülnek azok a kihívások, amelyek a rendőrség elektronikus formában végzett

ügyintézésének megújítását terhelik és/vagy hátráltatják. A kutatás negyedik szakaszában kvantitatív és kvalitatív kutatási módszerek együttes alkalmazásával vizsgáljuk az e-közigazgatás, valamint a rendőrség elektronikus ügyintézésének megújulási területeit az állampolgárok, mint ügyintéző személyek véleményeit elemezve az adott témakörben. Fókuszcsoportos interjúk keretében végezett (*párhuzamos*) vizsgálatok adatainak felhasználásával szakmai indikátorok és kijelölhető fókuszpontok kerülnek bemutatásra, amely a rendőrség összes szolgálati ágának bevonásával készült, figyelembe véve az e-közigazgatás kiszélesítésére vonatkozó kihívásokat és kockázatokat. A kutatás erősségét az e-közigazgatást érintő kihívások és kockázatok több oldalról történő megközelítése és vizsgálata nyújtja. A kutatás elsősorban az állampolgár - mint tényleges ügyintézést kezdeményeztő fél - szempontjából vizsgálja az aktuális kihívásokat az e-közigazgatás vonatkozásában, kiegészítve és keresztezve egy olyan még nem vizsgált speciális közigazgatási és hatósági jogkörrel rendelkező szervezet elektronikus közigazgatásra vonatkozó kihívásainak számbavételével, mint a rendőrség.

1. A e-közigazgatás tudományterületének átgondolása

A kérdéskör vizsgálata szempontjából elengedhetetlen az e-közigazgatás tudományterületének a pozicionálása, valamint egy átfogó megközelítést tartalmazó alapvető cél meghatározása. Az *e-közigazgatás alapvető célja*, hogy az állam az informatikai technológiák alkalmazásával és a közigazgatási rendszerekbe történő integrálásával biztosítsa a szolgáltatást igénybe vevő személyek számára a hatékony ügyintézést, valamint a releváns információk biztosítását úgy, hogy egyben hatékony költségfelhasználás és dinamikus ügyintézés kerüljön megvalósításra.[1] Számos hazai és nemzetközi eredményeket publikált tanulmány és a közigazgatás tudományterületét megalapozó kutatás fejti ki, hogy az e-közigazgatás alapvetően három tudományterület, nevezetesen a közigazgatás-tudomány, az informatika, a szervezés- és vezetéstudomány határán jött létre.[2] Ezt az elméletet erősíti meg hazai viszonylatban Budai Balázs, aki megfogalmazásában a három pillér stabilitásának nélkülözhetetlenségét emeli ki. Kutatásában felhívja a figyelmet a pszichológia, a szociológiai

[1] Az e-közigazgatás alapvető céljának megfogalmazása során a szerző a korábban a tudományterületre vonatkozó hazai és nemzetközi tudományos elméleteket vette elsődlegesen figyelembe, kiegészítve egyéni meglátásaival.

[2] Osborne, David – Hutchinson, Peter: *The Price of Government: Getting the Results Wee Need in an Age of Permanent Fiscal Crisis.* Basic Books, 2004. – pp. 25-28.

és a szociálpszichológiai tudományos eredményeinek fontosságára.[3] Mindazonáltal ezek a megközelítések figyelmen kívül hagynak egy lényeges tudományterületet, amely alkalmazásával hatékony eredményeket lehet elérni az e-közigazgatás fejlesztési irányvonalainak meghatározása vonatkozásában. Ez a tudományterület a statisztika. Jelen tanulmány egy hiánypótló kutatást végzett el az e-közigazgatás szakterületén a statisztika szakterületének a bevonásával. Akár a jelenlegi helyzetet vizsgáljuk, akár a jövőbeni irányvonalakat jelöljük ki egy szak-, vagy tudományterület sikeressége és alkalmazhatósága érdekében, lényeges szempont hogy tisztában legyünk a *hatékonyságával*, a *társadalomban betölteni kívánt szerepével és feladatrendszerével*, valamint a *szükségességével*. Az e-közigazgatás szakterületének az újra definiálásához a statisztika tudományterületének eszközeit használtuk fel, hogy válaszokat kapjunk a felvázolt hipotéziseinkre, és hogy a társadalmi szükségesség és hatékonyság elősegítése érdekében javaslatokat fogalmazzunk meg, mind a jogalkotás, mind a közigazgatás hatékonyságának elősegítése érdekében.

1.1. Az e-közigazgatás szerepe a hazai közigazgatásban

1.1.1. Az elektronikus formában végzett ügyintézés előnyei

Az elektronikus formában végzett ügyintézés számtalan olyan formákat biztosít, amelyek lehetővé teszik a gyorsabb és hatékonyabb közigazgatási folyamatok lebonyolítását. Sok esetben ez hatékonyabb és költségkímélőbb módszert is jelent, a hagyományos papír alapú ügyintézéssel szemben. Az ügyfél személyes jelenléte csak minimális esetben vagy egyáltalán nem szükséges a közigazgatási folyamat során. A kommunikációs eszközök fejlődésével párhuzamosan lehetőség nyílt bizonyos ügyek levélben, telefonon vagy egyéb telekommunikációs eszközön keresztül való ügyintézésére is. Utóbbi megoldás átmenetet képez a hagyományos és a modern ügyintézési metódusok között. Az e-közigazgatás számtalan előnnyel bír, azonban jelenleg vannak olyan hátrányok, amelyek kiküszöbölése érdekében elengedhetetlen a szakterület fejlesztése és újra pozicionálása. Az e-közigazgatás előnyei körébe sorolhatjuk a *gyorsaságot,* a *kényelmet,* a *folyamatos elérhetőséget*, az *alacsonyabb költségindexet*, az *interaktivitást* és a *kiterjedt lehetőségeket*. Mindezen előnyökkel szemben szükséges megfogalmazni azokat a kockázatokat, amelyek nagymértékben hátráltatják az e-közigazgatás elterjedését és hatékonyságát. Kockázatot jelent

[3] Budai Balázs: *Az e-közigazgatás elmélete – axiomatikus megközelítésben*. In.: Információs Társadalom: Társadalomtudományi Folyóirat. 2009. évi, 9. szám. – p. 69.

az adott közigazgatási honlapok szerkesztői által vétett hibák, az olykor elavult információk, az ügyet intéző személy kilétének hiánya, illetve (a kiberbiztonság szempontjából) létrehozhatnak olyan oldalakat, amelyek nem valósak adatokat tartalmaznak, így az adott személyek könnyen válhatunk csalás vagy lopás áldozatává.

Az elektronikus ügyintézés legfőbb előnye az egyszerű és gyors ügyintézés, ugyanis még a hagyományos személyhez kötött ügyintézés, meghatározott időben és helyen történik, addig (a tartózkodási helytől függően) az állampolgár elektronikusan intézheti ügyeit, hiszen az e-ügyintézés bármikor, kényelmesen kezdeményezhető otthonról, vagy akár munkahelyről. A másik előnye, hogy az ügyintézési folyamat elvégzése nem igényel ténylegesen papír felhasználást, ezáltal csökken a papír alapú ügyintézéssel járó környezetterhelés.[4] Az irattározási feladatok szintén nagyon minimálisra csökkenek és fontos kiemelni, hogy az elektronikusan tárolt dokumentumok között a visszakeresés nagyon egyszerű és gyors műveletté vált.

Az e- közigazgatás által nyújtott előnyök

[4] Ezzel kapcsolatban meg kell említeni az átmeneti, vagy végleges irattárakban elhelyezett papír alapú ügyiratok tárolásának, majd selejtezésének problémakörét is.

A bemutatásra került ábra jól szemlélteti, hogy nem csak a lakosság számára nyújt pozitív hatásokat az e-közigazgatás rendszere, hanem a vállalkozások és az állam számára is nyújt megfelelő alternatívákat a közigazgatási folyamatok gyorsítása és hatékonysága terén. Az állam szempontjából a pozitív érvek közé sorolható, hogy növeli a hatékonyságot, hiszen az online elérhető programok növelik például az információáramlást az egészségügyben, ezáltal gyorsabbá válik a betegellátás is. A vállalkozások szempontjából vizsgálva a pozitív hatásokat elmondható, hogy az e- ügyintézés megjelenésével növekszik a versenyképesség, hiszen csökken a hatósági ügyintézésre fordított idő, ezáltal a felszabadult időben az ügyintézők olyan tevékenységeket végezhetnek, melyek jobban szolgálják a profittermelő tevékenységet.

Az e-közigazgatás által javulnak a *szolgáltatások minőségei*, ugyanis a legtöbb országban ügyfélközpontú szemlélet uralkodik, ezáltal a felhasználók elvárásait figyelembe véve igyekeznek alakítani a közigazgatási struktúrát. Emellett javítja az életminőséget is, mivel az ügyintézésre fordított idő csökkentésével bővül az egyéb célokra rendelkezésre álló időkeret is.[5]

1.1.2. A hagyományos irodában végzett ügyintézés kihívásai

A hagyományos irodában végzett ügyintézés napjaink közigazgatási kultúráját tekintve nem egy hatékony ügyintézési forma.

Az ügyintézésben kezdeményező félként jelen lévő állampolgárokat is kihívások elé állító probléma a munkaidővel kapcsolatosan adódik, ugyanis ügyeket intézni csak meghatározott időben, úgynevezett munkaidőben lehetséges. Ez sok embernek okoz nehézséget, mert a magyar lakosság jelentős része is ugyanebben a meghatározott foglalkoztatási struktúrába dolgozik. A másik legszembetűnőbb dilemma, hogy a hagyományos irodában végzett ügyintézés helyhez kötött, melyet az ügyintézést kezdeményező ügyfélnek személyesen (*vagy meghatalmazott útján*) kell felkeresni. Alapvető nehézségként kell továbbá megemlíteni, hogy az ügyintézés szombaton, vasárnap, illetve ünnepnapokon (*némely speciális esetektől eltekintve*) nem történik a közigazgatásban.

---

[5] *Az e- közigazgatás előnyei*. (http://allampolgar.netenahivatal.gov.hu/miert-jo-az-e-kozigazgatas/az-e-kozigazgatas-elonyei-0 letöltés ideje: 2017.09.10.)

További kihívásként kell megemlíteni, hogy jelenleg a közigazgatási szektor jelentős részében az adatok tárolása és továbbítása papír alapon történik. Ez mellett tudunk érveket és ellenérveket is felsorakoztatni. Pozitív érvek körébe sorolhatjuk a könnyű ellenőrizhetőséget, hiszen a hosszabb terjedelmű dokumentumok oldalszámozással vannak ellátva, melyek hiányossága azonnal szembetűnő, illetve a nyomtatott példányok javítása, vagy átírása vizuális szempontból könnyen felismerhető és végrehajtható. A papír alapú dokumentumok hitelességét az adott személy aláírásával hitelesíti, ezáltal egyet ért az abban foglaltakkal és jogi érvénű hatálya keletkezik. Az ügyfél és az ügyintéző közötti személyes kontaktus igen fontos tényezője az ügyintézési folyamatnak. A személyes találkozó alkalmával lebonyolított ügyintézések metódusa kiforrott és leegyszerűsödött, erősítve a biztonságot és a kommunikációs hatékonyságot.

A hagyományos irodai ügyintézés folyamatának pozitivitása mellett a negatív és hátráltató tényezők vizsgálata is szükséges. A hagyományos ügyintézés hátrányai közül elsőként az ügyintézési folyamat lassúságát szükséges kiemelni. A teljes ügyintézési aktus sikerességéig több lépést kell megtennünk, amelyek az ügy érdemi elbírálása szempontjából kihagyhatóvá vállhatnak.[6] Akár egy közigazgatási szervezet, akár egy gazdasági társaság működési struktúráját vesszük alapul az ügyintézések során számos papír alapú dokumentum keletkezik. A hagyományos irodában végzett ügyintézést nagymértékben hátráltathatja az ügyintézést végző személy lassúsága is. Másik fő hátrány, hogy a nagy adathalmaz, amellyel az ügyintézők és a vezetők dolgoznak nem előnyös papír alapon. Ugyanis az ügyintézések során keletkezett adatmennyiség folyamatos növekedésével a feldolgozás kézi úton igazán bonyolulttá és időigényessé válik, amely egy idő után több problémát generál. Az egyes ügyirat típusokra vonatkozó selejtezési idő mértéke arányaiban nagyobb, ez által a papír alapú iratok mennyisége folyamatosan növekszik. Ezzel összefüggésben a rengeteg irat elhelyezése nagy gondot okozhat, nagyméretű irattároló szekrényt igényel és ez hátrányosan befolyásolja, mind az ügyintéző, mind az ügyfél hatékony együttműködését. Hangsúlyos kérdés az is, hogy a papír alapú dokumentálás esetében, hogyan történik a dokumentumok visszakeresése, esetlegesen több évre visszamenőleg is. Ez egy nagyon lassú folyamat, illetve minél régebbi a dokumentum, annál nehezebb visszakeresni. A közigazgatásban alkalmazott ügykezelési folyamat során a szervezetbe beérkező dokumentum első aktusként a postabontóba kerül, majd onnan a segédhivatalba, ahol az érkeztetést végzik. Az érkeztetést követően a beérkezett

[6] Az egyes közigazgatási ügyintézési lépések kihagyása a hatékonyság és gyorsítás érdekében mindenféleképpen újra gondolást igényel, mivel csak így érhető el a kívánt ügyintézési dinamika.

anyag iktatására, majd vezetői szignalizációjára kerül sor. A több lépcsős ügyintézési folyamat hátránya, hogy az ügyintézést folytató szervezethez kerülés lényegesen több időt vesz igénybe, mintha a dokumentum, vagy az ügyirat teljesen elektronikus formában kerülne hivatali feldolgozásra. Ez az időveszteség egy sürgős ügy esetében igen nagy fennakadásokat eredményezhet, amely az ügy érdemi döntésének tolódását is eredményezheti.[7]

1.1.3. A közigazgatási ügyfélszolgálati elvárások

A közigazgatási eljárások hatékonyságát és problémafeltáró jellegét vizsgálva figyelmet kell fordítani az ügyet kezdeményező emberek véleményére és igényeire egyaránt. Mindenki szereti ügyeit a lehető leggyorsabban és legkényelmesebben elvégezni, úgy hogy a hatékonyság iránti elvárás is kielégítésre kerüljön. Ezzel az állampolgári elvárással a közigazgatási ügykezelésben résztvevő minden szereplőnek számolnia kell és a lehető leghatékonyabb megoldásokat kell meg találni az emberek problémáira. Szükség van arra, hogy az emberek problémáinak struktúráját is lássa a hivatal, átérezze, értelmezze és az ügyfél legkisebb terhelésével oldja azt meg. Az ügykezelés komplexitása mellett igyekeznek az ügyeket közérthetővé, egyszerűvé és felhasználóbaráttá tenni.

Az ügyfelek elvárják (és egyben igénylik), hogy ügyeiket az általuk előre megválasztott időpontban, és olyan módon intézzék, ahogy azt ők szeretnék. Az ügyfél igénye nagymértékben meghatározza az ügy szerepét és jelentőségét. Az ügyfelek által megfogalmazott elvárások az egyén szerteágazó jelleméből fakadóan eltérők, azonban az alapstruktúra minden esetben hasonló jellegű.

A pozitív ügyintézői attitűd, nagymértékben befolyásolja az ügyfelet. Ide sorolhatjuk az olyan többletszolgáltatásokat, melyekre az ügyfél nem számít, azonban pozitívan csalódik benne. Például ilyen a *tájékoztatás, a tanácsadás, a közvetítésnyújtás és a szívélyesség*. Releváns tényező az is, hogy ha az ügyfelet nem éri kellemetlen meglepetés. Az ügyfél kiszámítható, átlátható és szabványos ügyintézésre számít, ha ezek valamelyike megváltozik azt, egy újabb tehernek fogja fel, amely csak rontja az ügyintézés színvonalát. „Az ügyfél minőségi, szakszerű és rendeltetésszerű szolgáltatást vár el. A hivatal erre olyan ügyportfólióval válaszol, ahol pontosan és hibamentesen azt kapja az ügyfél, amit kapnia kell, és pontosan annyit kell tennie, amennyit az ügy elintézéséhez feltétlenül muszáj. A

[7] *Informatikai biztonság és kriptográfia*. (http://www.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch01s03.html letöltés ideje: 2017.09.12.)

folyamatban az érdemi ügyintéző rendelkezik azzal a tudással (vagy eléri azt a tudástárat), hogy a lehető legjobb – tudásalapú– megoldást tudja kínálni.’’[8]

1.1.4. A fejlesztési irányvonalak a magyar közigazgatásban

A közigazgatás átszervezésére és modernizációjára vonatkozó fejlesztési irányvonalak kijelölése, már a rendszerváltás követő időszakban megkezdődött. A közigazgatás hatékonysága nem rendelkezett azokkal a dinamikus elemekkel, amelyek egy európai közigazgatási értékrendszer szerves részét képezhették volna. Ezeket a problémákat azonosítva Magyarország megkezdte az állami és közigazgatási műveletek átszervezését. A közigazgatás átalakítására vonatkozó folyamat eredményeként egy digitálisan szabályozott államgazdasággá vált, amely további cselekvési tervek formájában jelölte ki az e-közigazgatás kihívásaira vonatkozó irányvonalakat.[9]

A közigazgatási projektek első fázisa a lassú, papír alapú és a kevésbé hatékony rendszerekre irányult. Az állam célja egy digitális alapszolgáltatás létrehozása volt, amely egy hatékonyabb és gyorsabb ügyintézési mechanizmust valósít meg. Ez az átalakítás már figyelembe vette a közép- európai társadalmak ügyintézési igényeit és szokásrendszereit. Ennek következtében egy jelentős paradigmaváltás következett be a közigazgatási szektorban. Akár a jogalkotás, akár a kormányzat oldaláról vizsgáljuk meg az egyes kérdésköröket elmondható, hogy a legtöbb szakterületen sikerült átállni az elektronikus ügyintézésre és végrehajtásra, azonban még mindig találunk olyan közigazgatási szakterületeket, ahol még nem megoldott ennek a lehetősége. Mindazonáltal kijelenthető, hogy az állam megpróbál minél szélesebb körű e-szolgáltatásokat nyújtani az ügyintézést kezdeményező személyeknek. A jelenlegi és a közelmúltban megvalósított tervek messze meghaladják az előre kitűzött célokat és törekvéseket. A hatékonyság mellett megjelenik a *bevételszerzési* alkalmazások iránti igény, valamint a rugalmasabb és pontosabb szabályozás lehetősége, illetve szabálykonfigurációja. Nézzünk meg néhány olyan példát, ahol a közigazgatási rendszerek átalakításával igen magas hatékonyságú szintet sikerült elérni a hazai elektronikus ügyintézés

[8] Simon Barbara – Budai Balázs: *Elektronikus-közigazgatási modernizáció.* Nemzeti Közszolgálati Egyetem. 2015. - p. 71.

[9] Az e-közigazgatás hatékonyságát és a felkínált szolgáltatások igénybevételének társadalmi hajlandóságát abban az értelemben is vizsgálni szükséges, hogy az egyes generációk milyen formában képesek alkalmazni az e-közigazgatás elengedhetetlen összetevőit a technikai eszközöket. További kihívásként kell rögzíteni azt a tényt, hogy a digitális eszközökre vonatkozó portfólió csak az elmúlt 10 évben indult rohamos fejlődésnek, amely eredményeként vált a tömegek számára megfizethetővé.

és szolgáltatásnyújtás szempontjából. Ilyen például a *pályázatkezelés*, az *adózás*, a *dokumentumkezelés*, a *közlekedés*, a *közigazgatás* és a *mezőgazdaság* is, ahol megfigyelhető a beépülő innováció és a digitális átalakulás eredményei. Kijelenthető, hogy a magyar kormány elképzelése jövőorientált gondolkodás felé halad, mely olyan informatikai megoldások szerepét helyezi előtérbe, melyek kulcsszerepet játszhatnak a gazdasági és kormányzati struktúra megvalósításában és hatékonyságának fejlesztésében. Az újfajta megvalósítások új üzleti lehetőségeket is biztosítanak a vállalatok számára, továbbá egyszerűsített és hatékonyabb ellenőrzést az állami hatóságok számára. A továbbiakban bemutatásra kerülnek olyan hatékony és sikeres megvalósítások melyek elősegítik a társadalom produktív működését.

Elsőként vegyük alapul az adózás intézményét, melyben óriási előrelépés figyelhető meg az elektronikus ügyintézés területén. Évekkel ezelőtt, mint az intézményi, mind az ügyfél oldal súlyos problémákat okozott. A nagy mennyiségű papíralapú dokumentumok gyakran szülnek fennakadást az intézmények működésében. A túl bonyolult adminisztráció további problémákat okozott a vállalkozások és a magánszemélyek számára egyaránt. Ezzel szemben az elektronikus dokumentumkezelés segít a gyorsabb és könnyebb adóbevallásban is. Ezzel egyidejűleg az adminisztrációs költségek jelentősen csökkenése is megfigyelhető. Az elektronikus adatbázisok nagy előnye a nyomtatott dokumentációval szemben, hogy *integrált regisztereket* lehet létrehozni, amelyek segítségével az ellenőrzések gyorsabbakká és hatékonyabbakká vállhatnak. Mindezek mellett fejlett belső és külső adatközlő funkciókat lehet megvalósítani, amelyek segítségével elemzések végezhetők az egyes szinteken, ez által eredményként az egyes folyamatok egyszerűsítése érhető el.

Az állam következő lépése az elektronikus ügyintézés alkalmazása terén az online pénztárgépek bevezetése volt. 2012-ben a magyar kormány kulcsfontosságúnak tekintette a nemzet gazdaságának a kifehérítését. Ennek érdekében 2012-ben döntés született az online pénztárgépek rendszerének bevezetéséről. A jogalkotási rendelkezés értelmében 2014 szeptemberétől Magyarországon csak online pénztárgépek használhatók. Ezek a pénztárgépek napi 24 órában csatlakoznak a Nemzeti Adó- és Vámhivatal szervereihez, és előre meghatározott időközönként egy biztonsági rendszeren keresztül küldik el a gép üzemeltetésével kapcsolatos adatokat. Az új gépek bevezetésével a kormányzat célja az államháztartási bevételeket növelésének és stabilitásának a megteremtése volt. Az új technológia már képes részletesebb adatok tárolására, az adott napon kiadott számlák könnyen lekérhetők a rendszerből, továbbá folyamatosan figyelemmel kísérhető a készpénzforgalom. A rendszer működése során keletkező adatok segítik az adóellenőrök hatósági munkáját,

valamint szakmai iránymutatást adnak, arra vonatkozóan, hogy mely szervezeteket szükséges hatósági ellenőrizés alá vonni.[10]

Az állami szolgáltatói modell kialakítása érdekében jelentős változások figyelhetők meg 2010-től. Több, az állam és az önkormányzatok által nyújtott szolgáltatáshoz kapcsolódó intézményrendszer (pl.: *szociális terület, oktatásügy, művelődésügy*) jelentős átalakításon esett át annak érdekében, hogy hatékonyabb feladatellátás valósulhasson meg. A hatékonyabb feladatellátást az adott ágazathoz kapcsolódó állami és az önkormányzati feladatok, hatáskörök felülvizsgálata és újraelosztása jelentette. Általánosságban elmondható, hogy az érintett ágazatok esetében erősödött az állam koordinációs és irányító szerepe.[11] A fejlesztési irányvonalak megértéséhez elengedhetetlen az e-közigazgatás elméleti kérdésinek a bemutatása.

2. Az e-közigazgatás általános elmélete és kialakulása

2.1. Az e-kormányzat

Az e-kormányzat fogalmát sokan nehezen értelmezik, egyesek szerint megjelenése csak problémát szül, mások szerint pedig olyan szerepet tölt be, mint a 18. században lezajló ipari forradalmak. Ahhoz, hogy megfelelő kontextusban tudjuk értelmezni az e-kormányzat fogalmát, segítségül kell hívnunk az egyes társ- és határtudományokat. Ezen körbe tartozik a *szervezés- vezetéstudomány,* az *informatika* és a *közigazgatás-tudomány*.[12] A *szervezés- és vezetéstudomány,* mint a szervezés- tudományok csoportjainak olyan alapvető diszciplinája, melynek feladata a vonatkozó ismeretek és tapasztalatok gyűjtése, továbbá a módszertani fejlesztéshez, a gyakorlati tevékenység tökéletesítéséhez szükséges feltételek megteremtése.[13] Az *informatika* már úgynevezett differens tudomány. Különféle halmazok együttesét értjük ez alatt. Ilyen halmaz például az információ, a kód, az adat és számítógép is, hiszen az

[10] Innovation in public administration – an operating e-state. 13 outstandingly useful public IT solutions in Hungary. Nemzeti Hírközlési és Informatikai Tanács. 2015.

[11] Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia. 2014-2020. *Az állami szolgáltatói modell kialakítása*. – p. 15.

[12] Budai Balázs – Tózsa István: *Az e-közigazgatás elmélete*. Debreceni Egyetem, Agrár- és Műszaki Tudományok Centruma. 2007. – pp 8-10.

[13] Horváth István: *Közigazgatási szervezés- és vezetéstan*. Dialog Campus Kiadó, Budapest-Pécs. 2002. – pp. 29-31.

informatikai információ megszerzésével, tárolásával, feldolgozásával és továbbításával foglalkozó tudomány. Minden információt kódokká alakít át és az informatika elengedhetetlen része a számítógép.[14] A *közigazgatástudomány* az államhatalom gyakorlását kézben tartó intézményeknek alárendelt állami tevékenység szervezetére és működésére vonatkozó szabályokat jelenti.[15] A bemutatott tudományterületek mindegyike egyformán stabil és nélkülözhetetlen manapság ugyanis, bármelyiket elhagyjuk, vagy teljes mértékben nélkülözzük a másik interdiszciplináris területre tévedünk. A *közigazgatás*, ezen fajtáját szolgáltató jellegű közigazgatásnak is nevezik, ugyanis a stratégiai célok egyike, hogy minél kényelmesebb és hatékonyabb rendszert hozzanak létre a társadalom számára. Ezen rendszer lényege, hogy az ügyfél igényét szem előtt tartva nyújtja a szolgáltatást. Ennek a struktúrának az eszenciája nem más, mint az *internet*, amely manapság igen populáris a társadalom számára.[16]

Az *e- közigazgatás* és *e- kormányzat* fogalmát Magyarországon szinonimaként értelmezik, mindazonáltal konkrét tartalmak nincsenek rögzítve a fogalmak mögé. Közös nevezőként elmondható, hogy mindkettő célja az ügyfélközpontúság, a közigazgatás szolgáltató jellegének erősítése, és a közigazgatási szolgáltatások további támogatása. Az egyik része egy szolgáltatói oldalból áll, melyet idegen szóval *back officnak* hívunk és áll egy ügyfél oldalból, amely a *front office-nak*. A szolgáltatói oldal törekszik arra, hogy struktúrája minél fejlettebb és folyamatosan megújuló legyen, míg az ügyfél oldal az ügykezdeményező szerepet látja el a rendszerben. Az ügyféloldal attribútuma, hogy interneten keresztül felveszi a korrelációt, a szolgáltatói oldal pedig befogadja a dokumentumokat, feldolgozza azokat, illetve végrehajtja az ügyintézési mechanizmusokat. A szolgáltatói oldal minél hatékonyabb és magasabb minőségű működéséhez, fontos a háttérintézmények centralizálása és a decentralizált szolgáltatói intézmények létrehozása. Ahhoz, hogy ez megvalósuljon, ki kell térni a szolgáltatói oldal egyes sarkalatos problémáira. Az e- közigazgatás bevezetésével, szükségessé váltak egyes szakterületek integrálása, amely segítségével a szakértelem dinamikájának a növekedése vált elérhetővé. Az ügyintézésből eredeztethető hibák csökkentésének középpontba helyezésével jelentős negatív tényező kikerült a rendszerből. A folyamat kezelése és a hatékonyság fenntartása nem mindig zökkenőmentes, azonban jelentős

[14] Papp István: *Az informatika fogalma*. In.: Tudományos és Műszaki Tájékoztatás (Könyvtár- és Információtudományi szakfolyóirat) 50. évfolyam, 9–10. szám. – p. 5.

[15] Bednay Dezső: *Közigazgatási alapfogalmak*. Jogi asszisztens tanfolyami jegyzet. 2011. – p. 8.

[16] Jenei György: *Közigazgatás-menedzsment*. Századvég, Budapest. 2005. – p. 20.

hatékonyságjavulás elkönyvelése esetén arányosan növekszik a szolgáltatások színvonala is. A decentralizáció szintén egy nehezebb lépése ennek a folyamatnak. Ezen lépésnél fontos, hogy az ügyfelek számára elérhetőek legyenek olyan ügyintézési formák, melyek nem igényelnek magas szintű tudást az ügyfél részéről. A rendszer kialakításánál törekedni kell a központi tudásmechanizmus fejlesztésére, hogy az ügyfelek minél egyszerűbb kezelő felületet kapjanak.[17]

Megállapítható, hogy egyre több pozitív tapasztalatok hatására, egyre többen veszik igénybe az elektronikus közigazgatás szolgáltatásait, ezáltal az állam is próbálja bővíteni a szolgáltatások tárházát. A fejlesztés első lépcsőjeként megújításra került az elektronikus ügyintézés jogszabályi környezete, felszámolásra került több, az állampolgárok, vállalkozások magasabb szintű kiszolgálását, és az informatikai megoldások széleskörű alkalmazását és így terjedését korábban gátló előírás is. Az új jogszabályi környezet új e-ügyintézési modellt határozott meg az állam által kötelezően nyújtandó szolgáltatások vonatkozásában. Ezek részei a korszerű e-ügyintézési szolgáltatási rendszer kialakításának. A fejlesztések megvalósítása során kiemelt hangsúlyt kell fektetni az azonosítás és biztonságos kézbesítés kérdéskörére is. Az egyes fejlesztési ciklusokat úgy kell meghatározni, hogy kiemelt figyelmet kapjanak azok a közigazgatási szakterületek is, amelyek kisebb ügyfélforgalmat bonyolítanak le, azonban a közigazgatási rendszer fontos részét képviselik. Pl.: rendészeti közigazgatás.

2.2. Az e-közigazgatás jogi környezete

Jelen tanulmányban fontos prioritás az e-közigazgatás jogszabályi megfeleltethetősége. Elsőként a legfontosabb jogszabályt érdemes megemlíteni, amely rögzíti az elektronikus ügyintézés általános szabályait. A *2004. évi CXL. törvény* a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól kimondja, hogy az eljárás minden szereplője a törvényben meghatározottak szerint jogosult, illetve köteles az eljárási cselekményeit - *így különösen nyilatkozatát, döntését* - elektronikusan teljesíteni, ha az az adott eljárási cselekmény vonatkozásában értelmezhető.[18]

[17] Simon Barbara – Budai Balázs: *Elektronikus-közigazgatási modernizáció*. Nemzeti Közszolgálati Egyetem, Budapest. 2015. - pp. 15-18.

[18] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól. In.: Magyar Közlöny. 2004. évi 203. szám. – pp. 16142-16191.

Ide kell sorolnunk a *2015. évi CCXXII. törvényt* amely, az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályira vonatkozóan fogalmaz meg szabályokat. A jogszabály az eljárásokat gyorsítása, az adminisztratív terhek csökkentése, továbbá a lakosság számára korszerűbb és hatékonyabb közszolgáltatásokat nyújtása érdekében került megalkotásra. A jogalkotó az elektronikus ügyintézés alapelveit, magát az elektronikus ügyintézés kötelezettségét, tiltását és módját, valamint az átjárhatóságok lehetőségeit a papír alapú ügyintézés körében, illetve a szolgáltatásokra vonatkozó *alapelveket* határozta meg.

A jogszabály értelmében az ügyfél az elektronikus ügyintézéshez szükséges nyilatkozatokat, eljárási cselekményeket és egyéb kötelezettségeket egy erre a célra létrehozott elektronikus felületen, illetve az ügyintézést biztosító szerv által meghatározottak szerint elektronikus úton végezheti, abba az esetben, ha a törvény eltérően nem rendelkezik. Az elektronikus ügyintézés során, az üggyel foglalkozó szerv köteles a beérkező elektronikus nyomtatványokat hiteles papír alapú másolatokká, vagy azt hiteles papír alapú irattá alakítani. Ezekben az esetekbe a bizonyító ereje megegyezik az eredeti papír alapú dokumentum bizonyító erejével, ha elektronikus ügyintézési szolgáltatás szabályai szerint készítették el.

Nem lehetséges elektronikus ügyintézés abban az esetben, ahol a törvény, eredeti jogalkotói hatáskörben megalkotott kormányrendelet az ügyfél személyes megjelenését vagy meghatározott okiratok másként nem pótolható benyújtását kötelezővé teszi. Illetve abban az esetben, ahol elektronikus ügyintézés nem értelmezhető, ahol ezt nemzetközi szerződés, vagy az Európai Unió általános hatályú, közvetlenül alkalmazandó kötelező jogi aktusa kizárja és ahol minősített adatokat tartalmazó információk közlése szükséges. Az ügyfél akkor jogosult elektronikus azonosítás nélkül elektronikus ügyintézésre, ha az adott eljárási vagy ügyintézési cselekmény elvégzése vagy nyilatkozat megtétele nem elektronikus ügyintézés esetén egyáltalán nem igényli személyazonosító adat megadását.[19]

Az elektronikus ügyintézés részletes szabályait a *451/2016. (XII. 19.) Kormányrendelet* határozza meg. A rendelet részletezi többek között az elektronikus *ügyintézés biztosításának feltételeit,* az elektronikus *kapcsolattartás* egyes módjaival kapcsolatos részletszabályokat, az elektronikus *azonosítási* kötelezettség részleteit, a *dokumentumhitelesítést* és számtalan olyan szabályzó anyagot, amely elengedhetetlen az elektronikus ügyintézés szabályszerűségéhez.[20]

---

[19] 2015. évi CCXXII. törvény az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályiról. Magyar Közlöny. 2015. évi, 202. szám. – pp. 26809-26859.

[20] Roóz József: *Vezetésmódszertan*. Perfekt Kiadó, Budapest. 2001. – pp. 11-12.

A tanulmány szempontjából relevánsabb információ, hogy mivel a kormány a rendőrséget a rendészetért felelős miniszter útján irányítja, ezáltal a 2004. évi CXL. törvény alapján lehetőség nyílik a rendőrség hatáskörébe tartozó egyes közigazgatási hatósági ügyek elindítását elektronikus úton, az Ügyfélkapu Közigazgatási Portálon keresztül kezdeményezni. Azonban a rendőrség vonatkozásából vizsgálva a kérdéskört láthatjuk, hogy nem egyszerű az elektronikus ügyintézés részleges, vagy teljes ügymenetre vonatkozó folyamatának a lebonyolítása, mivel csak olyan ügy intézhető elektronikusan, amely nem igényli az ügyfél személyes megjelenését. Továbbá az ügyintézés során benyújtandó elektronikus formanyomtatványok a rendőrség internetes felületen érhetők el, melyeket kizárólag az Általános nyomtatványkitöltő program segítségével tölthető ki, amely a www.nav.gov.hu internetes portálon keresztül érhető el és telepíthető.[21]

Az e-közigazgatás jogi környezete hatékony alapot nyújt a közigazgatási modellben megfogalmazott célok eléréséhez és a feladatok teljesítéséhez. Az átlátható *intézményi struktúra*, a korszerű és ügyfélbarát *eljárásrend*, és a szakmailag felkészült *személyi állomány* segítségével elérhető a szolgáltató államra vonatkozó kormányzati elvárások. A jogi keretek finom hangolása elengedhetetlenné válik, abban az esetben, amennyiben a közigazgatás szervezetrendszerének korszerűsítése során további változások és változtatások szükségszerűsége elkerülhetetlenné válik a problémás területek kezelése érdekében.[22]

2.3. Információkezelés, adatbiztonság – adatvédelem

Az e-közigazgatás szakterületének komplex fejlesztéséhez elengedhetetlen az ügyintézést támogató informatikai háttér fejlesztése. Ezzel összefüggésben elsődleges prioritást élvez az *adatvédelem* és *adatbiztonság* kérdésköre. Az adatvédelem nem más, mint a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. Ezzel szemben az adatbiztonság az adatok jogosulatlan megszerzése, módosítása és megsemmisítése elleni műszaki és szervezési megoldások rendszere.[23] Az adatvédelem szabályozása a jogalkotó

---

[21] Elektronikus ügyintézés. (http://www.police.hu/hu/ugyintezes/elektronikus-ugyintezes letöltés ideje: 2017. 09.25.)

[22] Ilyen problémás területek a jogi keretek folyamatos változtatása, az átláthatóság és a stabilitás hiánya, a területi igazgatás túlzott széttagoltsága, a túl nagy adminisztrációs terhek, az ügyintézés alacsony minősége, valamint a szakmai hiányosságok növekedése.

[23] *Adatvédelmi értelmező szótár*. Nemzeti Adatvédelmi és Információszabadság Hatóság. (https://www.naih.hu/adatvedelmi-szotar.html letöltés ideje: 2017.10.12.)

többoldalról szabályozza. Fontos kiemelni a személyes adatok védelméhez való jogot, amely,, hozzáférésének, kezelésének kivételessége alapjogi védelemben részesül.[24] E jogot és ennek általános szabályait az információs önrendelkezési jogról és az információszabadságról szóló *2011. évi CXII. törvény* tartalmazza.[25] Azonban érdemes említést tenni a mára hatályon kívül helyezett e törvény elődjéről az 1992.évi LXIII. törvényről, amely rögzítette a személyes adatok védelmének általános szabályait. Mint azt már említett a szabályozás többrétegű, ugyanis nem csak a fent említett törvény szabályoz. Az Alaptörvény VI. cikke kimondja hogy, mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák. Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez. A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi."[26] Fontos említést tenni az Európai Unió Alapjogi Chartájáról is, amelynek 8. cikke rögzít, e témához tartozó lényeges megállapításokat. Ennek értelmében, mindenkinek joga van a rá vonatkozó adatok védelméhez, illetve hogy, mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíthatni.[27] Az adatvédelemmel szemben itt csak egy jogszabályt szükséges megemlíteni. A 2011. évi CXII. törvény támasztja alá az adatbiztonság védelmének követelményét. E törvény 7. szakasza rögzíti mindezeket: Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. (2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. (3) Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés,

---

[24] Tóth Judit: *A személyes adatok védelme és a közérdekű adatok nyilvánossága*. Szegedi Tudományegyetem, Állam- és Jogtudományi Kar. Szeged, 2012. – pp. 1-2.

[25] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Magyar Közlöny. 2011. évi 88. szám. – pp. 25449-25486.

[26] Magyarország Alaptörvénye. Magyar Közlöny. (egységes szerkezetben) VI. cikk. 2013. évi, 55. szám. - p. 14590.

[27] *Az Európai Unió Alapjogi Chartája*. (2012/C 326/02) Az Európai Unió Hivatalos Lapja. (http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12012P/TXT&from=HU letöltés ideje: 2017.09.26.)

valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.[28]

Az adatvédelem és adatbiztonság mellett, nem szabad megfeledkeznünk az *információkezelésről* vagy *adatkezelésről* szükségességéről sem. Az adatkezelés fogalmát szintén az információs önrendelkezési jogról és az információszabadságról szóló törvény rögzíti amely szerint az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése."[29]

A következőkben kiemelésre kerül néhány a törvényben rögzített adatkezelésre vonatkozó szabály:

- Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul,
- Az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie,
- Csak olyan adat kezelhető, amely az adatkezelés során elengedhetetlen,
- Az adott adat a meghatározott cél elérésére alkalmasnak kell lennie,
- Adatkezelő a helyreállításhoz szükséges technikai feltételekkel rendelkezzen,
- Adatok pontosságának, helyességének biztosítása.[30]

Az adatvédelemmel és az adatbiztonsággal összefüggő joganyagok rávilágítanak arra a tényre, hogy az információk biztonságos kezelése és elérhetősége milyen lényeges részét képezi az e-közigazgatás belső működésének. Az informatikai fejlesztések során figyelemmel kell lenni nem csak a társadalmi igényekre, hanem a közigazgatásban dolgozó személyek elvárásaira is a rendszer működésével kapcsolatban. A hatékony működés

---

[28] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (7.§(1)- (3) bekezdés)

[29] u.o. (3.§(10). bekezdés)

[30] *A személyes adatok védelme*. A személyes adatok védelme és a magánélet tiszteletben tartása fontos alapvető jogok. Az Európai Parlament mindig hangsúlyozza, hogy egyensúlyt kell találni a biztonság fokozása és az emberi jogok – köztük az adatvédelem és a magánélet védelme – között. Az uniós adatvédelmi reform meg fogja erősíteni a polgárok jogait, lehetővé téve számukra adataik jobb ellenőrzését, illetve biztosítva, hogy magánéletük a digitális korban is védelem alatt áll. Az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikke. Az Európai Unió Alapjogi Chartájának 7. és 8. cikke.

érdekében biztosítani kell az országos illetékességekhez történő ügyintézői (vezetői- és ellenőrzési jogkörrel rendelkező személyek számára is) hozzáféréseket, valamint a jelenleg széttagolt rendszer egységes rendszerbe történő integrálását, továbbá az átfogó monitorozás biztosítását.[31]

2.4. E-ügyfél, e-kártya, elektronikus regisztráció és azonosítás

A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény 2011-es módosításával vált lehetővé az elektronikus ügyintézés teljes körű alkalmazása az elektronikus azonosítás alkalmazásával. Az elektronikus ügyintézés az ügyfélkapu rendszer segítségével, egy személyi azonosítást követően történik. A regisztráció az elektronikus aláírással nem rendelkező ügyfelek kellő biztonságú kapcsolattartását biztosítja. A regisztrációt a központi elektronikus szolgáltató rendszer látja el, az ügyfélkapu segítségével. Az ügyfélkapu a kormányzati portál központi rendszerének az a logikai pontja, amelyen keresztül a személyazonosítást (*viszontazonosítást*) igénylő elektronikus szolgáltatás az azonosított ügyfél által elérhető.[32] Az ügyfélkapu biztosítja a személy számára, hogy kapcsolatba lépjen a szolgáltató szervvel, mindezt a személyazonossága igazolása mellett. Az Ügyfélkapu létesítését bármely természetes személy kezdeményezheti személyesen a regisztrációs szervnél, vagy elektronikusan, amennyiben 2016. január 1-jét követően kiállított érvényes személyazonosító igazolvánnyal rendelkezik. A regisztrációhoz meg kell adnia szabadon választott egyedi felhasználói nevét és elektronikus levélcímét (e-mail cím), mivel erre a címre kapja meg az első belépéshez szükséges egyszer használatos kódját.[33] A személyes ügyfélkapu regisztrációt három féleképpen tehetjük meg. Egyik módja a személyes megjelenés a regisztrációs szerv előtt, a második az online regisztráció elektronikus aláírással, a harmadik pedig az ideiglenes online regisztráció elektronikus aláírás nélkül. A regisztrációt

[31] Példaként megemlíthető a rendőrség igazgatásrendészeti szolgálati ágának tevékenységi körébe tartozó egyes rendészeti feladatok iratkezelésére vonatkozó problémákat. Akár a fegyverrendészetet, akár a személy- és vagyonvédelmi szakterület ügyintézései során keletkezett dokumentumokat vesszük figyelembe, probléma, hogy az iratkezelést csak rendőrkapitányságí szinten látják és más hatóság, vagy társ-szerv nem tud keresni, vagy ellenőrzést végrehajtani a dokumentumok vonatkozásában.

[32] A központi elektronikus szolgáltató rendszerről szóló 182/2007. (VII. 10.) Kormányrendelet, 2. §, v) pont.

[33] Ügyfélkapu. (https://ugyfelkapu.magyarorszag.hu/ letöltés ideje: 2017.09. 28.)

követően az ügyfél e-mailben egy öt évig érvényes kódot kap, melyet az első belépést követően meg is változtathat.[34]

2015. január 1-jén lépett hatályba az egyablakos ügyintézés lehetősége. Ez az ügyintézési forma számos európai államban bevezetésre került az elmúlt években. Célja, hogy az állampolgárok, minél egyszerűbben és hatékonyabban intézhessék ügyeiket. Lényege, hogy olyan ügyintézések esetében, amely több hatóság közreműködését igényli, anélkül továbbítják az ügy iratait, hogy az ügyfélnek személyesen közre kellene működnie.[35]

Az egyablakos ügyintézés mellett létrehozták az úgynevezett hivatali kaput, amely szintén a szolgáltató szervek közötti dokumentumáramlást szolgálja. A központi elektronikus szolgáltató rendszerről szóló rendelet értelmében a központi elektronikus szolgáltató rendszernek az a logikai pontja, amelyen keresztül a csatlakozott szervezet hozzáfér a központi rendszer által részére nyújtott szolgáltatásokhoz és információkhoz.[36] Az Európai Unió is felismerte az elektronikus azonosítás fontosságát, hatályon kívül helyezte a korábbi, csak az elektronikus aláírásra vonatkozó irányelvét, és az új, rendeleti szinten elfogadott szabályozás már kiterjed az elektronikus azonosításra is. Ennek értelmében kiemelt célként kell kezelni, hogy az állampolgárok minél nagyobb hányadban rendelkezzenek az elektronikus térben történő azonosításra és az elektronikus aláírás létrehozására alkalmas eszközökkel. Az államnak ösztönözni kell az állampolgárokat, hogy az ügyintézések jelentős száma az elektronikus térben kerüljön végrehajtásra. Ennek a célnak az elérése érdekében az államnak be kell avatkoznia, hogy biztosítsa az állampolgárok, a cégek és az egyéb szervezetek, közintézmények számára az elektronikus azonosításra, fizetésre és kapcsolattartásra vonatkozó képességeket.

---

[34] E-tananyag. Ügyfélkapu. (https://segitseg.magyarorszag.hu/etananyag/ugyfelkapu_etananyag.html letöltés ideje: 2017.09. 28.)

[35] Mire jó az egyablakos ügyintézés. (http://kormanyablak.reblog.hu/miert-jo-az-egyablakos-ugyintezes letöltés ideje: 2017.09. 28.)

[36] A központi elektronikus szolgáltató rendszerről szóló 182/2007. (VII. 10.) Kormányrendelet, 2.§, i) pont.

3. Az e-közigazgatás nemzetközi viszonylatban

3.1. Az E-kormányzás az EU-ban (hatékonyságtól a szolgáltató államig)[37]

Az e-közigazgatás szolgáltatási és ügyintézési rendszerének kibővítése és fejlesztése kiemelkedő prioritással bír az Európai Unió szakmai célstratégiájában. Ennek jelentős eredményei mutatkoznak meg a fejlődő infrastruktúrák kiépítésben, mely számos tagországban megfigyelhető. Ezen fejlődések ellenére fontos megjegyezni, hogy a közigazgatás elektronikus úton történő ügyintézése még a legfejlettebb országokban is korai szakaszát éli, mondhatni kezdeti stádiumban áll.[38]

3.1.1. Fejlesztési trendek nemzetközi viszonylatban

Az Európai Unió felismerte, hogy elengedhetetlen a közigazgatási rendszerek korszerűsítése, illetve azt is, hogy ezen korszerűsítési törekvések elmaradása komoly nemzetgazdasági hátrányokat is okozhatnak. Ez a felismerés vezetett az Európai Unióban végbemenő fejlesztésekhez.

1994: *Bangemann-jelentés*. Stratégiai javaslat az Információs társadalom megvalósítására.[39] A jelentés alapját az e-Government cselekvési tervekben megfogalmazott célok adták, amely értelmében azt a célt próbálták elérni, hogy minden állampolgár kapcsolódjon be az információs társadalomba.

A kiemelt célok között szerepel a már korábban prioritásként kezelt közszolgálati információk elérésének biztosítása, információszabadság és elektronikus átláthatóság. Az európai közösségi szintű közigazgatási szolgáltatások kialakítása érdekében stratégiai célként határozták meg a tagállami szabályozási környezetek harmonizálását is.

A cselekvési terv a legfontosabb feladatok közé emelte az általánosnak mondható célkitűzések (*hozzáférés, közérdekű adatok és e-közszolgáltatások elérése*) mellett a nyílt

[37] Frigyesi Veronika – Dedinszky Ferenc: *Az E-kormányzás az Európai Unióban és Magyarországon.* In.: E-világ. 2004. évi, 4. szám. – pp. 25-27.

[38] Tózsa István: *Az e-közigazgatás Európában – Jelen és jövő.* In.: Vezetéstudomány. 2011. évi, 3. szám. – p. 14.

[39] 2000: e-Europe. 2002: eEurope+. 2006 – i2010.

forráskódú szoftverek és az elektronikus aláírás használatának a közszférában történő támogatását.[40]

Az e-Europe 2005 akcióterv az alábbi célterületeket emelte ki:

- a közigazgatási szervek szélessávú hálózati összeköttetése;
- nyílt forráskódú szoftvereken alapuló megoldások;
- az alapvető közigazgatási szolgáltatások interaktívak és mindenki számára hozzáférhetők legyenek;
- elektronikus közbeszerzési szabályozás megalkotása és gyakorlati megvalósítása;
- nyilvános, közösségi Internet-hozzáférés biztosítása;
- a közadatok elérését lehetővé tevő szolgáltatások indítása és ennek szabályozása.

A 2006-ban elfogadott i2010 e-Government cselekvési terv fő célkitűzései.[41]

1. társadalmi csoportok integrációjának felgyorsítása az elektronikus kormányzaton keresztül;
2. magas felhasználói elégedettség, átláthatóság, elszámoltathatóság, az adminisztratív terhek csökkentése;
3. nagy jelentőségű alapszolgáltatások (például közbeszerzés) elektronikus elérése és lebonyolítása;
4. a közszolgáltatásokhoz történő biztonságos, interoperábilis, hitelesített hozzáférés 2010-re egész Európában;
5. részvétel és a demokratikus döntéshozatal erősítése.

Kiemelt célok:

- felhasználók bevonása az interaktív elektronikus közszolgáltatások rendszerébe
- a közszféra adatvagyonának további felhasználása, akár üzleti céllal is;
- a közigazgatási átláthatóságának javítása;
- akadálymentes közigazgatási szolgáltatások vállalkozások számára;

[40] Juhász Lilla: *E-közigazgatás Európában: fókuszban a közigazgatás racionalizálása és az állampolgár.* In.: E-közigazgatás. 2007. évi, 1. szám. – pp. 18-20.

[41] Molnár Szilárd (kutatásvezető): *Elektronikus közigazgatás. Éves jelentés 2006.* BME-UNESCO Információs Társadalom és Trendkutató Központ. Budapest, 2007. – pp. 10-13.

- határok nélküli közigazgatási szolgáltatások, egységes európai közigazgatási tér;
- hatékonyságnövelés, ügyfelek adminisztratív terheinek csökkentése.
- Elektronikus személyazonosítási (eID)[42] technológiák fejlesztése és széles körű alkalmazása. Cél a tagállami elektronikus személyazonosítási megoldások kölcsönös elismerését lehetővé tevő európai szintű megoldás kialakítása.
- Elektronikus hitelesítés, biztonságos dokumentumkezelés.

A Digitális Menetrend e-közigazgatással kapcsolatos célkitűzései között szerepel, hogy 2015-ig az uniós lakosság 50 %-a vegyen igénybe e-kormányzati szolgáltatásokat. További kiemelt cél, hogy 2015-ig legyenek online hozzáférhetők olyan határokon átnyúló alapvető közszolgáltatások, amelyek lehetővé teszik, hogy a vállalkozók származási helyüktől függetlenül Európa bármely országában vállalkozást hozhassanak létre és üzemeltethessenek, illetve bármely uniós polgár bármely európai uniós tagállamban tanulhasson, munkát vállalhasson, lakhasson és nyugdíjba vonulhasson.

3.1.2. A szolgáltatások elérhetősége az EU-ban (USA kitekintéssel)[43]

Az Európai Unió Tanácsa nagymértékben támogatja az e-közigazgatás kialakítását és fejlesztését. Az Információs Társadalom- és Média Főigazgatóság (*Information Society and Media Directorate-General*) és az Informatikai Főigazgatóság (*Directorate-General for Informatics*) több programon keresztül segítette és napjainkban is segíti ennek a célnak az elérését. Ezek közül a két legjelentősebb kezdeményezései voltak az európai e-kormányzati szolgáltatások átjárható átadása a közigazgatásoknak, vállalkozásoknak és állampolgároknak" (*Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*) (2005-2009 között) és az annak folytatásaként megvalósuló Interoperabilitási megoldások az európai közigazgatás számára. (*Interoperability Solutions for European Public Administrations*) A jelenlegi elektronikus kormányzati cselekvési terv az Európai Unió Tanácsa által 2010-ben elfogadott Európa 2020 stratégia (az EU foglalkoztatási

---

[42] Nyáry Mihály (szerk.): *Komoly biztonsági hiba (sebezhetőség) 750 ezer észtországi digitális személyiben.* (http://hirlevel.egov.hu/tag/eid/ letöltés ideje: 2017.09.23.) A tanulmány kifejti, hogy az EiD-k bevezetésének kockázataival és bevezetésük feltételeivel összefüggésben 2015-ben 750 ezer darab EiD kártyánál állapított meg komoly adatvédelmi hiányosságot. Ezt a hiányosságot 2014 októberétől kibocsátott kártyák esetében észlelték Észtországban.

[43] *Az e-közigazgatás szolgáltatásai és használata az Európai Unióban*. In.: Statisztikai Tükör. IV. évf. 134. szám. Központi Statisztikai Hivatal. 2010.

és növekedési stratégiája) részét képezi.[44] A tagállamokon túl az Európai Unió Tanácsának e-kormányzati törekvései és tevékenységei részben a tagjelölt államokra is kiterjednek (pl. Törökország)

Az e-közigazgatás on-line elérhetőségének megoszlása az uniós országokra átlagosan 74% volt 2009-be. A vizsgált országok közül Magyarország a 19. helyet foglalta el 63%-os online elérhetőséggel. 2007-es teljesítmény alapján 17. helyen volt azonban a százalékos megoszlásban csupán 50% volt.[45] Ezzel ellentétben az osztrák, a máltai, a portugál és a brit online közigazgatás közel *egésze* elérhető a vállalkozások és állampolgárok számára. Ezeket az országokat követi Svédország, és Szlovénia ahol az említett e-közigazgatás 95%-ban hozzáférhető és alkalmazható.

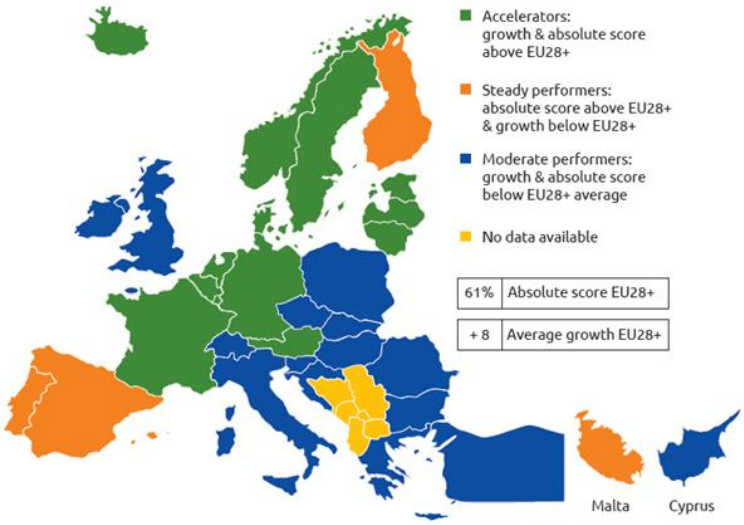
Az Európai Unió azon erőfeszítései melyek a tudásalapú információs társadalomra irányulnak már a kezdetektől magukba foglalták a közigazgatási szolgáltatások elektronikus hozzáférhetőségének szükségességét. Az online közszolgáltatások egyre inkább hozzáférhetők Európa szerte, azonban ez a fejlődés közel sem egyenletes, és az EU tagállamok között még mindig számottevő lemaradás figyelhető meg. A felhasználó központúság, az átláthatóság, valamint a határokon átnyúló mobilitás igénye sürgető az online közigazgatás kiépítésére melyet a magánszektor, és az állampolgárok igényei hajtanak.

Ezen kihívások kezelésének érdekében az Európai Bizottság új e-kormányzati terv kiépítését szorgalmazta a 2016 és 2020 közötti időszakban.

---

[44] Shailendra C. Jain Palvia & Sushil S. Sharma: *E-Government and E-Governance: Definitions/Domain Framework and Status around the World.* Computer Society of India. (http://csi-sigegov.orgwww.csi-sigegov.org/1/1_369.pdf letöltés ideje: 2017.10.13.)

[45] *A közigazgatás fejlesztése*. (http://vallalkozas.netenahivatal.gov.hu/miert-jo-az-e-kozigazgatas/a-kozigazgatas-fejlesztese letöltés ideje: 2017.08.08.) A tanulmány kifejti, hogy a kormány a közigazgatás átalakítása során alapvetően két szempontot tart szem előtt: az egyik a *hatékonyság*, a másik a közigazgatással kapcsolatba kerülő állampolgárok és vállalkozások életének *egyszerűbbé* tétele.



Az E-kormányzati szolgáltatások jelenlegi hozzáférhetősége és annak fejlődése[46]

Uniós jogszabályok, törvények, rendeletek

Az e-közigazgatási jogszabályi háttereknek első sorban az Európai Uniós jogszabályozásoknak kell megfelelniük, így a jogszabályi piramis tetején is ezen szabályozások helyezkednek el.

Uniós jogszabályok

- Az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről.

- COM(2010) 245 — Európai digitális menetrend.[47]

- COM (2006) 173 — i2010 eGovernment cselekvési terv - Az elektronikus kormányzat létrehozásának felgyorsítása a társadalom egészének javára.[48]

Az Európai Parlament és a Tanács 2003/98/EK Irányelve a közszféra információinak további felhasználásáról.

- Az Európai Parlament és a Tanács 95/46/EK irányelve (Adatvédelmi Irányelv)[49]

---

[46] *Jelmagyarázat*: *zöld*: gyorsulva fejlődők és a fejlődés, valamint az abszolút pontszám is az EU28+ felett található. *Narancs*: stabilan teljesítők, növekedés az EU28+ alatt és abszolút pontszám az EU28+ felett található. *Kék*: közepesen teljesítők, növekedés és abszolút pontszám is az EU 28+ alatt található. *Sárga*: nincs adat; forrás: https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly, 2017.09.22.)

[47] *Az európai digitális menetrend.* A bizottság közleménye az európai parlamentnek, a tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának. Brüsszel, 2010.05.19. COM (2010) 245. végleges.

[48] *i2010 eGovernment cselekvési terv: az elektronikus kormányzat létrehozásának felgyorsítása a társadalom egészének javára.* A bizottság közleménye a tanácsnak, az európai parlamentnek, az európai gazdasági és szociális bizottságnak és a régiók bizottságának. Brüsszel, 2006.04.25. COM (2006) 173. végleges.

Az Európai Bizottság az adminisztratív terhek csökkentése érdekében 2007-ben elfogadta azt a cselekvési tervet, amely a lakosság adminisztrációs ügyintézésével összefüggésben, valamint a jogszabályok nyelvezetének közérthetőbbé tétele érdekében fogalmazta meg álláspontját. Az intézkedések hatékonysága, valamint a tagállami jogalkotás elősegítése érdekében egy többlépcsős jogalkotási folyamat vette kezdetét. Az irányelvek eredményeképpen a kormány kiemelt ügyként kezelte a hatósági ügyintézés átláthatóságát és egyszerűsítését. Ennek érdekében a hazai törvényalkotás egy hatékony szabályozási és jogalkotási folyamat során megerősítette a közigazgatást (ezen belül az online szervezett és folytatott közigazgatást) és annak szolgáltatásait, figyelemmel az uniós szabályozásokra. Megfigyelhető, hogy a jogalkotó figyelembe vette a hazai közigazgatás sajátosságait is, és ezt a megközelítést alkalmazta a joganyagok megalkotása és minőségének javítása során.

Törvények

- Magyarország Alaptörvénye.[50]

- 2009. évi CLV. törvény A minősített adat védelméről.[51]

- 2010. évi CLVII. törvény A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.[52]

- 1995. évi LXVI. törvény A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről.

- 2001. évi XXXV. törvény Az elektronikus aláírásról.

Kormányrendeletek

- 78/2010. (III.25.) Korm. rendelet Az elektronikus aláírás közigazgatási használatához kapcsoló követelményekről, és az elektronikus kapcsolattartás egyes szabályairól.[53]
- 160/2010 (V. 6.) Korm. rendelet Az integrált ügyintézési és tájékoztatási pont kialakításáról, működtetéséről, valamint a működtető és az érintett szervek együttműködésének rendjéről.[54]

---

[49] *Az Európai Parlament és a Tanács 95/46/EK irányelve*. Hivatalos Lap L 281, 23/11/1995 o. 0031 – 0050.

[50] *Magyarország Alaptörvénye*. Magyar Közlöny. (egységes szerkezetben) VI. cikk. 2013. évi 55. szám.

[51] *2009. évi CLV. törvény A minősített adat védelméről*. Magyar Közlöny. 2009. évi 194. szám. – pp. 47843-47866.

[52] 2010. évi CLVII. törvény A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről. Magyar Közlöny. 2010. évi 196. szám. – pp. 29840-29844.

[53] 78/2010. (III.25.) Korm. rendelet Az elektronikus aláírás közigazgatási használatához kapcsoló követelményekről, és az elektronikus kapcsolattartás egyes szabályairól. Magyar Közlöny. 2010. évi 43. szám. – pp. 11798-11804.

[54] 160/2010 (V. 6.) Korm. rendelet Az integrált ügyintézési és tájékoztatási pont kialakításáról, működtetéséről, valamint a működtető és az érintett szervek együttműködésének rendjéről. Magyar Közlöny. 2010. évi 69. szám. – pp. 14546-14560.

- 82/2012. (IV. 21.) Korm. rendelet A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény elektronikus ügyintézéssel kapcsolatos kormányrendeleteinek módosításáról.[55]
- 83/2012. (IV. 21.) Korm. rendelet A szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról. (SZEÜSZ)
- 84/2012. (IV. 21.) Korm. rendelet Az egyes e-ügyintézéshez kapcsolódó szervezetek kijelöléséről (KEK KH, NISZ, Magyar Posta).
- 85/2012. (IV. 21.) Korm. rendelet az E-ügyintézés részletes szabályairól.
- 212/2010 (VII.1) Korm. rendelet Az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről.[56]
- A 160/2010. (V.6.) Korm. rendelet Az integrált ügyintézési és tájékoztatási pont kialakításáról, működtetéséről, valamint a működtető és az érintett szervek együttműködési rendjéről.
- 335/2005. (XII. 29.) Korm. rendelet A közfeladatot ellátó szervek iratkezelésének általános követelményeiről.

Miniszteri rendeletek és utasítások

- 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet A közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről.
- 16/2006. (IV. 6.) BM rendelet A közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverek megfelelőségét tanúsító szervezetek kijelölésének részletes szabályairól.
- 3/2005. (III. 18.) IHM rendelet Az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 114/2007. (XII. 29.) GKM rendelet A digitális archiválás szabályairól E-közigazgatási alapismeretek E-learning tananyag közszolgálati dolgozók számára.
- 13/2005. (X. 27.) IHM rendelet A papíralapú dokumentumról elektronikus úton történő másolat készítésének szabályairól.
- 17/2010. (VIII. 31.) KIM utasítás A Közigazgatási és Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról.

Az e-közigazgatás hazai és Európai uniós jogi környezetének és keretszabályozásának vizsgálat alapvetően fontos. A jog irányítja az ügyletek szabályosságát, hivatkozhatóságát és

[55] 82/2012. (IV. 21.) Korm. rendelet A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény elektronikus ügyintézéssel kapcsolatos kormányrendeleteinek módosításáról. Magyar Közlöny. 2012. évi 48. szám. – pp. 8439-8448.

[56] 212/2010 (VII.1) Korm. rendelet Az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről. Magyar Közlöny. 2010. évi 111. szám. – pp. 21695-21754.

kiszámíthatóságát.[57] Az elektronikus közigazgatás vizsgálatával összefüggésben még számos kérdés nem került tisztázásra. A kutatások kiindulási alapként tekintenek a hazai és a nemzetközi joganyagokra és gyakorlati rendszerekre. Bemutatásra és rendszerezésre kerültek az elektronikus közigazgatás joganyagai, amelyek segítségével egy átfogó képet kapunk a további irányvonalak (jogalkotási, strukturális, igazgatásszervezési, szakpolitikai) kijelölése vonatkozásában. A kutatásunk szempontjából releváns célkitűzés, hogy egyes Európai Uniós tagállamok e-közigazgatási modelljeinek vizsgálatával bizonyításra kerüljenek a felvázolt hipotézisek.[58]

4. Az e- közigazgatás jelenlegi szerepe a rendőrségi struktúrában

4.1. Nemzetközi kitekintés

4.1.1. A lengyel modell[59]

Az e-közigazgatás és az e-policing felhasználásáról Ziemba és Oblak 2014-ben folytatott kutatásokat Lengyelországban. A kutatás eredményeit bemutató tanulmányban a szerzők kifejtik, hogy az e-közigazgatás kialakításához szükséges információs rendszerek számos előnnyel járnak, amelyek elsősorban a polgárok számára nyújtott kormányzati szolgáltatások minőségét javítják. Lengyelországban a közigazgatási rendszer központi és lokális szintekre tagolódnak. Az e-közigazgatás információs rendszereinek kialakítása szempontjából egyrészt a közigazgatás felépítése, másrészt a gazdasági és szociológiai háttér (*példaként az internetet használók aránya Lengyelországban, 2013-as adatok alapján 62 %, az urbanizáció mértéke 2013-as adatok alapján 60,8 %*) meghatározók.

Ziemba és Oblak tanulmányának célja a lengyel közigazgatásban bevezetésre kerülő információs rendszerek (ezek közül is külön kiemelve az *Empa@tia* rendszert) leírása és kapacitásuk feltérképezése volt. Ennek során a bevezetésre kerülő információs rendszerek

[57] *E-közigazgatási szabályozás 2015*. Közigazgatási- és Igazságügyi Minisztérium. Budapest, 2013. – pp. 18-25.

[58] Zsom Brigitta: *Az elektronikus közigazgatás és a területi kutatások kapcsolatáról*. In.: Tér és Társadalom. 2014. évi 3. szám. – pp. 19-20. Egyetértek a szerző azon álláspontjával, hogy az elektronikus közigazgatás kutatása során kiemelt figyelmet kell fordítani a területi kutatásokra. Ezt kiegészíteném azzal, hogy a területi kutatásokat ki kell bővíteni a társadalomra vonatkozó egységes kutatásokkal, mivel ezeknek a kutatásoknak eredményei felhasználásával lehet a társadalmi igényeket figyelembe venni az elektronikus közigazgatás fejlesztése során.

[59] Ewa Ziemba & Iwona Obłąk: *The Survey of Information Systems in Public Administration in Poland*. In.: Interdisciplinary Journal of Information, Knowledge, and Management. 2014. évi 9. szám. – pp. 38-41.

listájának összeállítása, majd azok előnyeinek a projektekben való aktív részvételén keresztüli megfigyelését végezték a kutatók. A vizsgált Emp@tia rendszer célja többek között a hatékony interoperábilitás kialakítása a különböző társadalombiztosítási alrendszerek között, az interoperábilitás biztosítása a társadalombiztosítás területén kívül eső közigazgatási rendszerekkel, továbbá az elektronikus szolgáltatások nyújtása a kormányzati alkalmazottak és a társadalombiztosítási szolgáltatásokat igénylők számára.

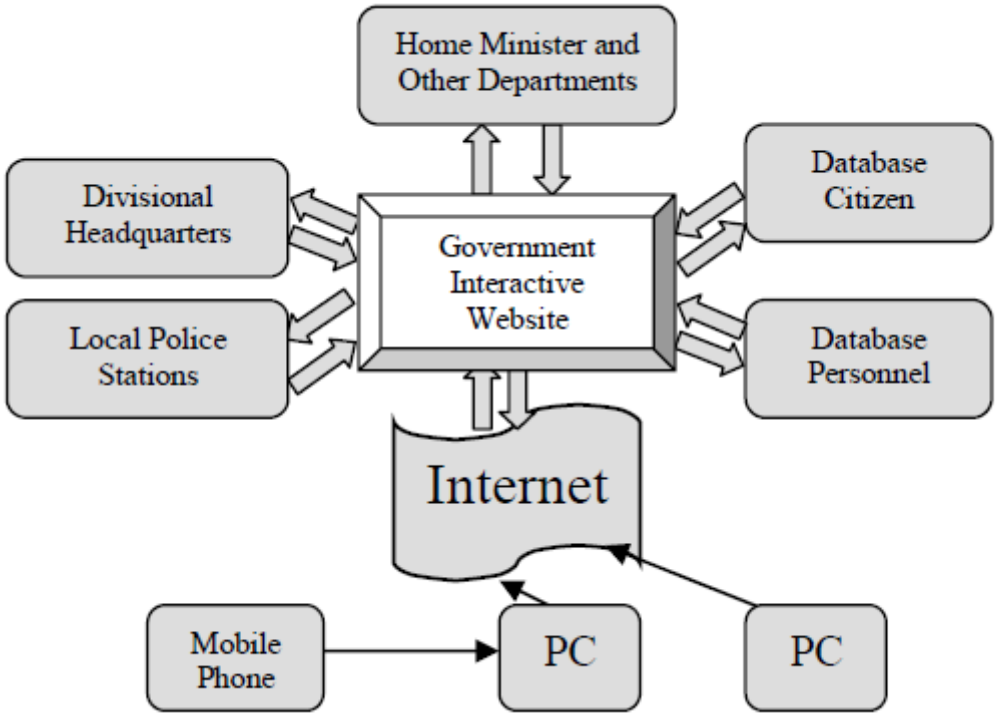
A kutatás megállapítja, hogy a különböző információs rendszerek nagyban növelik az információáramlás hatékonyságát a különböző közigazgatási szereplők között, mindazonáltal a szolgáltatások megfelelő minőségének biztosítása érdekében ezen információs rendszerek bevezetésekor figyelemmel kell lenni olyan alapvető elvárásokra, mint például, hogy az újonnan bevezetésre kerülő információs rendszerek interoperábilisak legyenek. Fontos tényező, hogy az információs rendszer a felhasználók számára könnyen kezelhető legyen, illetve, hogy a bevezetett információs rendszerek folyamatos karbantartása kiemelt figyelmet kapjon a folyamatos működés érdekében. A kutatás kiemeli, hogy számos olyan közigazgatási szakterület vonatkozásában nem készült átfogó kutatás az elektronikus közigazgatás rendszeréről, ahol az ügyfelek speciális környezetben és szervezeti struktúrában vesznek részt az ügyintézési eljárásban.

4.1.2. Digitális társadalom – digitális rendőrség

Egyes fejlett országokban (Amerikai Egyesült Államok, Kanada, Japán) az e-közigazgatás részeként az e-rendőrség fejlett információs technológiák alkalmazásával növeli a rendőri feladatok ellátásának hatékonyságát. Islam és munkatársai tanulmányukban a fejlődő országokban az e-rendőrség bevezetése és annak nemzetközi színvonalra emelése kapcsán felmerülő, megoldandó kihívásokkal kapcsolatban végeztek átfogó kutatásokat. Meglátásuk szerint az e-rendőrségi rendszer egyik előnye, hogy a rendőri munka során szükséges információ (élő kép is) elérhető és továbbítható akár az utcán feladatot ellátó rendőrök számára. Az e-rendőrség bizonyos adatbázisai (például körözött személyek adatai) a polgári lakosság számára is elérhetőek. Mindezen szolgáltatások a közrend és a közbiztonság növelését szolgálják és hatékonyan hozzájárulnak a rendőrségi közbizalom erősítéséhez.

Az e-rendőrségek hatékony működéséhez a következő tényezőket kell biztosítani. Az e-rendőrség felépítésében két különálló egység szerepel: egyfelől a helyi rendőrkapitányságok, börtönök és közlekedésirányító rendszerek állnak egymással összeköttetésben, másfelől pedig a nemzetbiztonságért felelős szolgálatok szerepe jelentős a

struktúrában, amelyek a rendőrkapitányságokon túl kormányzati adatbázisokkal is összeköttetésben állnak.



Az e-rendőrség rendszer blokkdiagramja (Forrás: Islam és Mtsai, 2014.)

Kiemelendő, hogy az egyes rendőrkapitányságok csak adatokat tudnak lekérni, de nem tudnak változtatásokat eszközölni a központi adatbázisokban. A hatékony működés érdekében a rendőrök munkáját intelligens szoftverek segítik, olyan módon, hogy a rendőri munka során beérkező adatok elemzésével a gyanúsítottak korábbi adatainak gyorsabb elérését biztosítják. Az e-rendőrségnek rendelkeznie kell olyan, az állampolgárok számára könnyen kezelhető, szabadon hozzáférhető webes felülettel, ahol bejelentéseket tehetnek a rendőrség felé, továbbá ezen felületen keresztül bírságok kifizetése is lehetségessé válik.

Az e-rendőrségek kialakítása több előnnyel jár a fejlődő országok számára. Jellemzően a fejlődő országokban a lakosság számához viszonyítva a rendőrök száma kisebb. Ez a probléma az e-rendőrségi rendszer a rendőri munka részleges megkönnyítésén keresztül a közbiztonság javulásához vezethet. Az e-rendőrség rendszer továbbá megkönnyíti a rendőri munka standardizációját is, amely alapvető fontosságú a több ország rendőrségének bevonásával járó nemzetközi bűnüldözési feladatok ellátásához is.

Az e-kormányzat fejlődése számos korábban megfogalmazott releváns kérdésre választ adhat számunkra. A közigazgatási rendszer átalakítása során figyelemmel kell lenni a kialakult kihívásokra és kockázatokra. Erősíteni szükséges a háttérbe szorult szervezeti

képességeket, amelyek a közigazgatási rendszer gyenge pontjait képezik. A rendőrség e-közigazgatási tevékenysége, valamint az e-rendőrség rendszere a következő lépések egyike a közigazgatás fejlesztése során. Az elektronikus közigazgatás eme két alrendszerének a fejlesztésével nemcsak a közbiztonság erősítése érhető el, hanem a rendőrség feladatrendszeréhez tartozó közigazgatási eljárások hatékonysága és gyorsítása érhető el. Olyan a rendőrséggel kapcsolatos szervezeti kihívás is hatékonyan kezelhetővé válhat az e-rendőrség fejlesztésével, mint a rendőrségi korrupció. Számos nemzetközi kutatás rávilágított arra, hogy az állampolgárok közbizalma a rendőrség irányában erősíthető, amennyiben az adott kormányzat az e-kormányzati struktúra fejlesztése során kiemelt figyelmet szentel az e-rendőrség fejlesztésére.[60]

Jelen kutatás a lefektetett hipotézisek mentén folytatott feltáró jellegű reprezentatív kutatásokat az állampolgárok körében. A kutatási eredmények felhasználásával a rendőrség minden szolgálati ágára kiterjedően folytattunk fókuszcsoportos beszélgetéseket, hogy milyen *ütemben,* milyen *rendszerben*, és milyen *struktúrában* lehet és szükséges-e a rendőrség e-közigazgatási rendszerének a fejlesztése és erősítése a kor rendészeti kihívásai kezelése érdekében.

5. Kutatás (leíró statisztika)

5.1. Demográfiai adatok

A megkérdezettek neme

Kérdőívünket viszonylag egyenlő arányban töltötték ki férfiak (42%) és nők (58%) egyaránt. Ez az arány a kutatásunk elemzéséhez meglehetősen előnyös, hiszen nem torzulnak el az adatok az erősen nemfüggő véleményektől. Ezen kívül a kérdőíves kutatást megelőző fókuszcsoportos interjúnk férfi-női aránya is hasonlóképp alakult, így ezen kettő összevetése stabil alapokon nyugszik.

A megkérdezettek betöltött éveinek száma

Ahhoz, hogy kérdőívünk kitöltőinek korát meg tudjuk vizsgálni, négy korosztályba soroltuk be őket. Ahogyan a diagramból is látható, a kitöltések száma a kor növekedésével

[60] Kazi I. Reasul: *E-Police System for Improved E-Government Services of Developing Countries*. In.: Conference: 25tth IEEE Canadian Conference on Electrical and Computer Engineering, At Montreal, Quebec. 2014. – pp. 2-4.

párhuzamosan, viszonylag egyenletesen csökkent. Legtöbb kitöltés a 19-22 éves korosztályból érkezett. A legidősebb kitöltő betöltötte a 63. életévét. A 23-33 évesek és a 33-40 évesek részvétele is erőteljes volt, így elmondhatjuk, hogy kérdőívünket főként a fiatal- és középkorú osztályok képviselői töltötték ki. Az átlagos életkor 32,8 év volt.

A megkérdezettek legmagasabb befejezett iskolai végzettsége

Kérdőívünk kitöltői mintegy 30 százaléka felsőfokú végzettséggel rendelkezik. Őket a gimnáziumot végzettek csoportja követi 24,7%-kal, illetve a szakközépiskola/szakiskola szintén ilyen arányú. Érdemes belegondolnunk, hogy a diploma vagy érettségi megléte/meg nem léte mennyiben befolyásolhatja az elektronikus ügyintézési szokásokat. Minden bizonnyal előítélet lenne azt állítani, hogy egy egyetemet végzett ember sokkal tájékozottabb és sokkal nyitottabb az elektronikus közigazgatás iránt, mint egy érettségivel sem rendelkező. Ha ez így is van, valójában mindegyik csoport véleményét figyelembe kell vennünk, hiszen az egész magyar társadalomra vetítve így tudunk csak releváns következtetéseket levonni.

A megkérdezettek foglalkozása

A válaszadók a legkülönbözőbb foglalkozási ágakhoz tartoznak, beleértve a biztonságot/honvédelmet, adminisztrációt, kereskedelmet, turizmust, az állami szektort, vagy épp az oktatás/tudományt, illetve a pénzügy/könyvelést, hogy csak a legfontosabbakat említsük. De kitöltötték a kérdőívet munkanélküliek is. A spektrum valóban széles. Ez is kellőképpen prezentálja, az kutatásban felmerült kérdéskör a társadalmi osztályokon és munkakörökön, foglalkozásokon átívelő, attól teljesen független.

5.2. A kérdőív kérdéseinek elemzése

5.2.1. Bevezető kérdések

A megkérdezettek jelentős többsége használ rendszeresen számítógépet, naponta többször internetezik és legfőképpen az otthonában vagy kisebb arányban a munkahelyén.

Internet előfizetéssel mindenki rendelkezik a háztartásában, vagy a kitöltő vagy a családjából egy másik személy által. Néhány kivételtől eltekintve pedig rendelkeznek asztali számítógéppel.

A megkérdezettek lakóhelyének településtípusa hipotézisek elemzésénél kiemelt hangsúlyt kap, így a kérdést abban a fejezetben tárgyaljuk.

Rendelkezik ön ügyfélkapus regisztrációval?

A kitöltők 79,4%-a rendelkezik ügyfélkapus regisztrációval. Ez a kérdés szintén kiemelt az egyik felmerült hipotézis problémakörében, így később visszatérünk rá.

Ismer –e olyan közigazgatási honlapokat amelyeken elektronikus úton tud ügyet intézni?

Az előző kérdéstől magasabb arányban (86,6%) ismernek olyan közigazgatási honlapokat a válaszadók, ahol elektronikusan tudnak ügyet intézni. Ezek után természetesen kértük, hogy soroljanak fel párat ezekből a weboldalakból, melyre a következő eredmények születtek. Pl.: *Ügyfélkapu, NAV, KSH, e-bank, ENKSZ, Magyar Államkincstár, Abev, Takarnet, Nemzeti Mobilfizetési Rendszer, EPER, MÁK, nyugdíj és postai szolgáltatások ügyintézése*.

Ismeri Ön az elektronikus közigazgatás (e-közigazgatás, e-kormányzat) fogalmakat?

Meglepőnek tűnhet, de a kitöltők alig 60 százaléka ismeri ezeket a fogalmakat. Az első legfontosabb probléma talán innen indul, hogy az emberek általában elutasítják, amit nem ismernek. És ezek szerint használnak bizonyos elektronikus közigazgatási rendszereket (mert esetleg rákényszerültek), de alapvetően nincsenek tisztában azzal, mit is értünk pontosan ezen a fogalmak alatt, és mik lehetnének a kínálkozó lehetőségek.

Pontosan ezért a következő „Ön mennyire tartja fontosnak az elektronikus közigazgatás megvalósulását, s ennek részeként a lakossági ügyintézés elektronikus útra terelését?” továbbá

az „Összességében mennyire tartja vonzónak saját maga számára az interneten keresztüli ügyintézés lehetőségét?” c. kérdésköröket alaposabban is körbejárjuk egy másik fejezetben.

A közigazgatásban az e-ügyintézés melyik formáját használta már?

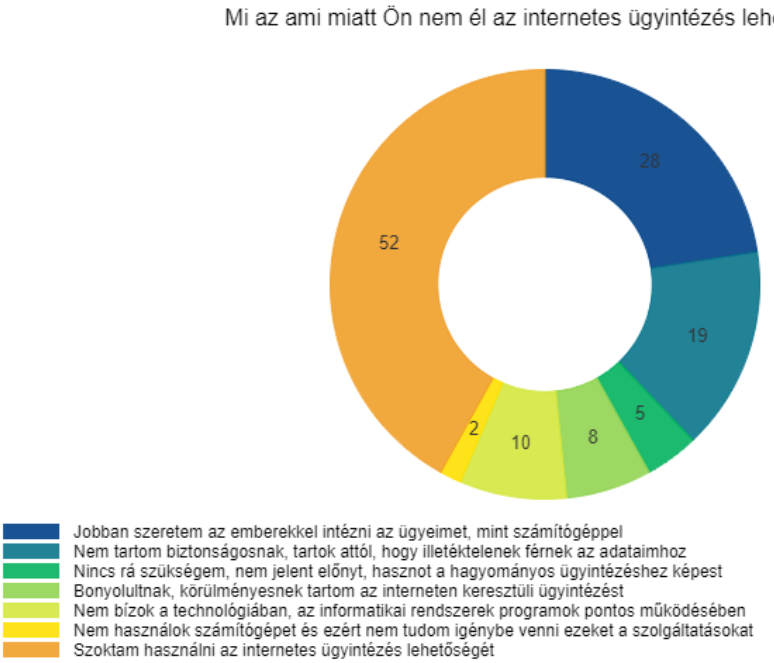
A kérdésnél egyszerre több választ is megjelölhettek, így az eloszlás kiegyensúlyozottabban alakult. A kérdőív feldolgozásakor erre a pontra érve már nem ért váratlanul minket, hogy a kitöltők 31,5%-a jelölte meg, hogy az ügyélkapu segítségével használ e-szolgáltatásokat. Kicsivel kevesebb, mint a válaszadók ötöde (18,8%) foglalt már időpontot okmányirodába és 9,6% már indított is ott ügyet, és körülbelül tizede (11,7%) csak informálódik. Többen kérnek információt e-mailben (9,1%) vagy ügyleírásokat olvasnak (8,1%). A kitöltői válaszok megoszlását tekintve 7,1% mondta azt, hogy nem használ e-szolgáltatásokat, tehát összesen közel 93 százalék az elektronikus közigazgatás valamely ágát, mégha nincs is tisztában azok fogalmával, használja. Sajnos kevés a teljes ügymenetet bonyolítók aránya, csupán 4,1%, ezt az űrt hivatottak betölteni, az erre vonatkozó kezdeményezések, melyre a kutatásunk is irányul.

Ha teljes ügyintézést bonyolított már le elektronikusan akkor, kérem adja meg, hogy milyen típusú ügyet intézett?

Megkértük a kitöltőket, hogy nevezzék meg ezeket a weboldalakat, amelyre a következő válaszok születtek: *Európai Betegbiztosítás Kártya ügyintézése, adóbevallás, hatósági erkölcsi bizonyítvány, állami pályázat benyújtása, tulajdoni lap lekérése, felsőoktatási jelentkezés, diák igazolvány igénylése, hitel igénylés.*

Mi az, ami miatt Ön nem él az internetes ügyintézés lehetőségével?

Itt szintén egyszerre több választ lehetett megjelölni. A legfontosabb leszögezni, hogy 41,9% szokott használni valamilyen formájú internetes ügyintézést (ez nem feltétlenül közigazgatási ügyeket jelent), hanem akár a banki elektronikus felületektől a telekommunikációs oldalakon át változatos spektrumon mozoghatnak. Aki azt mondja, hogy nem él ezzel a lehetőséggel, legtöbben a személyes, emberi kontaktus hiányát jelölték meg, 22,6 százalékban. A válaszadók egyhatoda bizalmatlan, a személyes adatainak védelmét nem látja biztosítottnak, és kisebb arányban vannak, akik nem bízok magában a technológiában, az informatikai rendszerek programok pontos működésében (8,1%). A legelenyészőbb válaszok a személyes attitűdökből adódtak. A kitöltők 6,5%-a tartja bonyolultnak vagy körülményesnek az internetes ügyintézést és 4% mondta azt, hogy semmilyen előnyt nem jelent számára.



Amennyiben otthon nem rendelkezik számítógéppel, internetkapcsolattal vagy felhasználói ismeretekkel, az elektronikus közigazgatás elterjedése késztetné Önt ezek beszerzésére?

A kérdést meg kell különböztetni a korábban tárgyalt technikai eszközök, illetve az internetkapcsolat meglétének kérdésétől a válaszadók otthonában, ugyanis itt a felhasználói ismeretek hiánya is szerepet játszik. A megkérdezettek 14,4% mondta azt, hogy késztetné az e-közigazgatás elterjedése ezek beszerzésére, 11,3% viszont abszolút nemmel válaszolt. A túlnyomó többség (74,2%) viszont rendelkezik a kérdéses kompetenciákkal, vagy azok valamelyikével. Az alábbiakban következő eldöntendő kérdéseket, melyek a rendőrségi elektronikus ügyintézés témakörét járják körül részletesen is elemezni fogjuk a hipotézisek vizsgálatánál, így most csak egy pár szóban említjük.

Amennyiben erre lehetőség nyílna intézné a rendőrségi ügyeket elektronikusan? (ügyintézés, feljelentés, bejelentés, tájékoztatás kérés stb.).

A kitöltők 70,1%-a állna pozitívan a jövőbeli elektronikus ügyintézés lehetőségéhez, ami rendkívül jónak mondható, mindösszesen csak 29,9 százaléka elutasító.

Tájékozódna ön a rendőrség honlapján ügyfélfogadási időről vagy ügyintézési módokról? (információnyújtás elektronikusan)

Az elektronikus rendőrségi tájékoztatásnak kivételesen magas a támogatottsága, amennyiben erre lehetőség nyílna (92,7%).

Töltene ön le elektronikusan rendőrségi ügyintézéshez szükséges nyomtatványokat? (egyirányú kapcsolat) Pl.: személy- és vagyonvédelem, fegyverügyintézés.

A válaszadók 84,5%-a élne az egyirányú kapcsolat lehetőségével, melyből egyértelműen tükröződik az igény erre a lehetőségre.

Töltene ön ki a rendőrség honlapján megtalálható online módon kitölthető űrlapokat (beleértve a hitelesítést), amennyiben az illeték befizetésére nincs lehetőség és az egyszeri személyes megjelenés továbbra is szükséges a hatósági ügyintézés lefolytatásához? (interaktivitás)

A kérdés támogatottsága 69,1%-os, ez egy kissé elmarad a rendőrségi közigazgatási rendszer információs lehetőségeinek kihasználásától, de ez az online ügyintézéstől vett általános bizalmatlanságot figyelembe véve megfelelő. Az interaktivitásba vetett bizalom növelésére szükség van a későbbiekben.

Igénybe venné ön a rendőrségi ügyintézés során a teljesen elektronikus ügymenet lehetőségét, beleértve az illeték lerovását is? (tranzakció)

Az online módon kitölthető kérdőívekhez hasonlóan a az illeték lerovással kiegészített, tranzakcióra vonatkozó kérdésre 68,0%-ban válaszoltak igennel a megkérdezettek.

Amennyiben az adott kormányszervnek (rendőrség) rendelkezésére állnának más adminisztratív forrásból az ön (ügyintézéshez szükséges) adatai, abban az esetben ön hozzájárulna, hogy azokat előzetesen feltüntessék egy személyre szabott űrlapban a hatósági ügyintézés megindításakor az ön személyes ügyintézési felületén? (perszonalizáció)

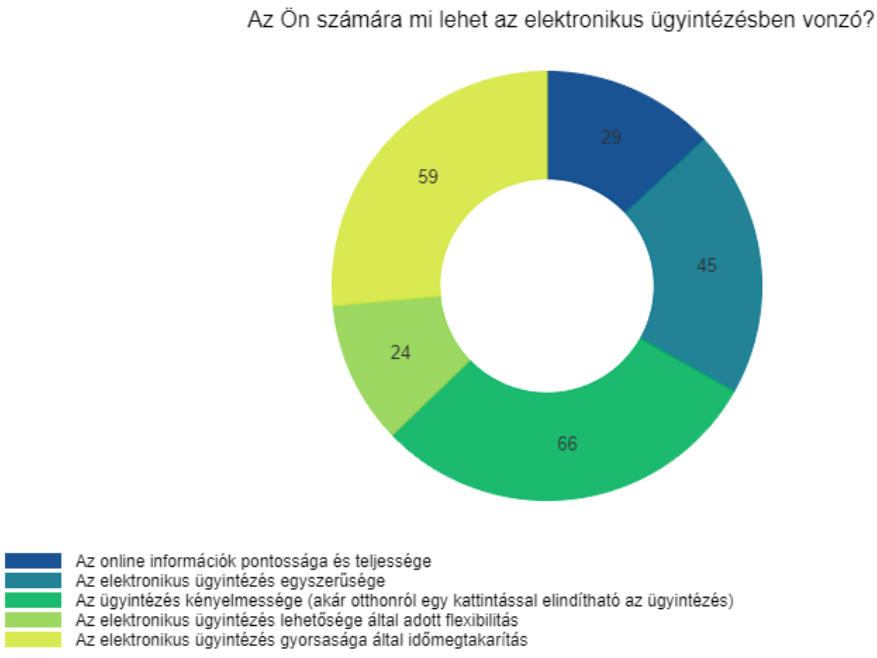
A személyre szabott űrlap a kérdések között a legalacsonyabb pozitivitást ért el, igaz a 60,8% közel sem mondható kevésnek. A mögötte meghúzódó okokat tüzetesebben is próbáljuk megvizsgálni a későbbiekben.

Az Ön számára mi lehet az elektronikus ügyintézésben vonzó?

Ennél a pontnál ismét több válasz megadására volt lehetőség. Az e-ügyintézés legvonzóbb tulajdonsága a felmérésünk szerint a kényelmessége (29%). Sokunk nem szereti a

sorban állást, a várakozási időt, időpontokat, hivatali bürokráciarendszert, vagy csak egyszerűen azt az ügyintézőt, akivel esetleg nehezebben értünk szót. Valóban komfortosabb a saját magánszféránkból pár kattintással elintézni a kötelező feladatokat. Ez a típusú ügyintézés valóban egy olyan újítása a modern, felgyorsult világunknak, mely léptékekkel megkönnyíti az azt kihasználó személyek életét. A vélemények 26,5%-a ebben a csoportban található. Az egyszerűsége mellett (is) párolók 20,2%-ot képviselnek. Ha megfelelően van felépítve az adott weboldal, ahol az információk strukturáltan és logikusan megtalálhatók, könnyedén eligazodnak rajta a felhasználók. Kevesebben tették le a voksukat (13,0%) az online információk pontossága és teljessége mellett. Ez adódhat abból, hogy a meglévő e-ügyintézési felületeken (közigazgatási ágtól függetlenül) találkoztak a felhasználók hiányosságokkal, vagy csak egyszerűen a válaszadó számára fontosabb volt megemlíteni például a kényelmességet, mint az információk teljességét.

Az elektronikus ügyintézés által élvezhető flexibilitás végzett az utolsó helyen (10,8%). Ami csak azért meglepő, mert ez az aspektus szorosan összekapcsolódik a kényelmességgel és az időmegtakarítással. Hiszen gondoljunk csak bele, mennyire sokat számít, hogy nincs szükség területileg elkülönült helyeken ügyeket intézni. Itt nem feltétlenül kell városokat áthidaló nagyságrendekben gondolkoznunk, inkább csak egyik hivataltól a másikig, vagy egy-egy szolgáltató cég közötti utazás, nyitva tartás, ügyfélfogadási rend és mindezekkel járó kényelmetlenség. Az otthonról végezhető ügyintézés hatalmas fokú rugalmasságot biztosít számunkra, csak lehet ebbe néha bele sem gondolunk.



5.3. Társadalmi kutatás

A kérdőíves kutatás során nem valószínűségi mintavételi eljárások közül az *önkényes mintavételi* mód került alkalmazásra. Mivel ez a módszer nem reprezentatív, ezért feltáró jellegű kutatásoknál alkalmazható a felvázolt hipotézisek megalapozása érdekében.

A lakóhely szerint megosztott válaszok értelmezéséhez mindenek előtt célszerű megvizsgálni a magyarországi lakónépesség településtípusok szerinti összetételét és változását.

A településtípusok közül a főváros, a megyei jogú városok és a községi jogállású települések természetes fogyását enyhíteni tudta a bevándorlási többlet. A városokban a népességhez viszonyítva a természetes fogyás és a bevándorlási többlet is mérsékeltebb volt, közülük a megyeszékhelyeken a természetes fogyás mellett a negatív vándorlási különbözet is csökkentette a lakónépességet.[61]

1. ábra A lakónépesség változásának tényezői, 2011

Településtípus	Természetes szaporodás (+), illetve fogyás (–)	Vándorlási különbözet, egyéb változás (+,–)	Lakónépesség, 2011		
	2001 és 2011 között, fő		fő	a 2001. évi százalékában	fő/km²
Főváros	–74 823	25 942	1 729 040	97,3	3 292,6
Megyeszékhelyek	–44 426	–12 086	1 761 657	96,9	535,9
Többi megyei jogú város	–7 695	5 881	267 736	99,3	291,5
Többi város	–106 666	48 187	3 145 425	98,2	130,9
Városok összesen	–233 610	67 924	6 903 858	97,7	240,0
Községek, nagyközségek	–153 595	58 594	3 033 770	97,0	47,2
Ország összesen	**–387 205**	**126 518**	**9 937 628**	**97,4**	**106,8**

Forrás:
2011. ÉVI NÉPSZÁMLÁLÁS 3. Országos adatok
Központi Statisztikai Hivatal, 2013.

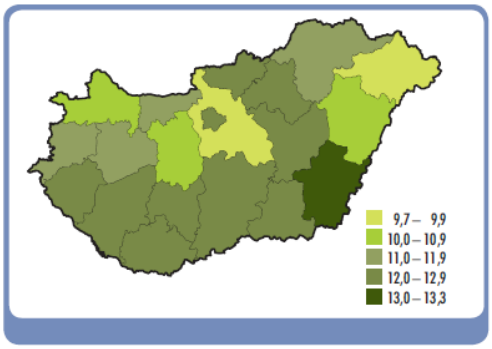
Az időskorúak közül különösen nagy mértékben növekedett a 60–69 éves korosztály létszáma. Az ország lakosságából minden tizedik lakos 70 éves vagy idősebb.

A megyék közül a növekvő népességű Pest megyén kívül Szabolcs-Szatmár-Bereg és Borsod-Abaúj-Zemplén megyében magas a gyermekkorúak aránya. Az időskorúak

[61] *2011. évi népszámlálás 3.* Országos adatok. Központi Statisztikai Hivatal, 2013. – p. 11.

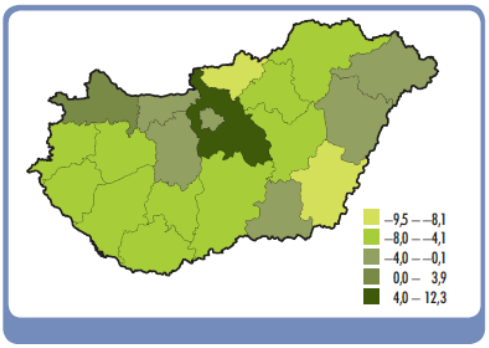
legnagyobb arányban Békés, Heves, Nógrád és Zala megyékben vannak jelen, ezekben a megyékben minden negyedik lakos 60 éves vagy idősebb.

2. ábra A 70 évesek és idősebbek aránya, 2011 (%)



Forrás:
2011. ÉVI NÉPSZÁMLÁLÁS 3. Országos adatok
Központi Statisztikai Hivatal, 2013

3. ábra A lakónépesség változása 2001. február 1. és 2011. október 1. között (%)



Forrás:
2011. ÉVI NÉPSZÁMLÁLÁS 3. Országos adatok
Központi Statisztikai Hivatal, 2013

A régiók közül egyedül Közép-Magyarország, valamint Győr-Moson-Sopron megye népessége növekedett kisebb mértékben.

Budapest viszonylatában a természetes fogyása mellett kismértékű vándorlási nyereséggel zárta az évtizedet. Az egyenleg egymással ellentétes folyamatok eredőjeként alakult ki: a – főként az agglomerációba történő – kivándorlás folytatódása mellett a visszavándorlási folyamat is elkezdődött, és megmaradt a főváros vonzóereje az ország többi megyéjével szemben is.

Összességében az elmúlt évtizedben a – *nem túl intenzív, évente a lakosság mintegy 4–5 százalékát érintő* – lakó- és tartózkodásihely-változtatások következtében a népesség az ország középső részére koncentrálódott, kisebb mértékben pedig a nyugati területekre.[62]

Az össznépességi megoszlási adatokkal összehasonlítva a válaszadók megoszlásában is érzékelhetők a fentiekben leírt tendenciák. A fővárosban nagy létszámmal élő aktív korú népesség magasabb arányban szerepel a mintánkban, ugyanakkor az egyéb városokban élők és a községek, nagyközségek lakossága

[62] *2011. évi népszámlálás 3.* Országos adatok. Központi Statisztikai Hivatal. 2013. – pp. 10-12.

megközelítőleg azonos mértéket reprezentál. Statisztikai szempontból az egyik legegyszerűbb kétváltozós elemzés a kereszttábla vizsgálat. Két vagy több változó közötti összefüggést vizsgál, illetve ezek kombinált gyakorisági eloszlását. A kérdőíves kutatás során rendelkezésre álló adatok elemzéséhez azért került kiválasztásra a kétváltozós elemzés, hogy a hipotézisek bizonyítása megfelelő tudományos alapossággal kerüljön kifejtésre.

5.4. Hipotézisek elemzése és bizonyítása

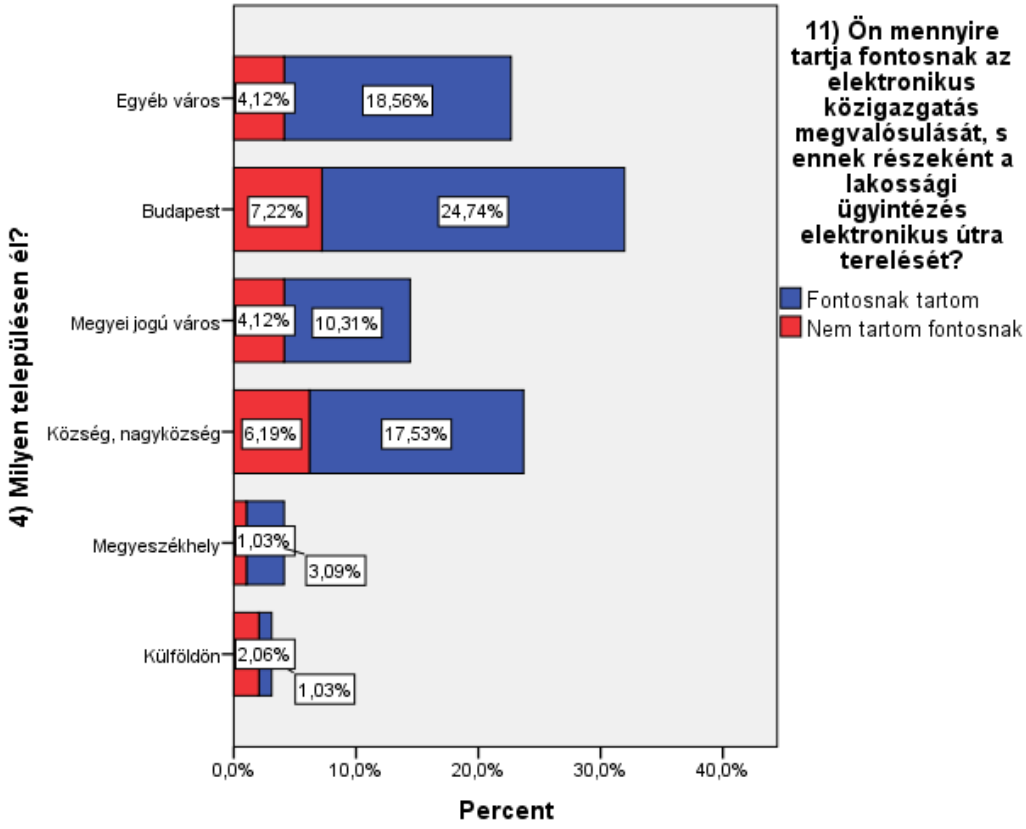
1. ***A magyar állampolgárok igénylik (ezáltal szükségesnek tartják) az e-közigazgatás feladatrendszeréhez tartozó szolgáltatások kibővítését és fejlesztését az egyes speciális szakterületek (úgy mint a rendőrség) vonatkozásában is.***

A hipotézisben a vizsgálatunk tárgyát a válaszadó személyek lakóhelye és az e-közigazgatás feladatrendszeréhez tartozó szolgáltatások közötti összefüggések képezik. A vizsgálat során először általánosságban, majd a speciálisabb rendőrségi kérdéskörök felé haladva került lefolytatásra az elemzés.

A megoszlások értelmezésének könnyítéseként rendelkezésünkre állnak grafikai eszközök, melyek közül jelenleg a *hisztogram* került alkalmazásra.[63]

[63] A hisztogram metrikusan skálázott tulajdonságok grafikus ábrázolása. Ha túl sok érték szerepel, akkor osztályokba vonják össze őket. Az egyes osztályok szélessége változhat. A mennyiségeket a szorosan egymás mellé rajzolt téglalapok jelölik, ahol az egyes téglalapok területe az adott osztály gyakoriságát mutatja. In.: Larry Wasserman: *All of Nonparametric Statistics.* Springer Kiadó. 2005. – p. 127.

4. ábra Az elektronikus közigazgatás megvalósulásának fontossága a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



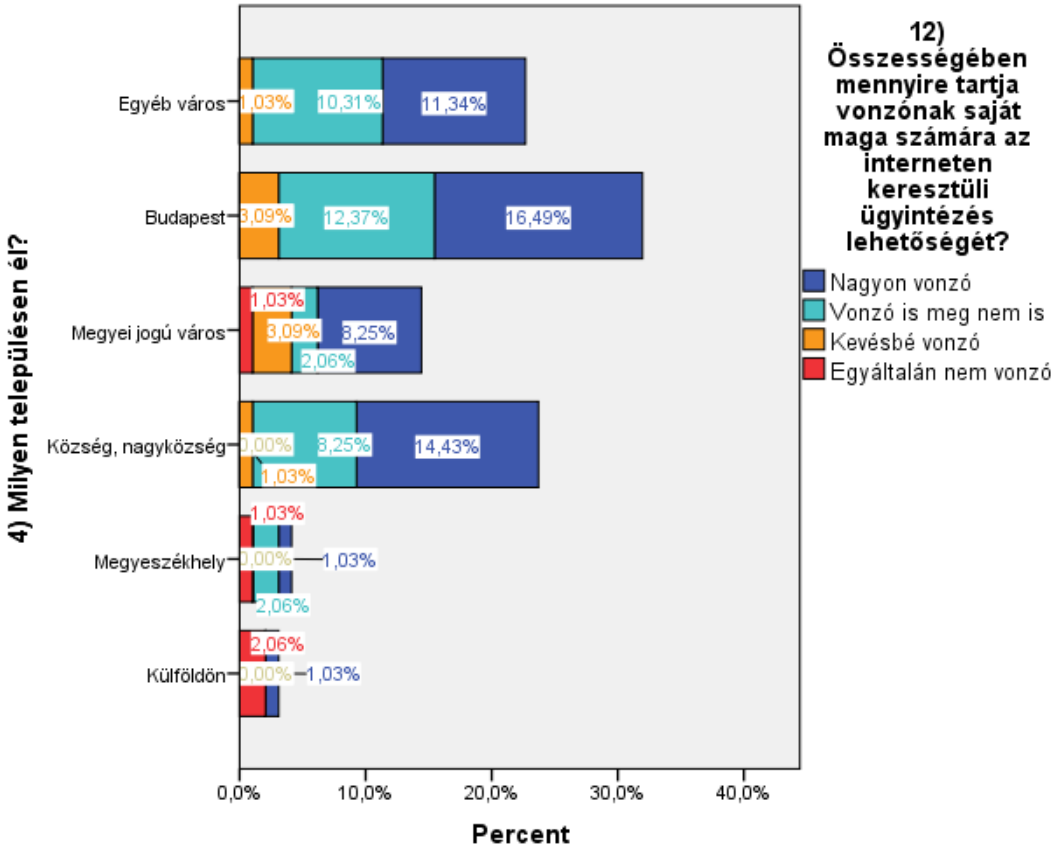
Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Az elektronikus közigazgatás megvalósulásának és további fejlesztésének a kérdését fontosnak tartók összesített aránya a megkérdezettek körében településtől függetlenül 75,26%. Az elemzett mintában az elektronikus közigazgatás megvalósulását elsősorban Budapesten (24,74%), az egyéb városokban (18,56%) és a községekben, nagyközségekben (17,53%) tartják fontosnak, ez együttesen a megkérdezettek 60,83%-át jelenti, ugyanezen településtípusokon, aki számára nem fontos az adott kérdés összesen 17,53%-ot eredményeznek.

Hozzá kell tenni, hogy az érdeklődés hiánya a teljes mintához képest legnagyobb arányban szintén a fővárosban figyelhető meg (7,22%), és csak az adott településcsoportot figyelembe véve mindösszesen ez a vélemények 22,59%-a. A külföldön élő magyar állampolgárok a teljes mintánkban csak 3,09%-ot képviselnek, viszont az ő fontossági véleményük fordítottan arányos a teljes mintánk vonatkozásában.

Az előzőkkel szoros összefüggésben vizsgálat alá került a válaszadók részéről a pozitív hozzáállás az interneten keresztül történő ügyintézés lehetőségéhez.

5. ábra Az internetes ügyintézés lehetőségének attraktivitása a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

A megkérdezettek több, mint fele (52,57%) egyértelműen vonzónak tartja; ha ehhez hozzávesszük a skála következő, többé-kevésbé vonzó (összesen 35,05%) kategóriáját még meggyőzőbb képet kapunk.

A fővárosban élők túlnyomóan pozitív véleménye közel 30 százalékát adja a mintánknak, ha a figyelmünk csak a községekre, nagyközségekre irányul, szintén ennyire kedvező a kép az együttes 22,68%-kal.

A külföldön élő magyar állampolgárok körében a legnagyobb arányú a teljes negativitás, de ez a mintánkat figyelembe véve elenyésző („Egyáltalán nem vonzó” - 2,06%).

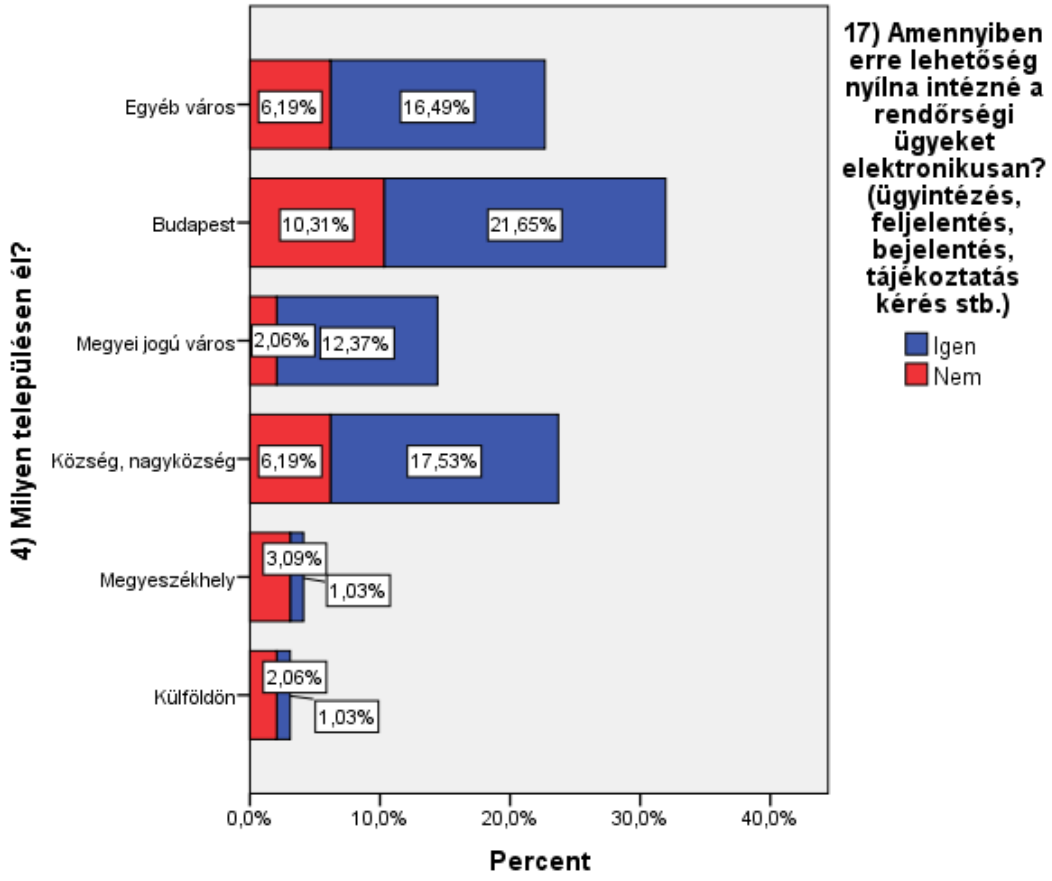
Árnyaltabb véleményeket tapasztalhatunk a megyei jogú városban és a Budapesten lakóknál („Kevésbé vonzó” - 3,09%).

A legkevésbé elutasítók az egyéb városokban és a községekben, nagyközségekben élők a teljes mintát figyelembe véve (1,03%) és az egyedi település kategóriákban is a többihez képest is.

A skálák egyenként is egyértelműen a pozitív attitűd felé tolódnak el, leszámítva a külföldön élő magyar állampolgárok válaszait. Az esetlegesen hezitálók, illetve részlegesen, vagy teljesen elutasítók indokaira a kutatás következő fejezeteiben további részletes elemzés keretében keressük a válaszokat.

A rendőrség, mint speciális közigazgatási szakterület vonatkozásában a válaszadók nagyobb része utasítja el az elektronikus ügyintézés lehetőségét a korábbi vélekedésekhez képest.

6. ábra A rendőrségi elektronikus ügyintézés jövőbeli lehetőségének kihasználása a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

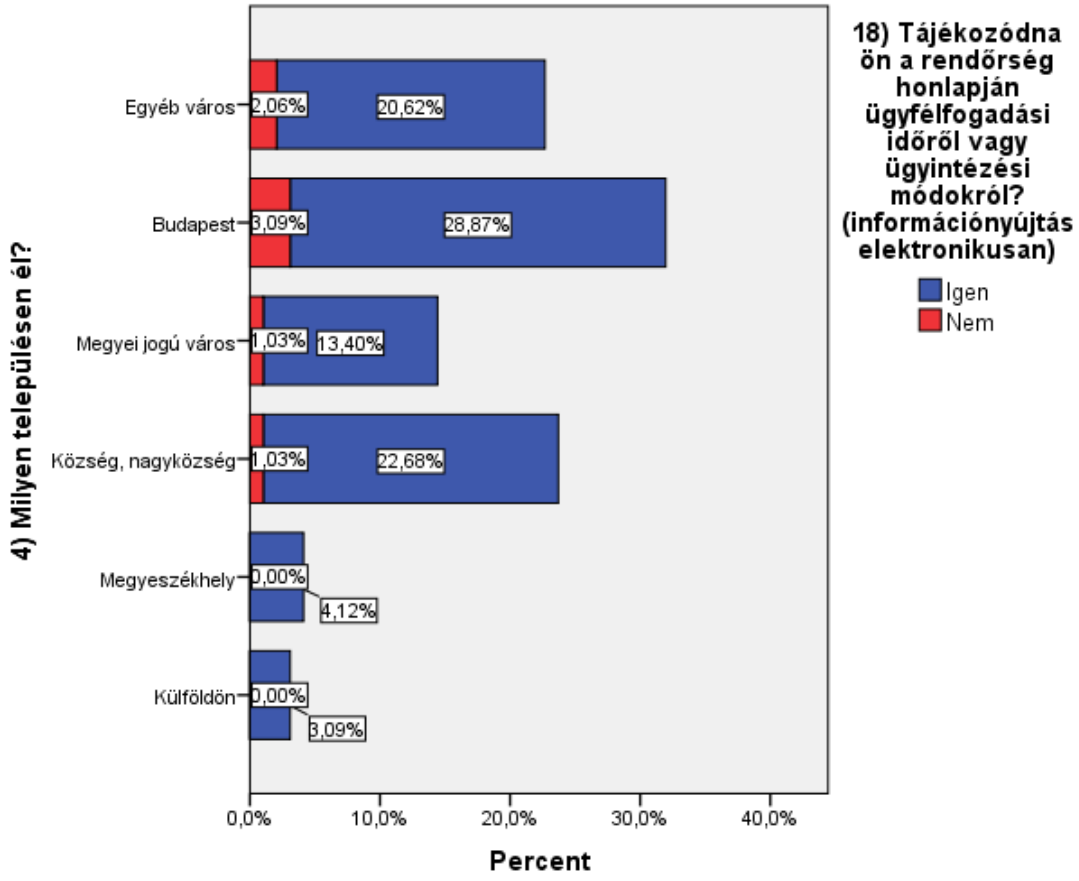
A fővárosban lakó személyek tekintetében érezhető a bizalmatlanság, mely a válaszok 10,31%-át jelenti, majd ezt követik az egyéb városok és a községek, nagyközségek egyaránt 6,19 százalékkal. Fontos hangsúlyozni, hogy a negatív

vélemények mögött meghúzódhatnak egyéb, nem kifejezetten a rendőrségre vonatkozó tapasztalatok, hanem inkább a napjainkban is sok esetben nehezen kivitelezhető, illetve használható elektronikus ügyintézési problémák.

Amennyiben a kitöltők három legnagyobb településcsoportját vesszük figyelembe, már a teljes mintához képest is meghaladja a kérdés az 50 százalékos támogatottságot, összesen pedig eléri a 70%-ot. A kérdés elemzése megalapozza a felvázolt hipotézist, hogy jelentős igény mutatkozik a rendőrségi elektronikus ügyintézés megvalósulására és kiterjesztésére.

Az elektronikus információnyújtásra vonatkozóan a kérdések közül az egyik legpozitívabb eredményt kívánjuk bemutatni.

7. ábra A rendőrségi elektronikus ügyintézés jövőbeli lehetőségének kihasználása a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

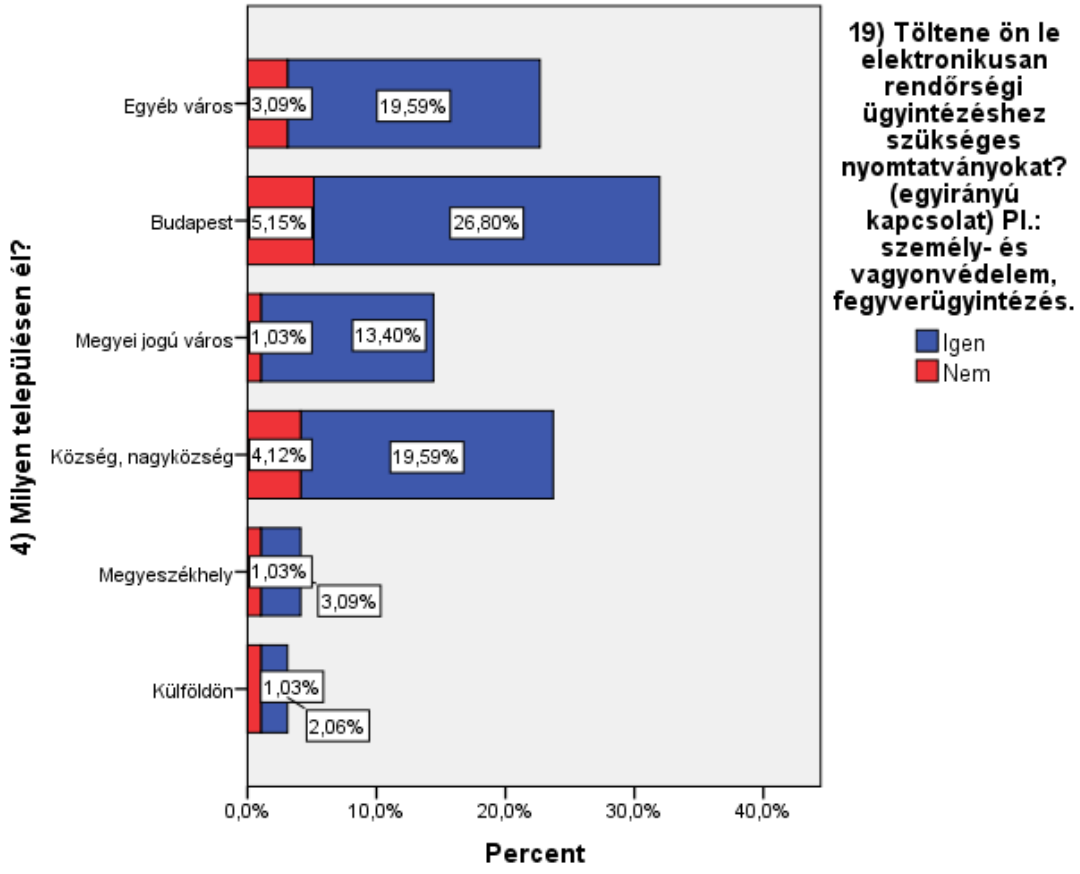
A megyeszékhelyeken és külföldön élő magyar állampolgárok vonatkozásában nem is találunk ellenző véleményt. Fordulatként mutatkozik, hogy a községek és a nagyközségek válaszadói a teljes minta 22,69%-os támogatottságát

adják. Ez azt jelenti, hogy ebben a településtípusban 95,66 százalék igényelné az információk ezen módjának a jelenleg alkalmazott elektronikus információs rendszer hatékonyságának kibővítésére vonatkozóan. A válaszadók számára nagy segítséget jelentene az elektronikus tájékozódási lehetőség biztosítása.

Egyértelműen látszik, hogy a megkérdezettek körében a lakóhelyek településtípus szerinti bontásának minden csoportjában 90,33 és 100,00 százalékos az igény az e-információnyújtás lehetőségének megteremtésére.

Hasonlóan kedvezők a vélemények az egyirányú elektronikus kapcsolat tekintetében. Minden lakóhelytípus mérlege a pozitív vélemény felé tolódik el jelentős mértékben.

8. ábra A rendőrségi elektronikus nyomtatványok kitöltésének jövőbeli lehetősége a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

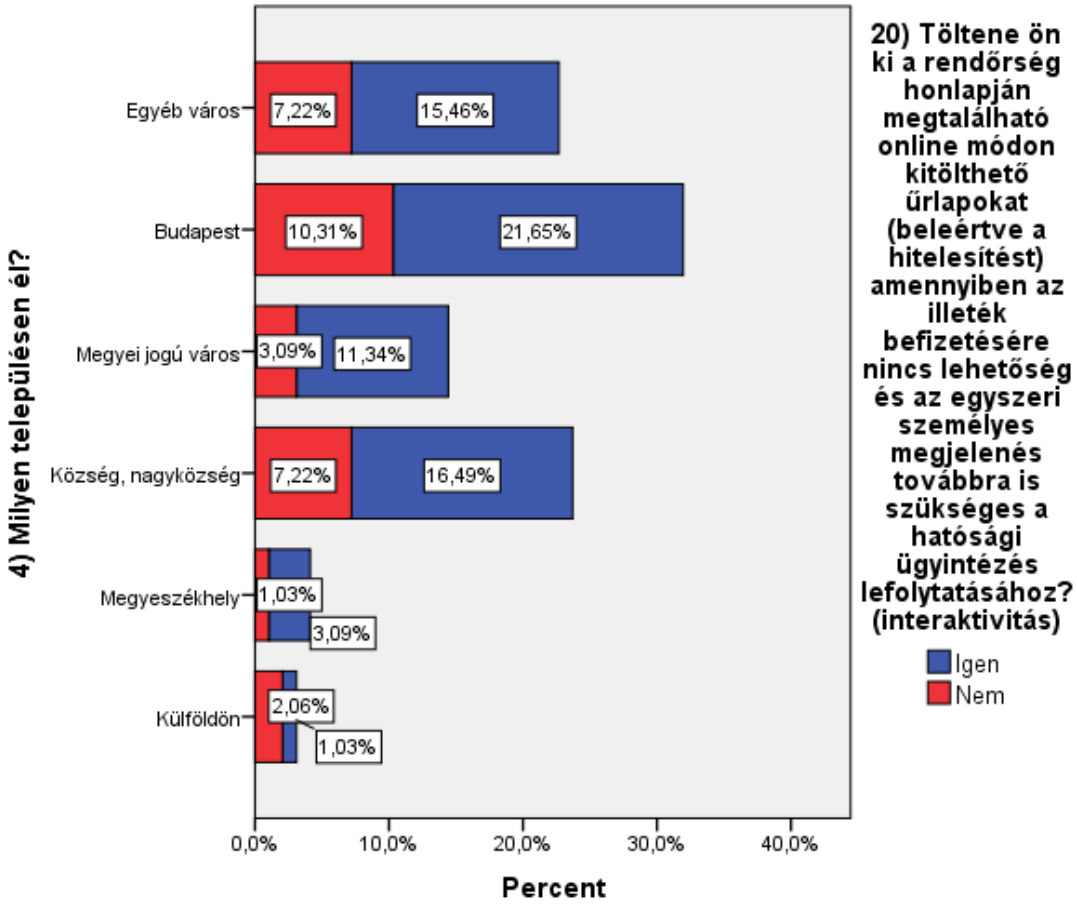
A nagyobb súllyal szereplő településtípusokat megfigyelve a megyei jogú városokban közel 93%-os a kitöltési szándék az elektronikus formátumban elérhető és letölthető nyomtatványokra vonatkozóan, ezt követik az egyéb városok 86,37

százalékkal, majd budapestiek (83,88%) és a községekben, nagyközségekben élő személyek (82,62%).

A rendőrségi e-ügyintézés interaktivitásra vonatkozó kérdését megvizsgálva - *melyben a hatósági ügyintézés egyszeri személyes megjelenési kötelezettséggel járna a nyomtatványok elektronikus kitöltését követően* - a hisztogram hatványozottan szimbiózisban mozog a rendőrségi elektronikus ügyintézés kérdésével (feltételek nélkül), melyet a 6. ábrán láthattunk.

Arányaiban kicsivel több pozitív választ kaptunk a megyei jogú városokban és a megyeszékhelyen élőktől (mely a válaszadók 3,49 és 1,03%-a), és kevéssel több negatívat az egyéb városokban és a községekben, nagyközségekben élőktől (7,22%).

9. ábra A rendőrségi elektronikus űrlapok kitöltésének jövőbeli lehetősége egyszeri személyes megjelenési kötelezettséggel a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



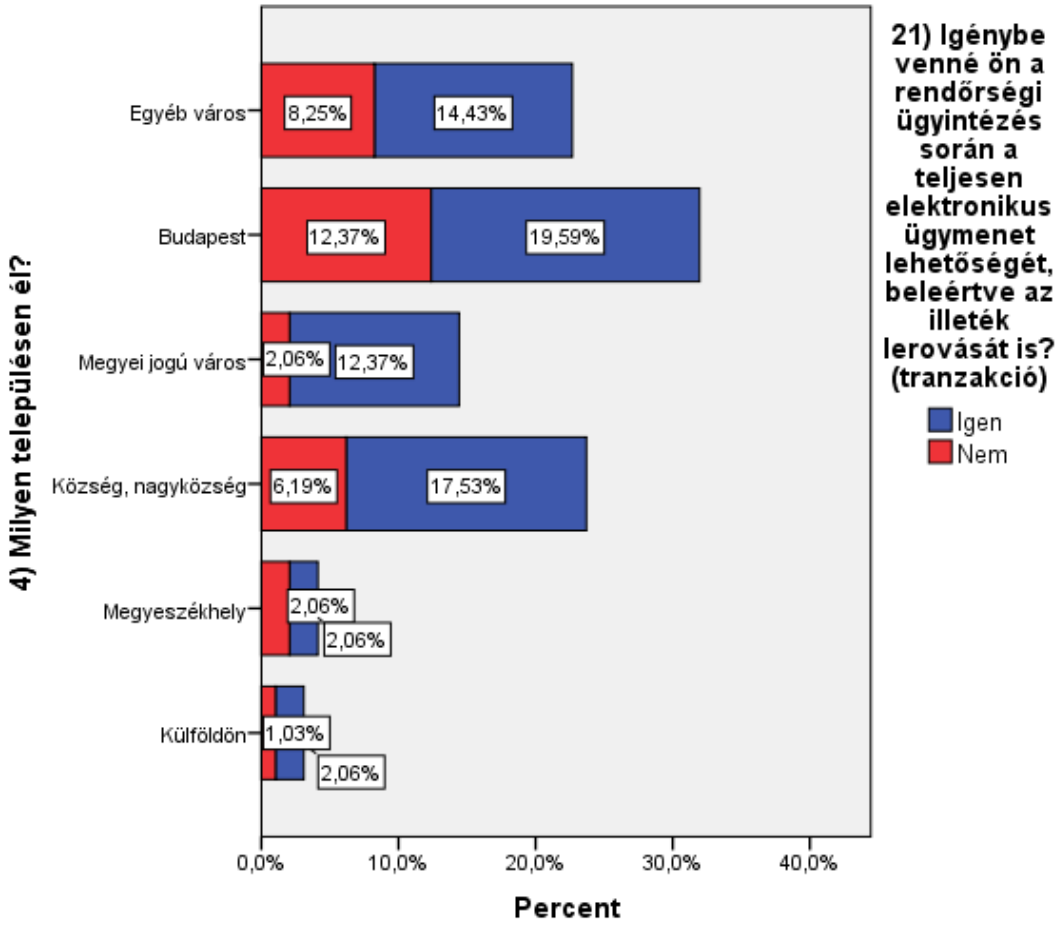
Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

A 10. ábrán a teljes elektronikus ügymenetre vonatkozó felvetésénél az első szembetűnő adat a külföldiek kétharmadának a támogatottsága.

A megyei jogú városokban az ellenzők mindösszesen a megkérdezettek 2,06%-a, amely az adott településtípusok tekintetében 85,72 százalékos támogatottságot jelent. A többi három jelentős lakóhelytípust a teljes ügyintézés bizalomrátáján léptékekkel megelőzi, de csoportonként a legalsó határ meghaladja a 60%-ot.

Valószínűsíthető, hogy a gyakorlati alkalmazás pozitív tapasztalatai által ezek az arányok is javíthatók vállhatnak.

10. ábra A teljes rendőrségi elektronikus ügymenet jövőbeli lehetősége a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



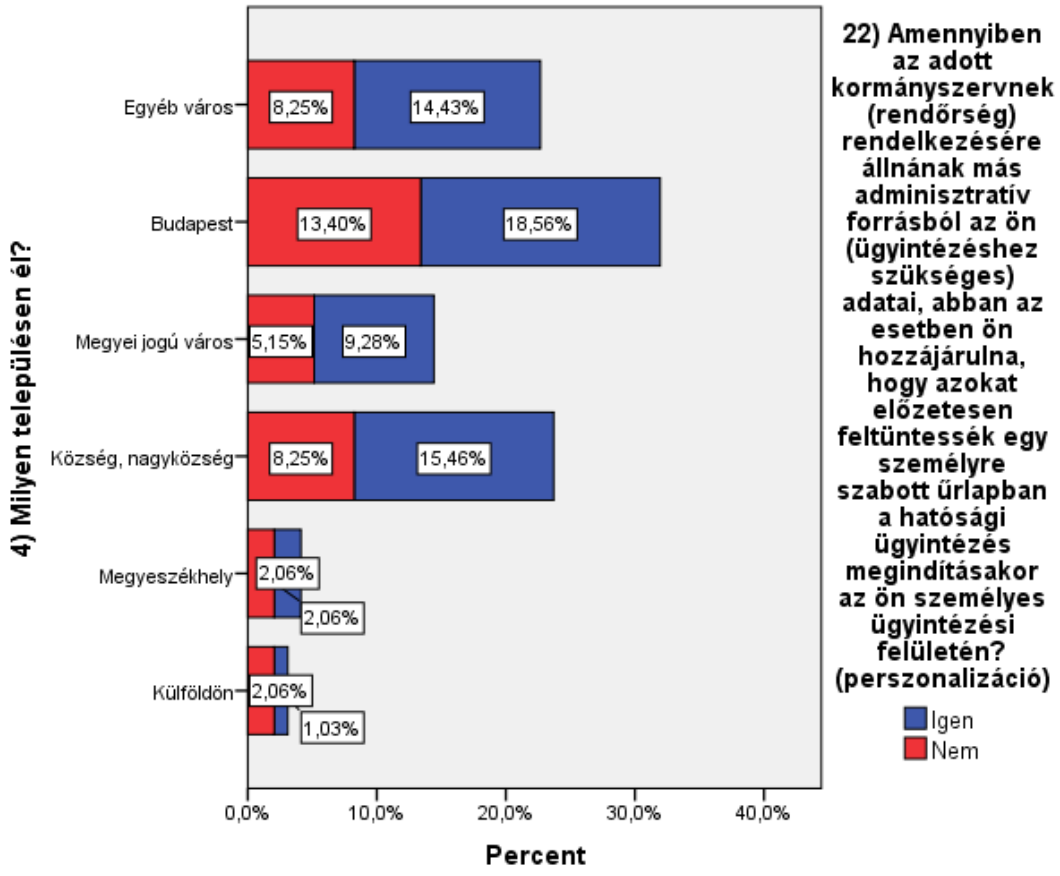
Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

A lakossági megoszlást tartalmazó elemzés utolsó részeként a perszonalizáció lehetőségét vizsgáltuk (11. ábra), vagyis a kitöltőktől az adminisztratív forrásból rendelkezésre álló, egyes ügyintézésekhez szükséges adatok előzetes kitöltéséhez történő hozzájárulási hajlandóságot kérdeztük meg a rendőrségi ügyintézés

szempontjából. A felvetés nem újkeletű, hiszen találkozhattunk már hasonló esetekkel más elektronikus kitöltő felületen, vagy közigazgatási oldalon.

A két legnagyobb csoportot képviselő településtípuson élők közül Budapest 58,07%, míg a község, nagyközség 65,2%-kal szerepel. A lakosság számát tekintve pontosan a skála két végén szereplő településeknél sem figyelhető meg drasztikus eltérés, vagyis a fővárosiaktól a legkisebb településig többé-kevésbé 60%-os a támogatottsága a perszonalizációnak (egyéb városok 63,62%, megyei jogú város 64,31%). A külföldön élő magyar állampolgárok a minta átlagos tendenciájától eltérően csak 33,33%-ban támogatják az adott kérdést.

11. ábra Hozzáárulás a hatósági ügyintézés személyre szabott űrlapon keresztüli ügyintézéséhez a válaszadók lakóhelye szerinti megoszlásban, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Összességében elmondható, hogy az adott hipotézis figyelembe vételével a kérdésekre adott támogatottság 60-100% közé esik a településtípusok szempontjából.

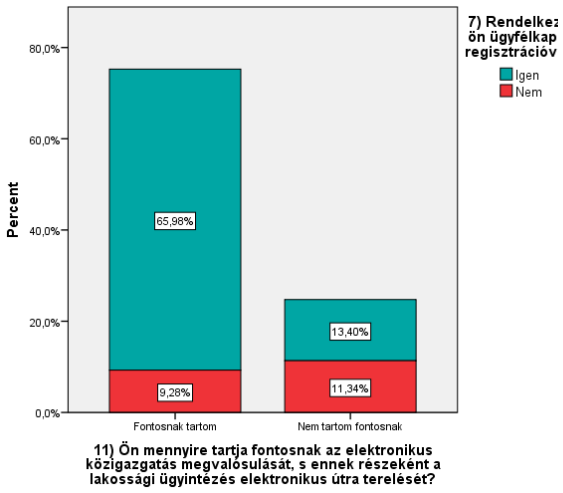
2. ***Az ügyfélkapus regisztráció hiánya, valamint azon közigazgatási honlapok ismeretlensége, ahol lehet részleges-, vagy teljes elektronikus ügyintézést folytatni, hozzájárul az Ügyfélkapu szolgáltatásainak kihasználatlanságához és az e-ügyintézési folyamatok gyengítéséhez.***

Vizsgálatunkban szintén a kereszttáblás elemzéseket hívjuk segítségül, szemléltetésül pedig ismét a hisztogramot használjuk.

Az ide vonatkozó kérdéseket az ügyfélkapus regisztráció meglétével illetve az elektronikus ügyintézési lehetőséggel rendelkező közigazgatási honlapok ismeretével kapcsolatban vizsgáljuk.

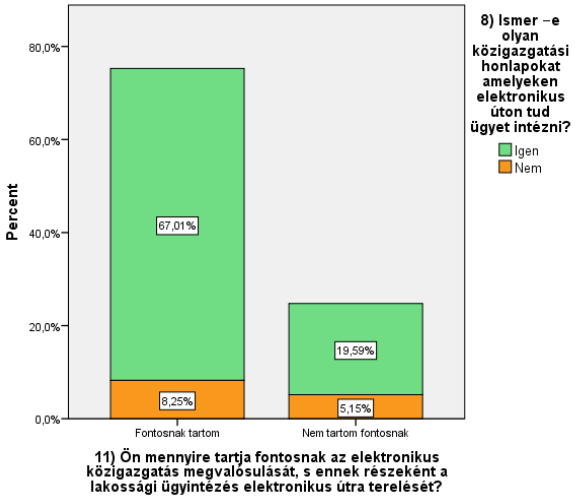
Elsőként az elektronikus közigazgatás megvalósulásának és ennek részeként az lakossági ügyintézés elektronikus útra terelését láthatjuk.

12. ábra Az elektronikus közigazgatás és az elektronikus lakossági ügyintézés fontossága az ügyfélkapus regisztráció függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

13. ábra Az elektronikus közigazgatás és az elektronikus lakossági ügyintézés fontossága elektronikus ügyintézési lehetőséggel rendelkező közigazgatási honlapok ismeretének függvényében, 2017 (%)



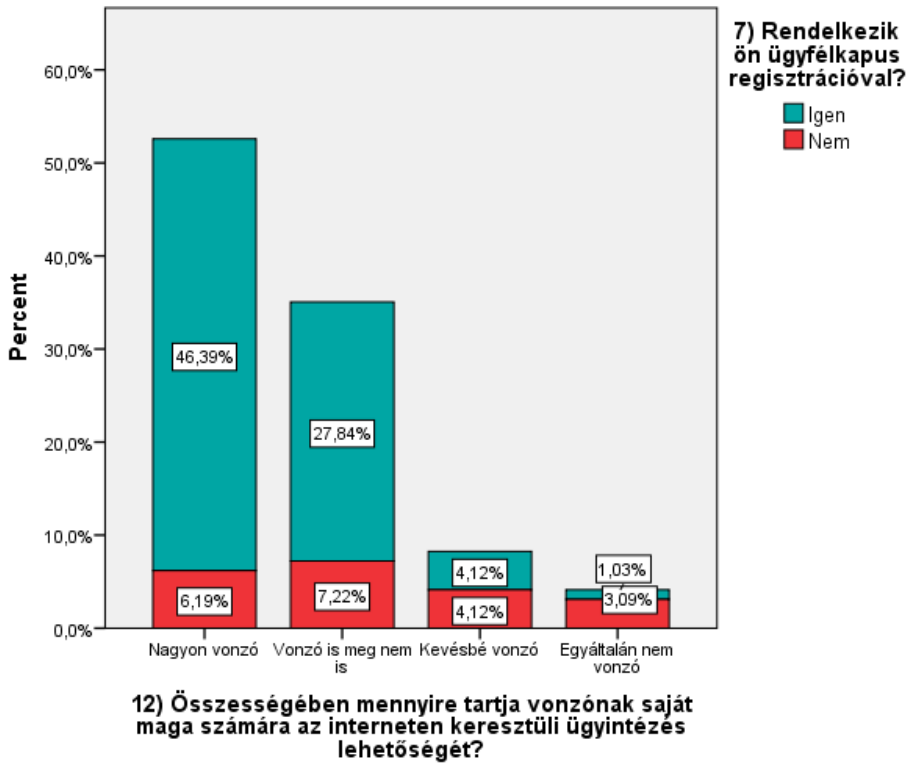
Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Megfigyelhető a két grafikon közötti hasonlóság a kérdést fontosnak tartók szempontjából. Azok számára, akik rendelkeznek ügyfélkapus regisztrációval 87,67%-ban, akik ismernek elektronikus ügyintézési lehetőséggel rendelkező

közigazgatási honlapokat 89,04%-ban fontos az elektronikus közigazgatás megvalósulása – ez a teljes mintánk 65,98 illetve 67,01 százaléka.

Arra a kérdésre, hogy összességében a válaszadók mennyire tartják fontosnak saját maga számára az interneten keresztüli ügyintézés lehetőségét, hasonló arányokat kapunk a kapcsolódó aspektusokkal vonatkozásában.

14. ábra Az internetes ügyintézés lehetőségének attraktivitása az ügyfélkapus regisztráció függvényében, 2017 (%)



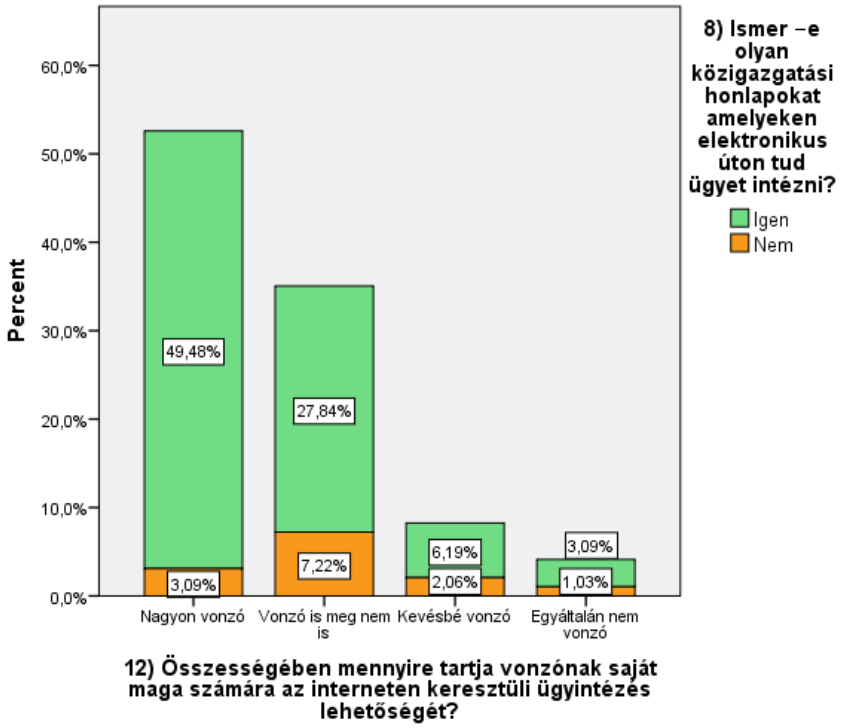
Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Az ügyfélkapus regisztráció meglétének szempontjából vizsgálva nagyon vonzónak tartják az e-ügyintézést 88,23%, ez a megkérdezettek csaknem felét (43,39%) jelenti, illetve vonzó is meg nem is vélemények is a minta további 27,84%-át teszik ki, tehát a pozitív véleményen lévők azok közül, akik rendelkeznek ügyfélkapus regisztrációval összesen a megkérdezettek háromnegyede (74,23%).

A kevésbé vonzó vélemények fele-fele arányban oszlanak meg az ügyfélkapus regisztráció tekintetében, de ez összesen a megkérdezettek 8,24%-ának felel meg. Akik egyáltalán nem tartják vonzónak háromnegyed részben nem is rendelkeznek ügyfélkapuval (3,09%).

Mindezt megvizsgálva azok körében, akik ismernek olyan honlapokat, ahol lehet elektronikusan ügyet intézni, közel hasonló eredményeket kaptunk, melyet a következő hisztogram szemléltet (15. ábra).

15. ábra Az internetes ügyintézés lehetőségének attraktivitása elektronikus ügyintézési lehetőséggel rendelkező közigazgatási honlapok ismeretének függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Akik számára a nagyon vonzó az elektronikus ügyintézés, 83,06%-ban ismerik ezeket a weboldalakat, ez a mintánk 49,48 százalékát jelenti, míg a vonzó is meg nem is kategóriában 79,40 % ezen válaszadók aránya. A negativitás mértéke közel hasonlóan alakul az ügyfélkapuval rendelkezők attraktivitásához.

Az ábrákból is látszik, hogy a válaszadók vonzónak, illetve inkább vonzónak tartják saját maguk számára az elektronikus ügyintézést, és döntő többségük használja az ügyfélkapus regisztrációt, valamint ismer elektronikus ügyintézési felülettel rendelkező közigazgatási honlapot.

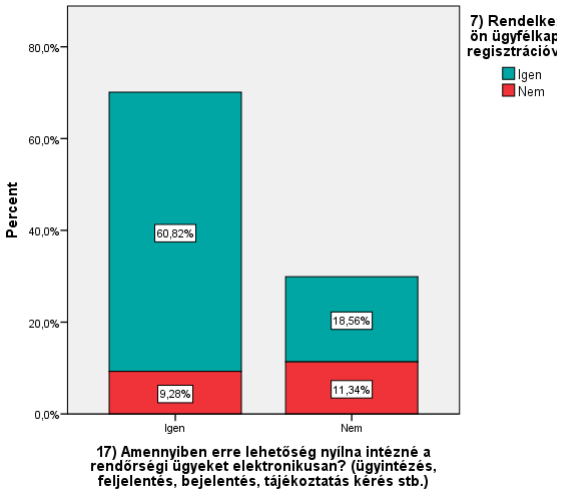
A továbbiakban a rendőrségi elektronikus ügyintézés jövőbeli lehetőségének kihasználását elemezzük a már korábban felvetett aspektusok figyelembe vételével.

A megkérdezettek 70,1 százaléka nyilatkozott úgy, hogy intézné a rendőrségi ügyeit elektronikusan, ebből 60,82% rendelkezik ügyfélkapuval és 63,92% ismer

elektronikus ügyintézéssel rendelkező közigazgatási weboldalakat - ez a teljes mintánk 86,76 és 91,17 százaléka.

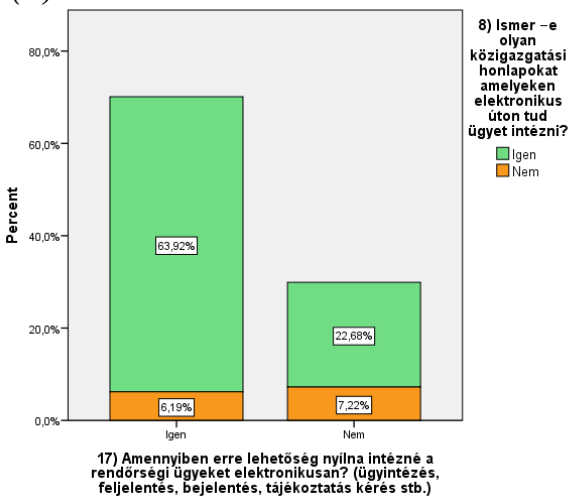
A negativitásnál az ügyfélkapuval nem rendelkezőknek nagyobb az aránya, ez a megkérdezettek 11,34%-át teszi ki, és van egy vékony réteg (7,22%), aki nem ismer e-közigazgatási weboldalakat sem. Elmondható, hogy nagy mértékben kedvezőnek tartják a válaszadók ezt a jövőbeli lehetőséget és élnének is vele.

16. ábra A rendőrségi elektronikus ügyintézés jövőbeli lehetőségének kihasználása az ügyfélkapus regisztráció függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

17. ábra A rendőrségi elektronikus ügyintézés jövőbeli lehetőségének kihasználása elektronikus ügyintézési lehetőséggel rendelkező közigazgatási honlapok ismeretének függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

Adott részvizsgálat a rendőrségi ügyintézés során a teljes ügymenet lehetőségének igénybe vételét vizsgálja. (18. és 19. ábra)

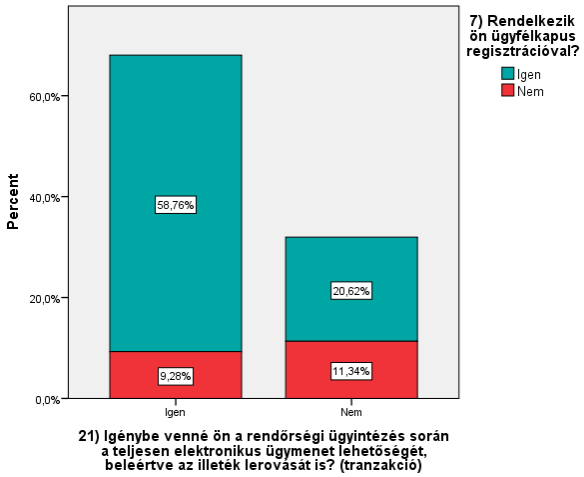
A megkérdezettek közel 70 százaléka igénybe venné a teljes ügymenet során az elektronikus rendőrségi ügyintézést. Közülük 86,36% rendelkezik ügyfélkapuval és 92,43% ismer e-ügymenettel rendelkező közigazgatási honlapokat.

A nemmel válaszolók körében magasabb arányban vannak azok mindkét grafikonon, akik nem is vennék igénybe a teljes ügymenetet, de mindez a teljes mintánkra vetítve csak 11,34 és 8,25 százalékot tesz ki.

Fontos felhívni a figyelmét a lakosságnak az elektronikus közigazgatásra vonatkozó aspektusokra, és kihasználni, feltárni a kínálkozó lehetőségeket.

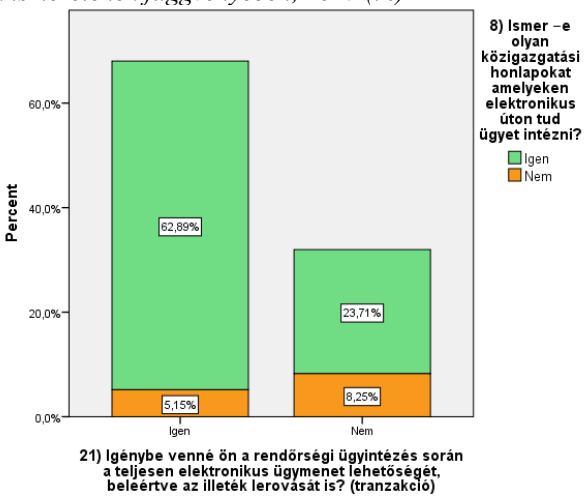
A rendőrség vonatkozásában pedig egyértelmű igény mutatkozik a felmérésből egyéb közigazgatási webfelületektől és ügyintézéstől függetlenül (természetesen azokat véve alapul).

18. ábra A teljes rendőrségi elektronikus ügymenet jövőbeli lehetősége az ügyfélkapus regisztráció függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPSS

19. ábra A teljes rendőrségi elektronikus ügymenet jövőbeli lehetősége az elektronikus ügyintézési lehetőséggel rendelkező közigazgatási honlapok ismeretének függvényében, 2017 (%)



Forrás:
Saját készítésű grafikon - Kérdőíves adatelemzés, SPS

5.5. Összefoglaló megállapítások a kutatáshoz

A rendőrség elektronikus formában végzett ügyintézésének, mint új képesség kihívásainak vizsgálata témakörben végzett kutatásunk második fázisa a kvantitatív kutatás, melyben a számszerűsített, mért adatokra fókuszálunk, ezáltal rendszerességeket és szabályszerűségeket keresve a megkérdezettek véleményeiből.

Jelen kutatási fázisban pontosabb, számszerű adatokat nyerhettünk ki a válaszok alapján.

A közel 100 megkérdezett véleményét bemutató eredményeket összesítve elmondható, hogy a kvantitatív kutatási fázis során adott válaszok arra utalnak, hogy felülvizsgálata szükséges a jelenleg alkalmazott e-közigazgatási modell egyes részeinek. Az állampolgárok valós igényeket fogalmaztak meg arra vonatkozóan, hogy a rendőrségi ügyintézés egyes elemei (a jelenleg elérhető ügyintézési struktúra mellett) az elektronikus közigazgatás részét képezzék. A válaszokból levonható további következtetés, hogy a külföldön állandó jelleggel tartózkodó magyar állampolgárok igényeire is figyelemmel kell lenni az elektronikus közigazgatás következő fejlesztési szakaszában. A felvázolt kormányzati stratégia deklarált célja a külhoni magyar közösségek igényeihez is igazodó, az azt kiszolgálni képes közigazgatás, e-közigazgatási szolgáltatások fejlesztése, az ügyfélkapcsolati pontok és az ügysegédi rendszer fejlesztése, a határokon átívelő elektronikus ügyintézés ügyféloldali lefedéséhez szükséges kiegészítő fejlesztések, valamint a külhoniak közszolgáltatásokhoz kapcsolódó élethelyzeteihez tartozó ügyek egyszerűsítése.

A fejlesztési stratégia céljainak és irányainak meghatározása során szem előtt kell tartani, hogy a rendőrség igazgatásrendészeti feladatrendszeréhez köthető ügyintézési folyamatok teljes mértékben nem kerülhetnek integrálásra az elektronikus közigazgatási rendszerbe. Az állampolgárok egy jelentős része még mindig bízik a személyes ügyintézővel történő kapcsolattartásban, valamint vannak olyan természetű ügyek, amelyekhez hozzátartozik a személyközi kommunikáció megléte. *A rendőrség vonatkozásában ilyen ügyek a lőfegyvertartási engedélyek kiadására, a lőfegyverek tartásának engedélyeztetése, a gáz- és riasztó fegyverek viselési engedélyeinek kiadása*, hiszen az engedélyeztetési eljárás szerves részét képezi az ügyintéző által (*a rendőrkapitányság épületében*) történő azonosítása. Amennyiben az igazgatásrendészeti szolgálati ág másik jelentős feladatrendszeréről beszélünk, akkor abban az esetben már más következtetésre jutunk. A magánbiztonsági

szakterület személy- és vagyonvédelmi, magánnyomozói, valamint vagyonvédelmi rendszert szerelői és tervezői igazolványok és működési engedélyek engedélyeztetési eljárása részleges, vagy teljes elektronikus ügyintézés alá vonhatóvá válhat, amennyiben a közigazgatás hatékonysága érdekében felvázolt beavatkozások elérik a kitűzött célokat. Azonban továbbra is figyelembe kell venni, hogy a rendőrség elektronikus közigazgatási rendszerét érintő fejlesztési és stratégiai célok meghatározása során az egyes szakterületek szakmai véleményét is ki figyelembe kell venni. Cél a hatékonyabb feladatellátás biztosítása, ezért elengedhetetlen a rendőrséghez kapcsolódó közigazgatási feladatok felülvizsgálata és esetleges újraelosztása akár a közigazgatás többi szereplője között.

5.5.1. Fókuszcsoportos elemzés

Kvalitatív kutatásunk során feltérképeztük a témakörben adott véleményeket, illetve kiderült, hogy milyen gondolatai lehetnek fókuszcsoportjainknak a hazai elektronikus közigazgatással, valamint a rendőrség elektronikus formában végzett ügyintézésével kapcsolatban, milyen hitek és tévhitek léteznek e tekintetben. Segítségével bizonyos feltételezéseket jobban átláthatunk és bár végső következtetéseket nem vonhattunk le belőle, mindenképp egy megfelelő kiegészítésül szolgál a kérdőíves kutatási fázisunk esetében.

A fókuszcsoportos kutatás keretében kettő csoportülésre került sor. Mindkét esetben a Komárom-Esztergom Megyei Rendőr-főkapitányság épületében került sor. Mind a kettő csoportülésen résztvevő személyek a rendőrség hivatásos állományú tagjai voltak, akik a rendőrség bűnügyi, közrendvédelmi, közlekedésrendészeti, hivatali és igazgatásrendészeti szolgálati szakterületén láttak el szolgálatot, különböző beosztásokban. Mind a két csoport egy csoportvezető irányítása mellett, kötetlen, félig-irányított beszélgetés során vitatták meg a kutatáshoz kapcsolódó egyes aspektusokat.

A beszélgetések során a kutatás vezető kérdéseire a csoport tagok által adott vélemények, egyéni meglátások, gondolatok és válaszok hozzájárulnak a rendőrség elektronikus közigazgatásban betöltött jelenlegi szerepének (szakmai szempontok alapján történő) megismeréséhez, valamint feltárásra kerülnek azok a kihívások és kockázatok, amelyek gyengíthetik a rendőrség elektronikus közigazgatásban betöltött szerepének erősödését. A fókuszcsoportos beszélgetés során az egyes szakterületek vonatkozásában és a szakmai szempontok figyelembe vételével világítunk rá azokra a képességekre, amelyek

fejlesztésével a rendőrség részleges, vagy teljes elektronikus közigazgatási tevékenysége fejleszthetővé válik.

Moderátor kérdése:

- Az egyes rendőrségi szakterületeket vizsgálva látnak arra lehetőséget, hogy bizonyos (közigazgatási) ügytípusok részleges, vagy teljes elektronikus ügyintézés keretében kerüljenek végrehajtásra?

  Válaszok:

  - „A bűnügyi szakterület vonatkozásában nem, mivel sem a gyanúsítási eljárás során, sem egyes nyomozati szakaszokban nem lehet nélkülözni a személyes jelenlétet. A jelenlegi szabályok szerint tanú írásban tehet vallomást, azonban ez sok esetben nem mellőzhető az eljárás során. Vagy egy szembesítési eljárás során sem lehet nélkülözni az adott személy jelenlétét. A büntető eljárás teljesen egységes, az csak egyféleképpen folytatható le. Ahol lehet mozgástér az elektronikus ügyintézés részleges lebonyolítására ott már jelenleg is lefolytatható. Pl.: az ügyvéd adhat be elektronikusan beadványt a hatóság felé. A büntető eljárás szempontjából nem értelmezhető az elektronikus eljárás rendszerének lehetőségei.
  - Akár a közigazgatási bírságokat, akár a helyszíni bírságolást vizsgáljuk jól látható, hogy jelenleg nem nélkülözhető az állampolgár aláírása. A bíróságokra történő ügyiratok megküldése történik elektronikusan. A helyszíni bírságolás kezdeti szakaszában a közigazgatási ügymenet gyorsítása érdekében lehetne bevezetni a bankkártyás fizetés lehetőségét.[64]
  - A szabálysértési eljárások szempontjából, egy balesetes ügyben ahol a tényállás nem tisztázott, ott akár az okozó, akár a tanú, akár a részes, akár az eljárás alá vont személy meghallgatása történik, azt csak személyesen lehet végrehajtani. Ott lehet mozgástér, ahol a feljelentés alapján a tényállás tisztázott, a határozat meghozatalát követően (amennyiben nem nyújt be a személy meghallgatási kérelmet) a teljes ügymenet elektronikusan végig vezethető a végrehajtási eljárás lezárásáig.

[64] A rendőrség 2010-ben már teszt jelleggel (legfőképpen németországi modell alapján) bevezette a helyszíni bírság bankkártyával történő kiegyenlítésének a lehetőségét. A rendszer törvényi háttere adott volt, azonban számos probléma és aggály is felmerült a rendszer tesztüzeme során. Azonban láthatjuk, hogy több Európai Uniós tagállamban (Németország, Ausztria, Horvátország) hatékonyan működik a helyszíni bírság bankkártyával történő kiegyenlítése. Horvátországban a bírság befizetési hajlandóság közel a duplájára emelkedett a bankkártyás fizetési lehetőség bevezetését követően.

- A közrendvédelemi szakterület vonatkozásában elsősorban a rendezvények bejelentése történhet elektronikus felületen, amennyiben nincs egyeztető tárgyalásra szükség. Viszont ebben az esetben kihívásként kell kezelni, hogy a bejelentő személy megkapta-e a hatóság tudomásulvételi szándékáról szóló határozatot és adott esetben az is kihívásként kezelendő, hogy az a személy kapja meg a határozatot, aki bejelentette az adott rendezvényt.
- A hivatali szakterület vonatkozásában eléggé fejlett az elektronikus ügykezelés. A KIR rendszerből szedjük le az anyagokat és az érkeztetést követően továbbítjuk őket a címzett szakterületnek.
- Az igazgatásrendészeti szolgálati ág rendészeti szakterülete szempontjából a fegyverrendészeti szakterület egyes lépései már most is lebonyolítható részleges elektronikus ügyintézés keretében. A kérelmi lapok elérhetők és letölthetők a rendőrség központi honlapjáról. Amennyiben az elavult lőfegyvertartási engedélyek jövőbeni cseréjére kerülne sor, akkor azoknak az okmányoknak a vonatkozásában elképzelhető további részleges elektronikus ügyintézési szakasz beiktatása. A személy- és vagyonvédelmi engedélyeztetési eljárás szempontjából már több lehetőséget látok. Akár a kérelem beadását, akár a hatósági szolgáltatási díj befizetését, akár a mellékletek benyújtását, akár az adott személy azonosítását és ellenőrzését, akár a hatósági igazolvány legyártását és postázását, mint egyes folyamatot vizsgáljuk, elképzelhető egy teljes elektronikus ügyintézés bevezetése és végrehajtása.”

A fókuszcsoportos kutatás igazolja azokat a hipotéziseket amelyek arra vonatkoztak, hogy a rendőrség elektronikus ügyintézési tevékenysége (egyes szakterületek vonatkozásában) fejleszthető. A fókuszcsoportos szakmai beszélgetés során elhangzottak alátámasztják a kérdőív eredményeit, abból a szempontból, hogy az állampolgárok igénylik a rendőrség elektronikus ügyintézési tevékenységének szélesebb körű alkalmazását. Ezekkel a szakmai álláspontokkal ellentétben azokat a szakmai szempontokat is figyelembe kell venni, amelyek a kockázatokat erősítik a rendszer fejlesztése területén. A szigorú adatvédelmi követelmények betartása mellett előtérbe kell helyezni a rendőrségi eljárások során keletkezett adatok védelmére és kezelésére vonatkozó kérdésköröket. Mindazonáltal a rendőrség iratkezelési és irattározási folyamatának egyes rendszerei, valamint a magánbiztonsági szakterület engedélyeztetési eljárásai végrehajtásában egyöntetű vélemény

alakult ki a fókuszcsoportos vizsgálat során, hogy akár teljes elektronikus ügyintézés is elképzelhető a jövőben.

Következtetések és javaslatok

A közigazgatás jogi alapjainak az újra definiálása az elmúlt évek egyik legnagyobb hazai kihívása volt a jogalkotás területén. A legfontosabb célkitűzés s szolgáltató állam megteremtése több nehézségbe ütközött. A megkezdett intézkedések hatékonyabb végrehajtása érdekében egy *önmagát erősítő* és *a valós értékeit* szem előtt tartó szolgáltató közigazgatási rendszer kiépítése az elsődleges cél. A Közigazgatás- és Közszolgáltatás fejlesztési Stratégia 2014-2020 munkaanyagban lefektetésre került, hogy a fejlesztés következő lépcsője a közigazgatás és a közszolgáltatások területének speciális szakterületei vonatkozásában kerül megvalósításra, elősegítve az adott szakterület hatékonyabb működését.

Az Ügyfélkapu közigazgatási ügyintéző és szolgáltató rendszer jelenlegi hatékonyságát és a közigazgatási rendszerben betölteni kívánt szerepét még nem érte el. A közigazgatásra vonatkozó fejlesztési célok konkrétan meghatározzák, hogy a közszolgáltatásokhoz történő hozzájutás átfogóan képezi a stratégia tárgyát. Az e-közigazgatási platformok és az Ügyfélkapu rendszerhez történő hozzáférés és alkalmazás társadalmi elfogadottsága érdekében elengedhetetlen az informatikai eszközök, internet-hálózatok, valamint a mobil hálózatok fejlesztése. A rendőrségi ügyintézési fejlesztések erősítése érdekében elengedhetetlen az Ügyfélkapu rendszer átstruktúrálása.

A rendőrség közigazgatási rendszerben betöltött dinamikus szerepe vitathatatlan. Az ügyfélközpontú és bürokráciacsökkentő szolgáltatások rendszerében történt fejlesztések és átalakítások a szolgáltatói rendészeti oldal szempontjából nem értek el kellő hatékonyságot. A rendőrség, mint közszolgáltatást nyújtó szervezet működési hatékonyságának és ágazati képességeinek fejlesztése érdekében, valamint a közszolgáltatások hozzájutásának elősegítése érdekében szükséges és elengedhetetlen a szervezeti struktúra rendszerének felülvizsgálata. A felülvizsgálat során ki kell térni az ügyfélbarát kommunikációs intézkedésekre, a jól megválasztott rendészeti struktúrára, valamint a rendőrség államigazgatási feladatrendszerének átstruktúrálására és újra szabályozására.

Az állam által megfogalmazott közigazgatási stratégiai kimondja, hogy ne szülessenek szabályok és döntések az ügyfelek véleményének kikérése nélkül.

Ennek az eszmének az érvényesítése érdekében jelen kutatás arra vállalkozott, hogy a rendőrség speciális közigazgatási feladatrendszerére vonatkozóan, kiemelten az elektronikus közigazgatás betöltött szerepét vizsgálva, egy nem reprezentatív feltáró jellegű kutatást végez el az állampolgárok körében. Az eredmények elemzéséből kimutatható, hogy a rendőrség közigazgatási rendszere fejlesztésre szorul, az egyes rendészeti területek túlszabályozottságát csökkenteni kell. Hatékony lépéseket kell tenni a rendőrség elektronikus közigazgatási rendszerben betöltött szerepének erősítése érdekében. Ennek érdekében az egyes szolgálati ágakat külön-külön kell vizsgálni, mivel a fókuszcsoportos (szakmai alapú) vizsgálat rávilágított, hogy az elektronikus platformra történő átállítás folyamata nem minden szolgálati ág szempontjából releváns és végrehajtható feladat. A kutatás rávilágított arra, hogy egyes rendőrségi rész-szakterületek vonatkozásában akár a teljes elektronikus ügyintézési folyamat megvalósíthatóvá válik, amely által a rendőrség elektronikus ügyintézési képességének erősítése érhető el. *További kutatásokat igényel a rendőrség ügykezelési és irattározási feladatrendszerének teljes elektronikus platformra történő átvitele, valamint a személy- és vagyonvédelmi szakterület teljes elektronikus ügyintézésének a megvalósítása.*

Irodalomjegyzék

- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól. In.: Magyar Közlöny. 2004. évi 203. szám.
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és bizalmi szolgáltatások általános szabályiról. Magyar Közlöny. 2015. évi, 202. szám.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Magyar Közlöny. 2011. évi 88. szám.
- 2009. évi CLV. törvény A minősített adat védelméről. Magyar Közlöny. 2009. évi 194. szám.
- 2010. évi CLVII. törvény A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről. Magyar Közlöny. 2010. évi 196. szám.
- 78/2010. (III.25.) Korm. rendelet Az elektronikus aláírás közigazgatási használatához kapcsoló követelményekről, és az elektronikus kapcsolattartás egyes szabályairól. Magyar Közlöny. 2010. évi 43. szám.
- 160/2010 (V. 6.) Korm. rendelet Az integrált ügyintézési és tájékoztatási pont kialakításáról, működtetéséről, valamint a működtető és az érintett szervek együttműködésének rendjéről. Magyar Közlöny. 2010. évi 69. szám.
- 82/2012. (IV. 21.) Korm. rendelet A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény elektronikus ügyintézéssel kapcsolatos kormányrendeleteinek módosításáról. Magyar Közlöny. 2012. évi 48. szám.
- 212/2010 (VII.1) Korm. rendelet Az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről. Magyar Közlöny. 2010. évi 111. szám.
- 2011. évi népszámlálás 3. Országos adatok. Központi Statisztikai Hivatal, 2013.
- Adatvédelmi értelmező szótár. Nemzeti Adatvédelmi és Információszabadság Hatóság. (https://www.naih.hu/adatvedelmi-szotar.html letöltés ideje: 2017.10.12.)
- Az Európai Unió Alapjogi Chartája. (2012/C 326/02) Az Európai Unió Hivatalos Lapja. (http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12012P/TXT&from=HU letöltés ideje: 2017.09.26.)
- Az Európai Parlament és a Tanács 95/46/EK irányelve. Hivatalos Lap L 281, 23/11/1995 o. 0031 – 0050.
- Az európai digitális menetrend. A bizottság közleménye az európai parlamentnek, a tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának. Brüsszel, 2010.05.19. COM (2010) 245. végleges.

- Az e-közigazgatás szolgáltatásai és használata az Európai Unióban. In.: Statisztikai Tükör. IV. évf. 134. szám. Központi Statisztikai Hivatal. 2010.
- Az e- közigazgatás előnyei. (http://allampolgar.netenahivatal.gov.hu/miert-jo-az-e-kozigazgatas/az-e-kozigazgatas-elonyei-0 letöltés ideje: 2017.09.10.)
- A közigazgatás fejlesztése. (http://vallalkozas.netenahivatal.gov.hu/miert-jo-az-e-kozigazgatas/a-kozigazgatas-fejlesztese letöltés ideje: 2017.08.08.)
- Bednay Dezső: Közigazgatási alapfogalmak. Jogi asszisztens tanfolyami jegyzet. 2011.
- Budai Balázs: Az e-közigazgatás elmélete – axiomatikus megközelítésben. In.: Információs Társadalom: Társadalomtudományi Folyóirat. 2009. évi, 9. szám.
- Budai Balázs – Tózsa István: Az e-közigazgatás elmélete. Debreceni Egyetem, Agrár- és Műszaki Tudományok Centruma. 2007.
- E-közigazgatási szabályozás 2015. Közigazgatási- és Igazságügyi Minisztérium. Budapest, 2013.
- E-tananyag. Ügyfélkapu. (https://segitseg.magyarorszag.hu/etananyag/ugyfelkapu_etananyag.html letöltés ideje: 2017.09. 28.)
- Ewa Ziemba & Iwona Obłąk: The Survey of Information Systems in Public Administration in Poland. In.: Interdisciplinary Journal of Information, Knowledge, and Management. 2014. évi 9. szám.
- Frigyesi Veronika – Dedinszky Ferenc: Az E-kormányzás az Európai Unióban és Magyarországon. In.: E-világ. 2004. évi, 4. szám.
- Horváth István: Közigazgatási szervezés- és vezetéstan. Dialog Campus Kiadó, Budapest-Pécs. 2002.
- Informatikai biztonság és kriptográfia. (http://www.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch01s03.html letöltés ideje: 2017.09.12.)
- Innovation in public administration – an operating e-state. 13 outstandingly useful public IT solutions in Hungary. Nemzeti Hírközlési és Informatikai Tanács. 2015.
- Jenei György: Közigazgatás-menedzsment. Századvég, Budapest. 2005.
- Juhász Lilla: E-közigazgatás Európában: fókuszban a közigazgatás racionalizálása és az állampolgár. In.: E-közigazgatás. 2007. évi, 1. szám.
- Kazi I. Reasul: E-Police System for Improved E-Government Services of Developing Countries. In.: Conference: 25tth IEEE Canadian Conference on Electrical and Computer Engineering, At Montreal, Quebec. 2014.

- Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia. 2014-2020. Az állami szolgáltatói modell kialakítása. 2015.
- Magyarország Alaptörvénye. Magyar Közlöny. (egységes szerkezetben) VI. cikk. 2013. évi, 55. szám.
- Mire jó az egyablakos ügyintézés. (http://kormanyablak.reblog.hu/miert-jo-az-egyablakos-ugyintezes letöltés ideje: 2017.09. 28.)
- Molnár Szilárd (kutatásvezető): Elektronikus közigazgatás. Éves jelentés 2006. BME-UNESCO Információs Társadalom és Trendkutató Központ. Budapest, 2007.
- Nyáry Mihály (szerk.): Komoly biztonsági hiba (sebezhetőség) 750 ezer észtországi digitális személyiben. (http://hirlevel.egov.hu/tag/eid/ letöltés ideje: 2017.09.23.)
- Osborne, David – Hutchinson, Peter: The Price of Government: Getting the Results Wee Need in an Age of Permanent Fiscal Crisis. Basic Books, 2004.
- Papp István: Az informatika fogalma. In.: Tudományos és Műszaki Tájékoztatás (Könyvtár- és Információtudományi szakfolyóirat) 50. évfolyam, 9–10. szám.
- Roóz József: Vezetésmódszertan. Perfekt Kiadó, Budapest. 2001.
- Simon Barbara – Budai Balázs: Elektronikus-közigazgatási modernizáció. Nemzeti Közszolgálati Egyetem. 2015.
- Shailendra C. Jain Palvia & Sushil S. Sharma: E-Government and E-Governance: Definitions/Domain Framework and Status around the World. Computer Society of India. (http://csi-sigegov.orgwww.csi-sigegov.org/1/1_369.pdf letöltés ideje: 2017.10.13.)
- Tóth Judit: A személyes adatok védelme és a közérdekű adatok nyilvánossága. Szegedi Tudományegyetem, Állam- és Jogtudományi Kar. Szeged, 2012.
- Tózsa István: Az e-közigazgatás Európában – Jelen és jövő. In.: Vezetéstudomány. 2011. évi, 3. szám.
- Zsom Brigitta: Az elektronikus közigazgatás és a területi kutatások kapcsolatáról. In.: Tér és Társadalom. 2014. évi 3. szám.

ÉRCES GERGŐ

KATASZTRÓFAVÉDELMI HÁLÓ

Absztrakt

A fenntartható fejlődés alapvető pillérei, többek között, a biztonság és az egészség. Életünk jelentős részét épített környezetben, épületekben éljük, ezért azok fenntartható és biztonságos kialakítása mára alapvető igénnyé vált. Az épületek biztonságának egyik fő területe a tűzvédelem, amely komplex módon szerves részét képzi az épületek teljes életciklusának.
A világ szinte minden országában az építészeti tűzvédelem jogszabályokon nyugszik. Tűzbiztonság-becslési módszereket, műszaki eljárásokat, kockázat-elemzéseket ismerünk a tűzvédelem tudományában, de azok nem ölelik át egy-egy épület teljes életciklusát az épület – ember – tűz hármas kölcsönhatás szempontjából, a komplex tűzvédelem: tűzmegelőzés, tűzoltás, tűzvizsgálat tekintetében. A nem komplex tűzvédelem következtében „fehér foltok", kritikus helyek és időtartamok alakulnak ki egy-egy épület tekintetében.
A közleményben az épületek teljes életciklusán átívelő komplex tűzvédelem megvalósulását elemzem. Értékelem az innovatív mérnöki szemléleten alapuló BIM alkalmazásokkal megvalósítható komplex tűzvédelemben, és az épületek teljes életciklusát lefedő katasztrófavédelmi hálóban rejlő fejlesztési lehetőségeket, amelyek által a digitális állam rendszerében, az OKOS VÁROS keretében, e-közigazgatás által megvalósítható egy új, magas szintű, hosszútávon fenntartható biztonság.

Kulcsszavak: komplex tűzvédelem, innovatív mérnöki módszerek, e-közigazgatás, okos város

Abstract

Basic pillars of sustainable development, among others, are safety and health. We spend a significant part of our lives in built environment, in buildings; therefore the sustainable and safedesign of them has become a basic need nowadays. One major area of the security of buildings is fire protection, which, in a complex way, is an integral part of the life cycle of buildings.
In almost every country of the world architectural fire protection is based on laws. We are aware of fire safety estimation methods, technical procedures, risk assessments in the science of fire protection, but they do not comprise the entire life cycle of a building in terms of building – human – fire triple interaction, nor take account of fire prevention, fire intervention, or fire investigation. On account of the non-complex fire protection become critical places and intervals in the life cycle of a building.
In the publication I analyze the implementation of complex fire protection across the full life cycle of buildings. I introduce the potential development opportunities lying in complex fire protection based on with BIM applications created innovative engineering methods, and also in disaster management net which covers the entire life cycle of buildings, which enable us to realize a new, high-level long-term sustainable safety by e-government in the system of digital state, within SMART CITY.

Keywords: complex fire protection, innovative engineering methods, e-government, smart city

1. Bevezetés

1.1. Okos ökoszisztéma napjainkban

Napjainkban az épületeink a külső, belső hőmérséklet mérésével automatikusan klimatizálják (fűtik, hűtik, árnyékolják) magukat, a hűtőnk értesítést küld, hogy melyik élelmiszerünkből mennyi fogyott vagy mikor jár le, a lakásriasztó rendszer élőképet küld az okos telefonunkra az otthoni helyzetről, és bárki a világ szinte bármely pontján kapcsolatba léphet bárkivel teret és időt áthidalva. Az okos épületek, okos eszközökön keresztül behálózzák az életünk egy jelentős hányadát. Az okos épületek és közterületi okos eszközök a saját okos készülékeinkkel egy okos ökoszisztémát hoznak létre, amely okos városok formájában manifesztálódik. Ebben a rendszerben kap létjogosultságot a biztonság új fogalma, amely a digitálisan átszőtt világunkban új minőségként kell, hogy megjelenjen. Ez az új minőség ki kell, hogy hasson a biztonság valamennyi rétegére a kritikus infrastruktúrák védelmétől az egyének személyes biztonságáig.

Ma a biztonságtechnikai rendszereink a legkülönbözőbb vezérléseket képesek végrehajtani: a lakásriasztó központ színes füsttel árasztja el a belsőteret, hogy a betörő cselekvését akadályozza, a gépjármű GPS rendszere átjelez az okos telefonokra, hogy merre található az ellopott gépjármű, a tűzjelző rendszer vezérli a tűzgátló ajtókat, hogy a tűz terjedését megakadályozza. Egy okos óra képes előre jelezni a kritikus vérnyomásunkat és pulzusunkat, amelynek köszönhetően egy szívroham még időben kezelhetővé válhat. Messze a teljesség igénye nélkül, már ebből a rövid felsorolásból is látható, hogy ma is sok különböző eszköz, rendszer áll elérhető módon rendelkezésre kényelmünk, biztonságunk és egészségünk érdekében, amely már jelen formájában is biztonság új minőségét vetíti előre.

A XXI. század embere számára a civilizáció jelenlegi fejlődési szakaszában a biztonság, egészség, fenntarthatóság kulcsfontosságú igénnyé lépett elő. Az európai életformánk és életszínvonalunk fenntartása és folyamatos fejlődése érdekében elengedhetetlen a biztonság sokrétű megvalósítása. A katasztrófavédelem a különböző típusú védelmi eszközök (életvédelem, vagyonvédelem, stb.) jelentős részében kiemelt helyet foglal el. A katasztrófavédelem fontossága megjelenik akár külső támadás esetében (terrorcselekmény során egy esetleges robbanás utáni tűzeset, bűncselekmény elkövetését, csalást leplezni kívánó szándékos tűzokozás), vagy emberi mulasztás okozta káresemények (szakszerűtlen tűzveszélyes tevékenység okozta tűzkeletkezés, tűzvédelmi szempontból fontos rendszer

karbantartásának hiánya, stb.), vagy egy-egy természeti katasztrófa okozta káresemények során is. Gyakorlatilag az általános biztonság terén az egyik legszélesebb spektrumban játszik szerepet, így széles körű alkalmazása nem elhanyagolható a mai társadalomban.

A tanulmány gondolatkísérlet formájában elemzi a napjainkban zajló információs forradalom nyújtotta fejlődésre építve az átfogó védelmi igazgatás e-közigazgatás kereteiben fejleszthető lehetőségeit. A katasztrófavédelem speciális kereteiben kísérletet tesz a tézisek igazolására, a fejlesztés reális megvalósításának tényszerű, gyakorlatban, mai eszközökkel is kialakítható lehetőségeire. Alapot kíván teremteni a fejlesztés aprólékos és mélységében megvalósítható és összefüggéseiben rendszerként alkalmazható részlet megoldásaihoz, amelyeket összegez, keretként előre vetít, hogy általánosítva a biztonság valamennyi szegmensére kiterjeszthető legyen.

1.2. Hipotézis

I. A biztonság a digitális állam nyújtotta keretek között, a digitális infrastruktúra nyújtotta lehetőségekkel élve, és digitális kompetenciák alkalmazásával az e-közigazgatás útján egy új, a jelenleg megvalósulónál magasabb minőséget képes elérni.

II. Az okos városok rendszerébe integrált épület információs modellezés (továbbiakban: BIM) alapon működő, térinformatikai hálózatot alkalmazó katasztrófavédelem egy új, minden eddiginél átfogóbb biztonsági szintet képes nyújtani, és egy katasztrófavédelmi hálóként képes lefedni a biztonság ezen teljes szegmensét.

III. A katasztrófavédelmi hálóba integrált, e-közigazgatás keretében megvalósuló innovatív mérnöki módszereken alapuló alkalmazások képesek lefedni egy-egy épület teljes életciklusára vetítve a biztonság teljes szegmensét: a tervezéstől a kivitelezésen át, a használaton és esetleges felújításokon keresztül a végleges elbontásig.

IV. Az egyes épületek életciklusában résztvevő szereplők (civilek: beruházók, tervezők, kivitelezők, stb. és a hatóságok: pl. katasztrófavédelem, továbbá a biztonságért felelős hivatásos szervek, önkéntesek, stb.) a katasztrófavédelmi háló keretében folyamatosan egy térben és időben tervezhetik, kivitelezhetik, épületfelügyelet keretében monitoringozhatják, hatósági eljárás keretében ellenőrizhetik, beavatkozás során információt nyerhetnek, stb. az adott épületről.

V. Az egyes BIM alapon megtervezett egyes épületek összessége, az adott településszövetben egy kiterjesztett térinformatikai struktúrában az okos város biztonsági faktorát szolgálja, és a

katasztrófavédelem hatékonyságát mind a megelőzés, a beavatkozás és az elemzés fázisában növeli.

VI. A fenti elveken alapuló katasztrófavédelmi háló kiépítése egy olyan adatbázis felállítását képes létrehozni, amely valós eredményekkel szolgálja a továbbfejlődés lehetőségét, terjeszti ki az innovatív mérnöki módszereken nyugvó műszaki megoldások összességét, hogy a biztonság növelése folyamatos lehessen.

1.3. A tanulmány célja

Jelen tanulmány célja tudományos úton igazolni a felvetett hipotézisek relevanciáját, továbbá az így kapott új eredményekkel segíteni a katasztrófavédelem, és ezáltal az általános biztonság, a védelmi igazgatás fejlesztését, a digitális ökoszisztémába történő hatékony integrálását, a biztonságot szolgáló infokommunikációs képességek növelésével.

2. Digitális ökoszisztéma

2.1. Európai Digitális Menetrend

A digitális ökoszisztéma megvalósításának alapját az Európai Bizottság 2010-ben bemutatott „Európa 2020” stratégia határozta meg. Az EU hét kiemelt kezdeményezést alakított ki, ezek közül az egyik legfontosabb az Európai Digitális Menetrend, amely az információs és kommunikációs technológiák alkalmazásának minél szélesebb körű előmozdítását célozza. A katasztrófavédelem nyújtotta biztonság minőségi fejlesztése is ezen infokommunikációs technológiák alkalmazásán nyugszik.

Európai Digitális Menetrend alappillérei:

1. egységes digitális piac
2. átjárhatóság megteremtése
3. bizalom és biztonság erősítése
4. nagy sebességű és szupergyors internet-hozzáférés
5. kutatás fejlesztés erősítése (http://digitalismagyarorszag.kormany.hu/europai-digitalis-menetrend)

2.2. Digitális Magyarország

„A hazai informatikai és távközlési szektor fejlesztésének stratégiai irányait, fejlesztési súlypontjait a 2014-20-as időtávra vonatkozóan az uniós elvárásokkal is összehangolt

Nemzeti Infokommunikációs Stratégia (illetve az erről szóló 1069/2014. (II.19.) Korm. határozat) és Zöld Könyv jelöli ki. A stratégia megvalósításának akciótervi kereteit a Digitális Nemzet Fejlesztési Program (1631/2014. (XI. 6.) Korm. határozat) rögzíti.

A Nemzeti Infokommunikációs Stratégiában (NIS) megfogalmazott törekvések végső célja a Digitális Magyarország létrehozása, amely a kormányzat, az intézményi és a piaci szereplők közös szerepvállalásával valósul meg. (http://digitalismagyarorszag.kormany.hu/digitalis-magyarorszag)

A program 4 fő alappillére:

1. szupergyors internet
2. digitális közösség és gazdaság
3. e-közszolgáltatások
4. digitális készségek

A katasztrófavédelmi háló a fenti alappillérekre illeszkedve terjeszti ki az e-közigazgatás keretében a biztonság dimenzióit.

Ehhez fel kell állítani egy alap feltételrendszert, amelyet a NIS az alábbi rendszer felépítésével céloz megvalósítani:

- Digitális infrastruktúra: a digitális szolgáltatások nyújtásához és igénybevételéhez szükséges sávszélességet biztosító elektronikus hírközlési infrastruktúra rendelkezésre állása a hálózat valamennyi szegmensében (gerinc-, felhordó- és helyi hálózat);
- Digitális kompetenciák: a lakosság, a mikro- és kis –és közepes vállalkozások, illetve a közigazgatásban dolgozók digitális kompetenciáinak fejlesztése, az elsődleges (digitális írástudatlanság) és másodlagos (alacsony szintű használat) digitális megosztottság mérséklése, a mikro- és kisvállalkozások és a közigazgatásban dolgozók képessé tétele az IKT rendszerek bevezetése által előálló üzleti lehetőségek felismerésére és kihasználására, illetve a tartósan leszakadók részesítése a digitális ökoszisztéma előnyeiből (e-befogadás)

- Digitális gazdaság: egyrészt a szűkebben értelmezett IKT szektor, másrészt az általa biztosított elektronikus (kereskedelmi, banki stb.) szolgáltatásokat igénybe vevő vállalkozások külső és belső informatikai rendszereinek fejlesztése, illetve az IKT-fejlesztésekre és az IKT-n alapuló fejlesztésekre irányuló kutatás-fejlesztési és innovációs tevékenység ösztönzése

- Digitális állam: a kormányzat működését támogató belső IT, a lakossági és vállalkozói célcsoportnak szóló elektronikus közigazgatási szolgáltatások, illetve az állami érdekkörbe tartozó egyéb elektronikus (pl. egészségügyi, oktatási, könyvtári, kulturális örökséghez kapcsolódó vagy az állami adat- és információs vagyon megosztását célzó) szolgáltatások, valamint e szolgáltatások biztonsági hátterének biztosítása. (http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf)

2.3. Digitális állam

Az alapvető biztonság „digitalizálása” kizárólag ellenőrzött és a közigazgatás keretrendszerén belül képzelhető el, amelyhez egyedüli platformot a digitális állam képes biztosítani.

A NIS-ban megfogalmazott törekvések végső célja a Digitális állam létrehozása a kormányzat, az intézményi és a piaci szereplők közös szerepvállalásával valósul meg. Ebben a halmazban foglal el a biztonság részhalmazában egy jelentős területet a katasztrófavédelem, amely részben már a szolgáltató állam keretein belül integrálódott az e-közigazgatásba, de még messze nem teljesült ki olyan módon, hogy a tűzbiztonság, katasztrófavédelem szintjét a komplex tűzvédelem, a digitálisan átfogó katasztrófavédelem megvalósulása irányába jelentős mértékben elmozdította volna. Alapvető feltételként természetesen meg kell jelennie a rendszeren belüli interoperabilitásnak, valamint az egységes szabványokon nyugvó megoldásoknak.

A NIS alapján, a digitális állam infrastruktúrájának, az internet nyújtotta virtuális rendszernek köszönhetően kialakítható egy a komplex katasztrófavédelmet lefedő katasztrófavédelmi háló, amely az e-közigazgatás keretében működik szabályozott módon.

2.4. E-közigazgatás

A katasztrófavédelem, mint a hatályos közigazgatásban szereplő, hatósági és szakhatósági hatáskörökkel ellátott szervezet a belügyminisztérium alá tartozó hivatásos szervként már napjainkban is részese az e-közigazgatásnak.

A katasztrófavédelem három szinten szerepel az elektronikus közigazgatásban:

I. országos szint – központi szerv – BM Országos Katasztrófavédelmi Főigazgatóság

II. megyei szint – területi szerv – fővárosi- és megyei katasztrófavédelmi igazgatóságok

III. térségi szint – helyi szerv – katasztrófavédelmi kirendeltségek (65 db.) (Muhoray, 2016)

Valamennyi szinten megjelenő elektronikus eljárás például az építésügyi hatósági engedélyezési eljárásokat támogató elektronikus dokumentációs rendszerben (ÉTDR) történő engedélyezési eljárás. Az államigazgatásban a katasztrófavédelem is integráltan alkalmaz egyes szabályozott elektronikus ügyintézési szolgáltatásokat (SZEÜSZ).

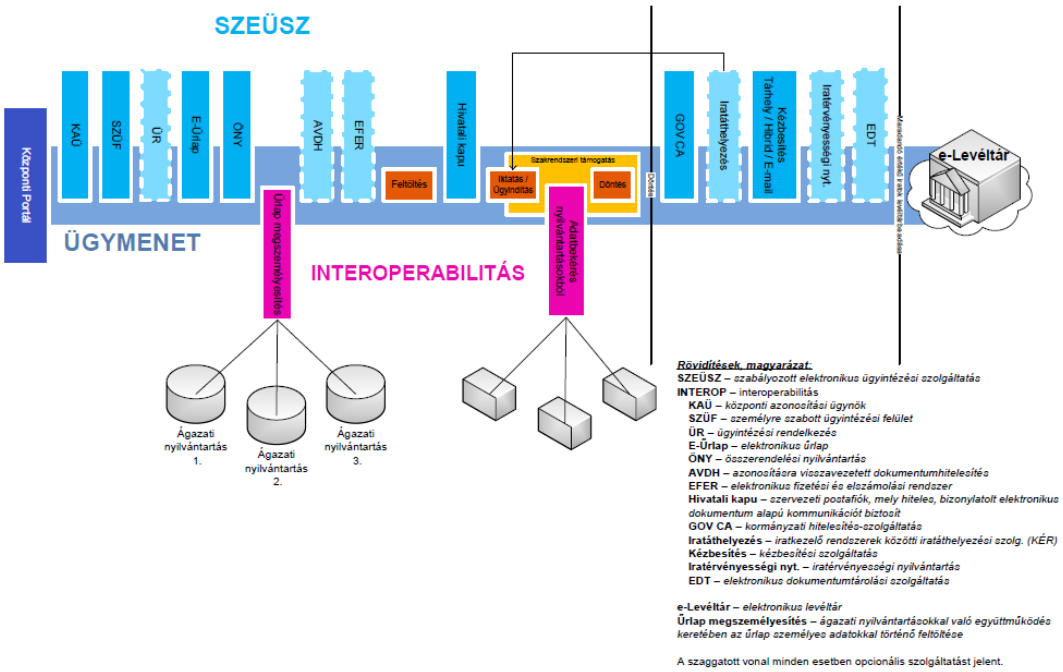
Az elektronikus közigazgatás az elektronikus közigazgatás kiterjesztésével kapcsolatos feladatokról szóló 1743/2014. (XII. 15.) Korm. határozattal a Kormány döntést hozott az e-közigazgatás fejlesztésének fő sarokpontjairól.

A NIS négy pillére (digitális infrastruktúra, kompetenciák, gazdaság és állam) mentén történő digitalizációnak központi eleme egy olyan kormányzati szolgáltatási platform, mely minden szereplő számára egységes logikai rendszerben kiépült hálózati és kormányzati adatközponti infrastruktúrán, szabványosított kapcsolórendszereken elérhető szakrendszerek csatlakozásával, szabályozott elektronikus szolgáltatások igénybevételét, összefoglalóan korszerű elektronikus közigazgatás elérését biztosítja. (http://www.kormany.hu/download/0/05/50000/E-k%C3%B6zigazgat%C3%A1si_keretrendszer_koncepci%C3%B3.pdf)

Az e-közigazgatás kiterjesztéséhez és a biztonsági rendszerek széleskörű működtetéséhez kormányzati adatközpontok működtetésére van szükség, amely képes az átfogó felhő alapú szolgáltatások kezelésére. Ezzel a Belügyminisztérium a NISZ Zrt. bízta meg elsődleges szolgáltatóként. A rendszer felépítéséhez napjainkra tehát minden alapfeltétel adott.

2.5. Összegzés

A fentiek alapján a kitűzött célok megvalósítása esetén a rendszer alkalmas egy új biztonsági szintet nyújtani, amely megfelelő komponensek esetében a katasztrófavédelem szakterületére vetítve egy új minőséget hozhat létre. A komponensek és minőségi paraméterek megalkotásával a biztonság a digitális állam nyújtotta keretek között, a digitális infrastruktúra nyújtotta lehetőségekkel élve, és digitális kompetenciák alkalmazásával az e-közigazgatás útján egy új, a jelenleg megvalósulónál magasabb minőséget lesz képes elérni, olyan módon kiterjesztett módon, amelyre jelenleg még nincs lehetőség.



1. ábra elektronikus ügyintézés sematikus ábra: http://www.kormany.hu/download/0/05/50000/E-k%C3%B6zigazgat%C3%A1si_keretrendszer_koncepci%C3%B3.pdf

3. Komplex katasztrófavédelem

3.1. Számítógéppel segített tervezés

A biztonság kialakítása a katasztrófavédelmi kérdésekben, azonos módon bármely más szakterület tekintetében, a tervezéssel kezdődik. A tervezés napjainkra számítógéppel segített tevékenység formájában történik.

A számítógéppel segített tervezés ma a digitális állam kereteiben az e-közigazgatásban válik hatósági aktussá. A különböző építési eljárások engedélyezése ma teljes egészében elektronikus úton történik az ún. építésügyi hatósági engedélyezési eljárásokat támogató elektronikus dokumentációs rendszerben (ÉTDR). Ezáltal egy-egy épület engedélyezési fázisaiban a heterogén komplex tűzvédelem egyes szereplői a virtuális térben egy-egy rövid időintervallumban találkoznak.

A jövőkutatás szerint a nem oly távoli jövőben 2020-2030-ra az okostelefonokat szupertelefonok váltják, amik a szenzorok által szinte minden emberi érzékszervet képesek lesznek helyettesíteni. A körülöttünk lévő teret valóságos 3D-ben tapogatják le, érzik majd az

ízeket, azonosítják a hangok forrását és azok távolságát, sőt mérik a vérnyomásunkat, a közvetlen környezetünk fizikai paramétereit, a levegő minőségét, a hőmérsékletet, stb. (Maliosz, 2016)

A szenzorok mögött intelligens, fejlődni képes számítógépes rendszerek - hatalmas adatelemző szerverek állnak majd. Digitális okoseszközeinkkel a mai kijelzőknél sokkal természetesebb módon, kiterjesztett és a virtuális valóságban (AR és VR) tartjuk majd a kapcsolatot, valamint kép- és hangutasításainkat is tökéletesen megértik majd. (Maliosz, 2016)

A fenti nem oly távoli jövő biztonságos felhő alapú rendszerként valósulhat meg. Ebbe a rendszerbe, a fenti elveken kell integrálni az új komplex tűzvédelmet, amely a digitális állam keretein belül, a korszerű infokommunikáció alkalmazásával, az innovatív mérnöki szemlélet mellett, képes lenne a tűzvédelmi biztonság eddig volt legmagasabb minőségét elérni. Ezzel valósulna meg az új komplex tűzvédelmi minőség, a teljes életciklust lefedő katasztrófavédelmi háló.

3.2. Épületinformációs modellezés (BIM)

A fenti rendszer valóságos jelenléte kézzel fogható, egy-egy épület teljes életciklusát tekintve az épületek életciklusának kezdeténél. Gyakorlatilag az épületek tervezése, a tervek feldolgozása ma már digitális rendszerekkel, számítógépes szoftverekkel történik. Ezek az építészeti és egyéb kiegészítő szoftverek képesek a három dimenziós (3D) virtuális tér megalkotására, olyan módon, hogy a 3D elemek intelligensen hordoznak információkat az épületről. „A BIM, épületinformációs modellezés folyamata tulajdonképpen egy szemléletmódot jelent, mely az építési folyamat komplett egészét egységként kezeli, az épület tervezésétől a kivitelezés végéig (vagy még annál is tovább, az üzemeltetésig). A BIM egymást kiegészítő megoldások hatékony készletével jeleníti meg és szimulálja a projekteket, teszi hatékonyabbá a dokumentálást és a rajzolást, kezeli az adatokat, és segíti elő a projektekben részt vevő személyek együttműködését. Számos előnyt biztosít a projekt teljes élettartama során a tervezők, kivitelezési szakemberek és tulajdonosok számára.” (Fritts, 2016) Az egyes épületelemek, szerkezetek információkat hordoznak, amelyek segítik a tervezés folyamatát, és képesek arra, hogy a hordozott információkat tovább örökítsék. Az épített terek három dimenziósak, csakúgy, mint a tűz jelensége, ezért a 3D tervezés,

modellezés kompatibilis elvek alapján működhet, és kellene is, hogy működjön. El kell felejteni a 2D-ben történő gondolkodást mind a tervezői, mind a hatósági, szakhatósági oldalon, mert a valóság 3D. Ezt a tényleges térben történő tervezést és ellenőrzést nagymértékben elősegítik a már most rendelkezésre álló szoftverek. Képesek 3D metszetek felvételére, amelyeken látható a teljes épület mélységében átmenő tűzszakaszolás, amely sosem egy-egy vízszintes és/vagy függőleges vonal csak, hanem 3D-ban tört folytonos síkok kapcsolatrendszere, amely tereket határol. A tűzterjedés mérnöki szemléletű elemzése már ebben a tervezési fázisban meg kellene, hogy történjen, és a fenti eszközök és módszerek alkalmazásával könnyedén meg is történhet. Az építészeti modell megfelelő adaptálásával, a hő-és füstelvezetést, vagy a kiürítést szimuláló szoftverek képesek lesznek és részben képesek ma is a hordozott információk felhasználásával egy a valósághoz hasonlító szimulált jelenség leképzésére, ezáltal a tervezés és a mérnöki gondolkodás kiszélesítésére. Minden szereplő számára megkönnyíti, és nagymértékben pontosítja a megfelelő tűzvédelem megvalósulását a rendelkezésre álló szoftveres lehetőségek alkalmazása.

Mára egyértelművé vált, hogy a mérnöki módszereknek nevezett eljárások csak részeredményeket szolgáltatnak, egy olyan részrendszerben, amelyben konkrétan vizsgálat alá kerültek, de önmagukban nem nyújtanak teljes megoldást egy-egy adott egyedi problémára, és ezért nagymértékben hozzájárulhatnak a hamis biztonságérzet megvalósításához.

3.3. Innovatív mérnöki módszerek

Egy meghatározott módon elvégzett valós tűzteszt (pl.: homlokzati hőszigetelés tűzterjedési vizsgálata) az adott térbeli kialakítási problémát kezeli, de minden egyedi épületre ugyanaz a rendszer más-más beépítési helyzetben, térbeli kialakításban csak közelítően értékelhető ugyanolyan módon. (Kerekes, 2008) Felhasználva a valós tűzteszt eredményeit - megfelelő modell tűz választása esetén - (Szabó, Beda, 2014) és a BIM (épület információs modellezés) alapú tervezés térbeli információit, a ma már rendelkezésre álló és rohamosan fejlődő szimulációs szoftverekkel rendelkezésre áll az a képesség, amellyel tervezhetővé válik a fenti probléma megoldása. Ez természetesen minden egyedi kialakítás esetében egyedi megoldásokat takar, több mérnöki módszer megfelelő alkalmazását követeli meg és egy értékelő-elemző összegzésben ölt végleges formát, amellyel igazolhatóvá válik a tűzvédelmi követelménynek való megfelelés. A mérnöki módszerek tudatos és innovatív alkalmazása egységes szemléleten és közel azonos mértékű tudáson alapuló szakember gárdát igényel,

mind a hivatásos, mind a civil szféra szereplőitől. Ezt nagyon alapos és célirányos szakmai képzéssel lehet elérni. **Az innovatív mérnöki módszer tehát egy összefüggés rendszer, újfajta szemléletmód, amely az adott egyedi tűzvédelmi problémára úgy ad egyedi megoldást, hogy a szükséges mértékben a szükséges mérnöki módszereket vegyíti, egymásra hatásukat elemzi és a tapasztalati, mért eredményekkel összehasonlítva összegzi, értékeli az épület kritikus helyén, egy-egy kritikus időpontban, vagy intervallumban.**

Az innovatív mérnöki módszerek alkalmazásával lehetőség nyílik egy épület életciklusa során a kritikus helyek és potenciálisan tűzveszélyes időszakok meghatározására, ezáltal a megfelelő biztonság kialakítására. Ez a biztonság szolgálja a tűzoltói beavatkozás speciális helyszíni biztonságát is. (Bérczi, 2012) A kritikus helyek meghatározásával egy új típusú, mérnöki módszerekkel igazolt használat tervezhető a potenciálisan kockázatos időintervallumokra. A jogszabályokon nyugvó statikus (csak a jogszabályváltozástól függő szabályozás) használati szabályok helyett új szemléletű **dinamikus használati szabályozás** alakítható ki.

3.4. Katasztrófavédelmi követelményeknek való megfelelés

A tűzvédelem fenti átalakításához mérnöki módszerek alkalmazására lesz szükség, olyan innovatív mérnöki módszerekre, amelyekkel képesek leszünk az információ fogadására, feldolgozására, a döntések előkészítésére, és a leggyorsabb és legmegfelelőbb reakciók megadására. Ez a folyamat ma már számítógépek támogatása nélkül elképzelhetetlen. Az épített környezetünket gyakorlatilag olyan módon kell ellátnunk, szabályozott módon, már a tűzmegelőzés korai fázisában, hogy az érzékelések lehetővé tegyék a fenti folyamatok lezajlását. Ez azt jelenti, hogy a tervezésnél figyelembe kell venni azokat az érzékelési, vezérlési lehetőségeket, amelyek a passzív tűzvédelem aktív módon történő alkalmazását teszik lehetővé. Ez azt jelenti, hogy BIM rendszerben információkkal és képességekkel felruházott szerkezeti elem, pl. fal, amely tűzgátló alapszerkezetként, pl. tűzgátló falként kerül kialakításra az épület teljes életciklusa alatt aktív módon, mért rendszerben helyezkedik el, és szükség esetén a benne lévő nyílások, átvezetések, stb. alkalmazkodnak a tűz kialakuló jelenségéhez. Ez több annál, mint amit ma egy egyszerű intelligens beépített tűzjelző berendezéssel kihasználunk. Olyan információkat lesz képes eljuttatni egy ilyen aktív módon alkalmazott passzív tűzvédelmi eszköz, amely információt nyújt a beavatkozó állomány

részére is, hogy mekkora hőmérséklettel, milyen mértékben kiterjedt tűzzel, a tűzfejlődés mely szakaszával, az épületszerkezet állékonyságának melyik fázisával kell, hogy szembesüljön a tűzoltás során. A tűzoltás-vezető már a vonulás során távolsági felderítéssel okoseszközén keresztül megszerezheti a fenti információkat, így a beavatkozás biztonsága és a beavatkozás hatékonysága a lehető legmagasabb szintet érheti el. Hosszútávon és fenntartható módon ez a kombináció teszi leghatékonyabbá és leggazdaságosabbá a tűzvédelmet. (Érces, 2016)

Világszerte elfogadott és működő módszer a tűzvédelemi problémákra adott megoldások jogszabályi követelménnyel való összehasonlítása. (Bérczi, 2012) Ezáltal sok esetben megállapítható, hogy az ismert tűzvédelmi paraméter megfelel-e az ismert követelmény értéknek vagy nem. Azonban ez a szótár jellegű módszer csak a meghatározott problémákra ismer válaszokat és a problémák összetettsége is véges lehet. Messze nem fedi le az építészeti tűzvédelem összetett jellegét, nem tudja követni a kortárs építés technikai fejlődését. Sok esetben a rendelkezésre álló technika – akár egy szoftver, akár egy műszaki termék esetében – fejlettsége előre mutatóbb a rugalmatlan jogi szabályozásoknál. Mérnöki szemléleten alapul a fenti módszer fejlesztése, amely során követelményeknek való megfeleltetés műszaki irányelvek, műszaki szabványok felhasználásával biztosított. Ezen módszerrel jelentősen nő a mozgástér, a tervezés, megvalósítás szabadsága, de még mindig egy keretrendszerben mozoghat csak a módszer alkalmazója. Ma ez a módszer a legelterjedtebb, és optimálisan a legjobban használható. Ezt a módszert alkalmazzák Európa több országában (harmonizált szabványok alkalmazása), közte Németországban (DIN, VDS rendszer), vagy Magyarországon (harmonizált szabványokon alapuló tűzvédelmi műszaki irányelvek alkalmazása), továbbá az Amerikai Egyesült Államokban is hasonló rendszer működik (NFPA, FM szabványok alkalmazása). (Zellei, 2013) Léteznek úgynevezett komplex tűzvédelmi értékelések, amelyek szintén mérnöki elveken nyugszanak, és műszaki szemlélettel kezelik az adott tűzvédelmi problémákat komplex módon is, de nem kezelik egy épület teljes életciklusán keresztül. A jövőt a szabályozott mérnöki szemléleten és alapokon működő módszerek jelentik, amelyek kombinált alkalmazásával minden egyedi problémára a legmegfelelőbb egyedi megoldás biztosítható olyan módon, hogy egy épület teljes életciklusára vetítve átfogó képet kapjunk annak tűzvédelmi helyzetéről, a kritikus helyek és potenciálisan kockázatos időszakok figyelembevételével. A mai magyar tűzvédelmi szabályozás előremutató és modern módon, mérnöki szemléleten alapulva lehetővé teszi a

fenti fejlődés biztosítását. Ehhez azonban a már megkezdődött szemléletváltást ki kell terjeszteni, szélesíteni és fel kell gyorsítani, hogy rendelkezésre álljon egy stabil, egységes gondolkodásra képes, kreatív szakembergárda, amely lefedi a komplex tűzvédelmet.

3.5. Épület – ember – tűz

A világ szinte minden országában az építészeti tűzvédelem jogszabályokon, irányelveken, szabványokon nyugszik. Tűzbiztonság-becslési módszereket, műszaki eljárásokat, kockázat-elemzéseket ismerünk a tűzvédelem tudományában, de azok nem ölelik át egy-egy épület teljes életciklusát az épület – ember – tűz hármas kölcsönhatás szempontjából, a komplex tűzvédelem: tűzmegelőzés, tűzoltás, tűzvizsgálat tekintetében. (Beda, 2004) A nem komplex tűzvédelem következtében „fehér foltok", kritikus helyek és időtartamok alakulnak ki egy-egy épület esetében. (Beda, 1999) **A tűzvédelem több szempontból is heterogén, több szereplős, nagy időintervallumot folyamatosan átívelő, térben több helyen lejátszódó folyamat, amely kritikus, potenciálisan tűzveszélyes helyekkel és időpontokkal egy térbeli-időbeli mátrixot alkot.**

A biztonság szempontjából az épület-ember-tűz hármas viszonya játssza a legfontosabb szerepet. Külön-külön ismerjük azokat a paramétereket, amelyek definiálják a tűzvédelemben mérhető biztonságot az adott tényezők esetében. A probléma ott rejtőzik, hogy ezek valós egymásra hatása sok esetben bizonytalan módosító tényezőket, jellemzően rontó tényezőket eredményez. Egy takarítás során, a takarító felszerelést hordozó kocsival kitámasztott, alapvetően szabályos, önműködő csukó szerkezettel ellátott tűzgátló ajtó nem képes betölteni szerepét, ezáltal a tűz több tűzszakaszba történő terjedése lehetővé válik (emberi tényező). Egy elhúzódó építészeti átalakítás során az elbontott, de időközben vissza nem épített tűzgátló szerkezetek (falak, födém, stb.) hiánya ugyancsak a tűz gyors terjedését eredményezi (épület tényező). Az épület használata során felhalmozott éghető berendezések, installációk, tárgyak, anyagok égése során felszabaduló toxikus gázok, égéstermékek szintén negatív értelemben befolyásolják az épület tűzvédelmi helyzetét (Beda, Kerekes, 2006), ami kihat többek között az épületben tartózkodó emberek menekülési képességére, amelyet a tervezéskor nem tudtak, vagy nem vettek figyelembe (tűz tényező).

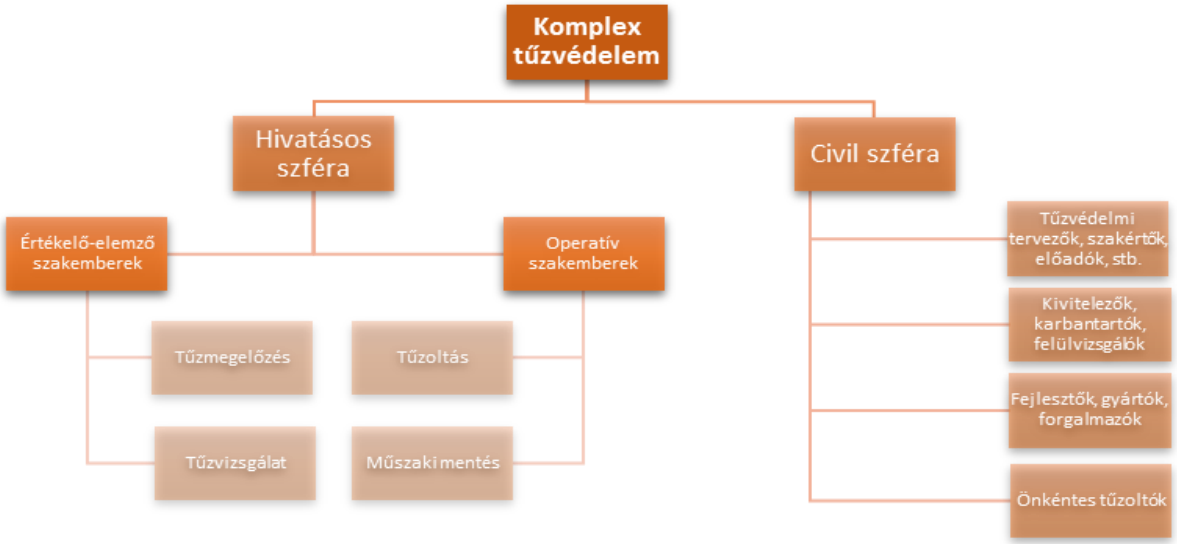
Az egyszerű példákból is látható, hogy egy épület használata során az emberi tényező a legbizonytalanabb, amelyre egzakt mérnöki megoldás nem adható. Az egyetlen reális megoldás az emberek tudatos és folyamatos tűzvédelmi képzése, oktatása már kisgyermek

kortól egészen idős korig. Ezáltal egy automatizmus alakul ki, amely kedvezően hatna a nem szándékos gondatlan cselekvések elkerülése tekintetében. Mérnöki megoldások szempontjából az épület- és a tűz tényező kezelése már egyszerűbb probléma, mert léteznek egzakt megoldások. (Buchanan, 2001) A problémát ezen tényezők esetében az egymásra hatások megfelelő elemzésének és értékelésének hiánya okozza, amely a jellemzően heterogén és hosszú életciklusból és a tűzvédelem szereplőinek különböző tér- és időbeni elhelyezkedéséből fakad.

3.6. Tűzvédelem szereplői

A szereplők összetétele szintén heterogén. Alapvetően két részre osztható: hivatásos és civil tűzvédelmi szakemberekre. A hivatásos szakember teamnek két kategóriáját különböztetjük meg: az értékelő-elemzőt és az operatív teamet, amelyek további három fő alcsoportra, szakterületre bonthatók: tűzmegelőzési, tűzoltási és tűzvizsgálati szakterületre.

A civil tűzvédelemi szféra négy csoportból áll: a tűzvédelmi tervezők, szakértők, tűzvédelmi előadók, főelőadók; a kivitelezők, karbantartók, felülvizsgálók; a fejlesztők, gyártók, forgalmazók; és az önkéntes tűzoltók csoportjából. Az egyes csoportokon, alcsoportokon belül további specializálódás figyelhető meg, amely tovább erősíti a heterogén tűzvédelem megvalósulását.



2. ábra Komplex tűzvédelem szereplői (saját szerkesztés)

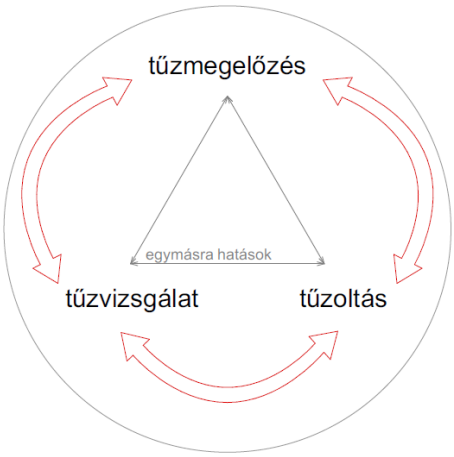
A komplex tűzvédelem három alappilléren (három speciális szakterület) nyugszik:

1. tűzmegelőzés

2. tűzoltás

3. tűzvizsgálat. (1996. évi XXXI. törvény)

A három szakterület a gyakorlati alkalmazás terén jelenleg elkülönül, de a hármas egység körkörös, oda-vissza alapon történő egymásra hatása szakmai szempontból megbonthatatlan. A korszerű tűzoltóság ezen hármas egység megvalósításával védekezik leghatékonyabban a tűzesetek ellen.



3. ábra A tűzvédelem hármas egymásra hatása (saját szerkesztés)

A tűz elleni védekezésben részt vevő szereplők a gyakorlatban két nagy csoportra bonthatók:

1. hivatásos tűzoltóság (katasztrófavédelem különböző szintű szervezeti egységei)

a) központi szint

b) területi szint

c) helyi szint

2. civil szféra szereplői

a) tűzvédelmi mérnökök, szakmérnökök, szakértők, főelőadók, előadók, stb.

b) adott létesítményben a tűz elleni védekezésért felelős személyek

ba) ügyvezető, üzemeltető, vagy megbízottjaik

bb) biztonsági személyzet (tűzjelző-, tűzoltó berendezés felügyeletét ellátó személyzet)

bc) tűzvédelmi szolgáltatást ellátók (üzembe helyezők, karbantartók, felülvizsgálók)

c) tűzvédelmi eszköz forgalmazók, gyártók.

A tűzvédelem, a biztonság megvalósítása terén betöltött súlyának megfelelően, szerteágazóan és több szinten valósítható meg. A több szintű megvalósítás egy-egy védeni kívánt épített környezeti elem (építmény, épület) esetében különböző időbeli periódusokban jelenik meg. (Ziebs, 2014) A különböző időintervallumokban különböző szereplők vesznek részt, amelyek között léteznek átfedések, de bizonyos időpontok egy épített környezeti elem esetében teljesen elkülönülnek, nem valósul meg a tűzvédelem teljes folytonossága. Egy, a mai elvárásoknak eleget tevő, ötven évre tervezett építmény életét nem fedi le egy teljes egészében átívelő, egységes tűzvédelmi védőháló.

4. Épületek tűzvédelmi életciklusa

4.1. Egy építmény életének ciklusai

1. építési szándék, koncepció – tűzvédelmi koncepció (tűzvédelmi tervező, szakértő)

2. tervezési fázis – tűzvédelmi tervezés (tűzmegelőzést végző hivatásos tűzoltó állomány tagja, tűzvédelmi tervező)

3. kivitelezési fázis – tűzvédelem érintőlegesen jelenik meg, vagy hiányzik (a kivitelezésben részt vevő tűzvédelmi képesítéssel rendelkező személy)

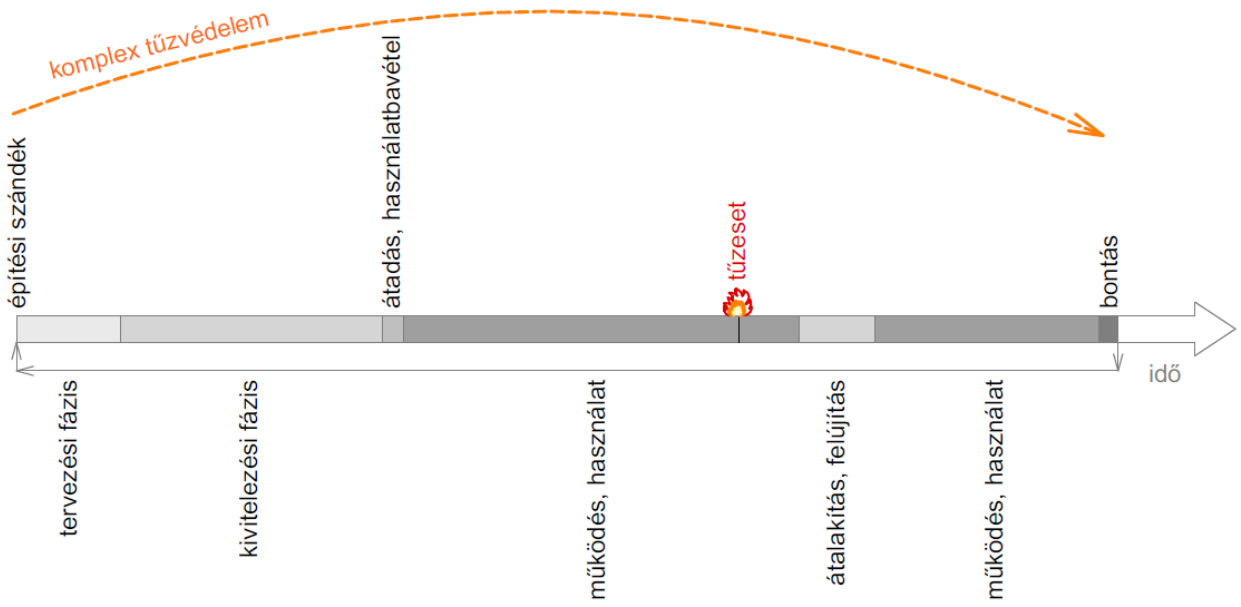
4. használatbavétel, építmény átadása – jellemzően a legjobb (pillanatnyi) tűzvédelmi állapot (tűzvédelmi képesítéssel rendelkező felelős személy, tűzmegelőzést végző hivatásos tűzoltó állomány tagja)

5. használat, működés – tűzvédelem csak bizonyos esetekben jelenik meg, csak specifikus területeken (tűzvédelmi képesítéssel rendelkező szakember: pl. tűzvédelmi előadó, főelőadó, karbantartók, stb, tűzmegelőzést végző hivatásos tűzoltó állomány tagja ellenőrzés keretében, beavatkozó hivatásos tűzoltó állomány gyakorlat keretében)

6. átalakítás, felújítás, rendeltetés megváltoztatás – tűzvédelmi rendszerekben történő változás, de nem minden esetben tűzvédelmi tervezés (átalakítás körében és mértékében a tűzmegelőzést végző hivatásos tűzoltó állomány tagja, megfelelő tűzvédelmi képesítéssel rendelkező szakember)

7. bontás – tűzvédelem nem jelenik meg

+ esetleges tűzeset valamelyik ciklusban, vagy ciklusok közötti átmeneti állapotban (tűzoltást, tűzvizsgálatot, tűzvédelmi ellenőrzést végző hivatásos tűzoltó állomány, tűzvizsgálati szakértő, igazságügyi szakértő) (Érces, Restás, 2017)



4. ábra Az épület teljes ciklusán átívelő komplex tűzvédelem (saját szerkesztés)

Egy építmény teljes élete során a fő ciklusok idején komplex tűzvédelem sok esetben a szakterületek és szereplők terén párhuzamosan, metszéspont(ok) nélkül valósul meg, amely a teljes tűzvédelem folytonosságán szakadásokat, fehér foltokat eredményez.

Az eleve összetett építészeti tűzvédelmi tervezésben megjelennek az automatikus beépített aktív tűzvédelmi berendezések, amelyek szerepet játszhatnak akár a tűzterjedés elleni védelemben is, úgy, hogy azok működését egy automatikus beépített tűzjelző rendszer vezérli. Azaz egy alapvető építészeti tűzvédelmi kérdésre -tűzterjedés elleni védelem- egyszerre három szereplőnek kellene összehangolt választ adnia: tűzvédelmi tervező, beépített automatikus oltóberendezés (tűzterjedés gátló berendezés) tervezője, beépített automatikus tűzjelző rendszer tervezője. Mivel valamennyi rendszer építési terméknek számít, ezért már a termék kiválasztásánál jelentős szerepet játszik annak tűzvédelmi teljesítménye, minősítése, amelyet a fejlesztők, gyártók határoznak meg és igazolnak. A teljes folyamatot felügyeli a hivatásos szféra legalább két szempontból: hatósági (azon belül engedélyezési, piacfelügyeleti) és szakhatósági formában. Ezt az egyetlen tűzterjedési problémát tekintve is jól látható, hogy milyen bonyolult és összetett ma a tűzbiztonság megvalósítása. A fenti szereplők egyszerre nincsenek egy térben és időben, és jellemzően a különböző szereplőkön belül is több különböző szakember jár el, így az információ áramlás homogenitása hiányos, ezért hibahelyek alakulnak ki. Egyik szereplő nem tudja pontosan, hogy mit csinál a másik, ezért fontos adatrészletek vesznek el, és végeredményben egy egyszerűnek tűnő tűzterjedés elleni védelem nem lesz képes ellátni megfelelően a feladatát. Ezáltal jelentősen megnő a beavatkozó tűzoltó állomány helyszíni döntéshozatali kényszere, amely sok esetben nem az adott épület mérnöki tűzvédelmi paraméterein alapszik, ezért eltér attól, és így megnövekedhet a beavatkozás ideje, ezáltal a tűzkár. (Restás, 2013) Összességében tehát az a probléma akár egy ilyen egyszerű esetben is, hogy hajlamosak vagyunk elhinni, hogy sok pénzért, sok szakember bevonásával biztosan megfelelő védelmet építettünk ki, és ezáltal hamis biztonságérzetet teremtünk. A gond az, hogy ma alig-alig létezik olyan időpont, amikor a szereplők egy térben jelen vannak és komplexen kezelik ezt a kérdést. Ez ma gyakorlatilag egyedül az épület használatbavételének időpontja lehet, de ez sem törvényszerű. A megoldás abba az irányba kell, hogy mutasson, hogy a szereplők tevékenysége minél homogénebb legyen, minél több és aktívabb kapcsolódási pont alakuljon ki, ezáltal felállítható egy jól működő kontroll rendszer is, kialakul egy folyamatos oda-vissza csatolás minden szakember között. A speciális szakterületek eredményei valóban hatni kezdenek egymásra. Ennek a

rendszernek a megvalósulása eredményezi a komplex tűzvédelem kialakulását. Amikor valamennyi szereplő, valamennyi speciális szakág tevékenysége – egy-egy épület esetében, annak teljes életciklusát átívelve, térben és időben – kölcsönösen hat egymásra, folyamatos és intenzív kölcsönhatásba kerül, létrejön a komplex tűzvédelem.

Ennek a rendszernek a digitális, elektronikus megvalósítás az útja, amelyhez a mai infokommunikációs világunkban az infrastruktúra teljes mértékben rendelkezésre áll. (Haig, 2008) Az infokommunikáció lehetővé teszi a szereplők egy „térben", virtuális térben és valós időben történő jelenlétét, továbbá szolgálja az elektronikus adatbázisok kapacitásának kényelmes elérését. (Haig, 2013) Így a szakember fluktuáció miatt sem történik információ vesztés, bárki be tud kapcsolódni az adott rendszerbe.

4.2. Kritikus helyek és időpontok

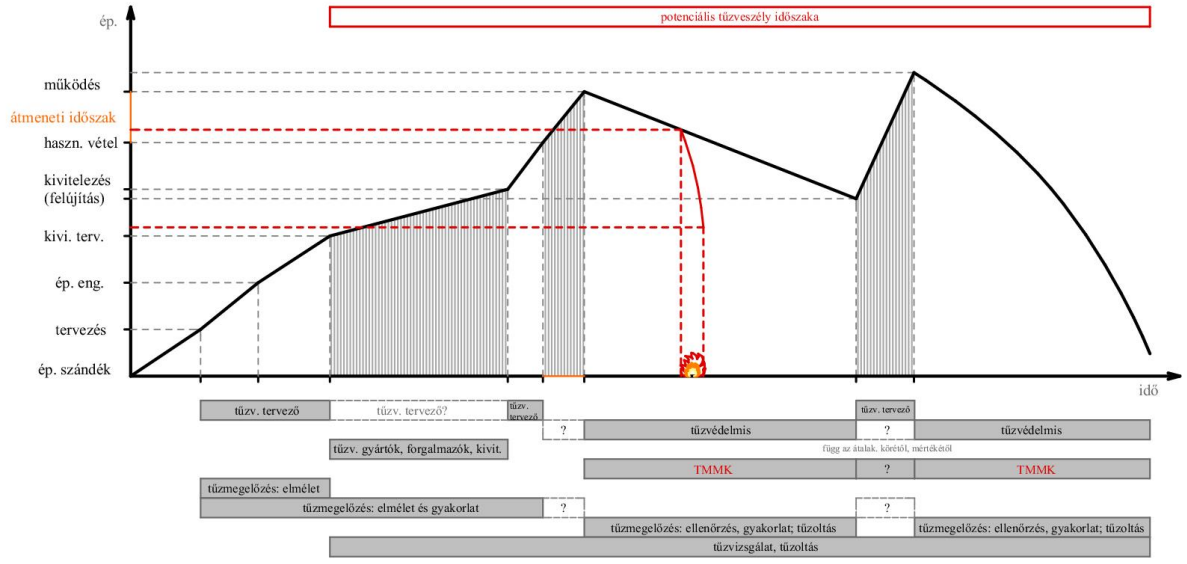
A kritikus idő intervallumok megállapításában a tűzvizsgálat tapasztalatai jelentik az origót. Egy a tervezéstől az újratervezésig, vagy bontásig tartó épület életciklus során különböző kritikus fázisok alakulnak ki, amelyek fehér foltként jelennek meg a tűzvédelemben. Három kritikus fázist mutatok be különböző nemzetközi tűzesetek példáján.

Az első esetben egy folyamatban lévő felújítás során keletkezett tűz a párizsi Ritz Hotelben, 2016. január 19-én. A már újranyitás előtt álló szálloda építészeti szempontból már szinte elkészült, de tűzvédelmi szempontból mégis egy kedvezőtlen, kritikus állapotban volt. A tűzvédelmi rendszerek nem rendeltetés szerinti állapotban működtek, mert folyamatos munkálatok zajlottak az épületben. A használat sem volt rendeltetésszerű, hiszen építkeztek. Mégis az épület és tűz paraméter majdnem olyan értékeket vett fel, amelyek igazak egy rendeltetésszerűen funkcionáló épületre.

A második esetben egy átalakítás alatt álló épület, de kivitelezéssel nem érintett, elhagyott építési helyszínen keletkezett tűz Budapesten, az Andrássy úton, 2014. július 15-én. A palota épület felső szintjeiből a belső falakat és födémeket kibontották, ezáltal egy hatalmas légtér, egy óriási tűzszakasz alakult ki, amely hosszú időn keresztül fennállt. A hatalmas tűzesetet, a tűz kiemelten nagy területre történő terjedését a tűzterjedést gátló épületszerkezetek hiánya okozta. A szétbontott, egy légteret eredményező zárt tér hosszú időn át fennálló állapota, azaz az épület paraméter játszott szerepet a kritikus hely és hosszú potenciálisan tűzveszélyes időszak kialakulásához.

A harmadik esetben pedig a tűz paraméter határozta meg a tűzesetet. 2016. január 1-én a dubai The Address Downtown Hotelben keletkezett tűz. A szilveszteri tűzijáték során egy pirotechnikai termék okozta a tűzesetet. A kritikus időpontban több helyen is az eltérő használat eredményeként újra értékelődnek a különböző paraméterek. Szilveszterkor koncentráltan megnő a használatban lévő pirotechnikai termékek száma, amely potenciális tűzveszélyt okoz. A tűz paraméter ebben a példában olyan kritikus értéket vett fel, hogy képes volt tüzet okozni.

A példákból látható, hogy mindhárom tűzeset egy-egy tűzvédelmi szempontból kritikus időben keletkezett, valamelyik tűz kölcsönhatás paraméter (épület-ember-tűz) szélsőérték felé történő tolódásával. A tűzvizsgálat mérnöki szemléletű lefolytatásával a tűzhatás szerkezetekre vonatkozó következményei egzakt módon megállapíthatóak. A hagyományos használati szabályok, vagy szakhatósági eljárások szemszögéből mindhárom eset kezelt probléma volt, de időbeli mélységben nem került vizsgálat alá a kritikus időtartamok alatti tűzvédelmi helyzet, így a megfelelő tűzbiztonságot nem alakították ki, ezért tűz keletkezett. A tűzvédelem szereplői vagy nem, vagy csak részlegesen voltak jelen a folyamatokban, így a folytonos tűzvédelmi háló helyenként megszakadt.



5. ábra kritikus helyek az idő függvényében (saját szerkesztés)

4.3. Innovatív mérnöki módszerek alkalmazása

Az épület-ember-tűz tényezők valós egymásra hatásai mérnöki módszerekkel tervezhetők (Badonszki, Szikra, Szilágyi, 2013), amelyek által pontos képet alkothatunk az épületünk

tűzvédelmi életciklusáról. Ilyen módszerek többek között a valós tűztesztek, a szimulációs vizsgálatok, számítások, az elemzés-értékelés, és az épület diagnosztika, amelyek által előre megállapíthatjuk az épületünk életciklusának alakulását. (Kerekes, 2008) A módszerek önmagukban azonban téves, félrevezető eredményekhez is vezethetnek. A különböző módszerek vegyes alkalmazása, a különböző eredmények egymáshoz viszonyított értékelése adja a mérnöki módszer lényegét. Önmagukban a különböző módszerek csak részeredményeket szolgáltatnak, csak olyan részrendszerben, amelyben konkrétan vizsgálat alá kerültek. Egy meghatározott módon elvégzett valós tűzteszt (pl.: homlokzati hőszigetelés tűzterjedési vizsgálata) az adott térbeli kialakítási problémát kezeli, de minden egyedi épületre ugyanaz a rendszer más-más beépítési helyzetben, térbeli kialakításban csak közelítően értékelhető ugyanolyan módon. Felhasználva a valós tűzteszt eredményeit, megfelelő modell tűz választása esetén, Szabó, Beda, 2014) és a BIM (épület információs modellezés) alapú tervezés térbeli információit, a ma már rendelkezésre álló és rohamosan fejlődő szimulációs szoftverekkel rendelkezésre áll az a képesség, amellyel tervezhetővé válik a fenti probléma megoldása. Ez természetesen minden egyedi kialakítás esetében egyedi megoldásokat takar, több mérnöki módszer megfelelő alkalmazását követeli meg és egy értékelő-elemző összegzésben ölt végleges formát, amellyel igazolhatóvá válik a tűzvédelmi követelménynek való megfelelés. A mérnöki módszerek tudatos és innovatív alkalmazása egységes szemléleten és közel azonos mértékű tudáson alapuló szakember gárdát igényel, mind a hivatásos, mind a civil szféra szereplőitől. Ezt nagyon alapos és célirányos szakmai képzéssel lehet elérni. Az innovatív mérnöki módszer tehát egy összefüggés rendszer, amely az adott tűzvédelmi problémára úgy ad egyedi megoldást, hogy a szükséges mértékben a szükséges mérnöki módszereket vegyíti, egymásra hatásukat elemzi és a tapasztalati, mért eredményekkel összehasonlítva összegzi, értékeli az épület kritikus helyén, egy-egy kritikus időpontban, vagy intervallumban. A különböző módon mért eredmények (számítások, szimuláció, tűzteszt) validálásával a valóság leképzése történhet meg, amely hosszú távú megoldásokat biztosít majd a tűzvédelem tudományában.

Az innovatív mérnöki módszerek alkalmazásával lehetőség nyílik egy épület életciklusa során a kritikus helyek és potenciálisan tűzveszélyes időszakok meghatározására, ezáltal a megfelelő biztonság kialakítására. Ez a biztonság szolgálja a tűzoltói beavatkozás speciális helyszíni biztonságát is. (Pántya, 2013) A kritikus helyek meghatározásával egy új típusú, mérnöki módszerekkel igazolt használat tervezhető a potenciálisan kockázatos

időintervallumokra. A jogszabályokon nyugvó statikus (csak a jogszabályváltozástól függő szabályozás) használati szabályok helyett új szemléletű dinamikus használati szabályozás alakítható ki.

4.4. Aktívan alkalmazott passzív tűzvédelmi rendszerek

Egy építmény teljes élete során a fő ciklusok idején a komplex tűzvédelem sok esetben a szakterületek és szereplők terén párhuzamosan, metszéspont(ok) nélkül valósul meg, amely a teljes tűzvédelem folytonosságán szakadásokat, fehér foltokat eredményez. (Bérczi, 2016) A fenti probléma megoldása szempontjából kiemelten fontos, hogy egyensúlyban lévő tűzvédelmi rendszerekkel alkossuk meg egy épület tűzvédelmi helyzetét, amelyhez rugalmasan alkalmazkodni képes a kortárs dinamikus használat.

A főként aktív tűzvédelmi rendszerekre épülő tűzvédelmi koncepció legfőbb gyengesége az időbeli avulás, amely instabillá teszi a rendszert. Az instabilitás következtében kialakulhat az a helyzet, hogy a védelem nem képes ellátni a szerepét. Zárt terek esetében ezáltal jelentős mértékben megnő a kockázat, amely az épület teljes életciklusának kritikus pontjainál csúcsosodik ki.

A főként passzív tűzvédelmi rendszerekre épülő tűzvédelmi koncepció legfőbb gyengesége a variábilis kialakításban mutatkozik meg. A fixen, épített szerkezeti elemekkel megvalósított térbeli kialakítás (átmeneti védett terek, tűzgátló módon – tűzgátló fallal, tűzgátló válaszfallal – leválasztott helyiségek, önálló tűzszakaszok, vagy tűztávolsággal kialakított tűzterjedés elleni védelem, stb.) kismértékben ad lehetőséget a multifunkcionalitásnak, viszont stabil egyensúlyi helyzetben tartható az épület.

A fentiek alapján az a következtetés szűrhető le, hogy modern épületek esetében a leghatékonyabb és a teljes életciklusra vetítve legoptimálisabb tűzvédelmi helyzet az egyensúlyi állapotok figyelembevételével az aktívan alkalmazott passzív védelmi rendszerek kialakításával érhető el. Mit jelent ez? Alapvetően a térbeli struktúrát tűzvédelmi szempontból lekövető, vagy sok esetben alakító kialakítások az épület információs rendszerét képző automatikus beépített tűzjelző rendszer működésének hatására passzív, de mobil tűzterjedés elleni gátlást valósítanak meg (tűzgátló nyílászárókat, mobil füstkötény rendszereket aktiválnak). Az intelligens érzékelés és vezérlések (Ramachandran, 1991) hatására aktivált

tűzvédelmi rendszerelemek a folyamat végén passzív módon fejtik ki hatásukat, ezért stabil egyensúlyi helyzetet hoznak létre, úgy hogy a passzív módon lehatárolt térről a tűzjelző rendszer képességeinek hatására már a tűzoltás felderítés szakaszában információkkal rendelkezik a beavatkozó állomány. A passzív rendszerek tűzjelző berendezés nélkül is képesek automatikus módon aktiválódni: hőre habosodó rendszerek, hőre tűzgátlást biztosító felkeményedő habok, stb.) Ezen rendszerek alkalmazásával az építészeti terek átjárhatósága biztosított, variálható az adott funkció igényeknek megfelelően, ugyanakkor stabil egyensúlyi helyzetben biztosítja a védelmet. Az adott zárt terek kiürítése, ezáltal az életvédelem magas szinten biztosítható.

Megállapítható, hogy mérnöki módszerek innovatív és kombinált alkalmazásával – az egyedi tűzvédelmi kérdések megoldásán túl – a tűzvizsgálat mérnöki eredményei és tapasztalatai alapján kockázatos időszakok és helyek határozhatók meg, amelyekre egzakt módon tervezhető a használat. Ez a módszer az innovatív mérnöki módszer, amely egy szerteágazó, korszerű számítógéppel segített elemző, értékelő módszer. A BIM (Building Information Modelling) alapú tervezéssel és a felhő alapú korszerű infokommunikációs rendszerek alkalmazásával aktívvá tehetjük a passzív tűzvédelmi eszközeinket. (Érces, Restás, 2017) Így gyakorlatilag az aktív módon alkalmazott passzív tűzvédelmi rendszerek működtetésével egy új típusú dinamikus használati szabályrendszer alakul ki, amely folyamatosan stabil egyensúlyi állapotban biztosítja egy épület teljes életciklusán át a biztonságot.
A hazai tűzvédelemben, a stabil tűzvédelmi egyensúlyi helyzet kialakítása céljából, a mérnöki módszerek innovatív és kombinált alkalmazása folyamatosan beépíthető a vonatkozó tűzvédelmi műszaki irányelvekbe, így gyakorlatilag jelentős mértékben bővíthető a tervezői szabadság, olyan módon, hogy a tűzbiztonság folyamatosan erősödik. A tűzvédelmi műszaki irányelvekbe történő integrációt megelőző alkalmazás során pedig jóváhagyási eljárás keretében igazolható a megfelelő tűzbiztonság, jelentős mértékben csökkentve ezzel a jogszabályi előírások alól történő eltérési engedélyezési eljárások lefolytatásának szükségességét, amely által az erőforrás többlet miatt nő a tűzvédelmi hatóság hatékonysága. (Érces, 2016)

5. Tűzvédelmi háló

5.1. A tűzvédelmi háló felépítése

Az innovatív mérnöki szemlélettel megvalósuló tűzvédelem a tűzvédelmi hálóval hozható létre, a kezdeti tervezési fázistól egy tűzeseti beavatkozáson át az épület teljes elbontásáig, majd onnan ismételten kezdve.

A tűzvédelmi háló, mint egy mátrix tartalmaz minden információt az aktuális tűzvédelmi helyzetről, amelyet a hálózatra csatlakozó személyek felhő alapú megosztott rendszerekből elérnek. Az információ mindig egy közös tárhelyen van, amely változása minden időpillanatban minden szereplő számára egyértelmű és folyamatosan nyomon követhető. Gyakorlatilag folyamatos kontroll alatt áll, és a virtuális térben könnyedén elérhető. Tehát az információ elhelyezésre kerül egyértelműen beazonosítható módon a hálóra (pl.: egy tűzszakasz hőmérséklete, ami egyértelmű azonosítót kap, pl.: I. tűzszakasz, egy adott épületben, amely egy adott egyedi helyrajzi számon található. A tervezők létrehozzák ezt az információt, BIM alapú eljárással virtuális valósággá alakítják, majd igény esetén elhelyezik a különböző szimulációs szoftverekben elemzés céljából. Itt további információkkal bővítik az adott tűzszakasz adatait, amelyek összevethetők valós tűztesztek adataival, tűzvizsgálati eljárások eredményeivel, számításokkal. Természetesen az adott szakkérdésbe több tervező, több szereplő is bevonásra kerül, akik azonos módon hozzáférnek az információhoz és képesek bővíteni is azt. Végül az információ halmazt elemzik, értékelik és kiválasztanak egy optimális megoldást, amelyet már a digitális állam kereteiben lévő elektronikus rendszerben helyeznek el, ahol a tűzvédelem további szereplője, az engedélyező team is teljes körűen hozzáfér az eredményekhez. Ahhoz, hogy a tűzvédelmi háló teljes mértékben kiszélesedhessen, a jelenleg használt ÉTDR rendszer pdf alapú statikus file rendszere nem alkalmas a cél eléréséhez.

A mindenki által elérhető felhő alapú dinamikus file-ok lehetővé teszik, hogy a már okos készülékekről is elérhető e-naplóba a kivitelezés változásait is dinamikusan lehessen átvezetni, amely minden szereplő számára ismertté válik. A megvalósulást követően a tárhelyen egy megvalósult állapot jelenik meg, amely a használathoz az aktívan használt passzív tűzvédelmi rendszerekből dinamikus használatot eredményez, amelyet nyomon követhetünk, később egy-egy ellenőrzés, vagy tűzoltói beavatkozás során is. A kritikus helyek

és időpontok ismeretében pedig lokális aktív tűzmegelőzést hajthatunk végre a passzív rendszereinken is.

6. ábra Tűzvédelmi háló (saját szerkesztés)

5.2. Digitális tűzoltó

A megvalósult érzékelőkkel ellátott, mért tereknek köszönhetően egy esetleges tűzesetre a digitális tűzoltó a tűzvédelmi háló segítségével már az okos készülékén keresztül a vonulás során valós távolsági felderítés keretében fel tud készülni és a legbiztonságosabb és leghatékonyabb beavatkozást tudja egy döntés segítő rendszer alkalmazásával megvalósítani. Ezáltal a legkorszerűbb beavatkozás válhatna valóra. A tűzoltásvezető olyan információkkal rendelkezne egy tűzeset helyszínére érkezve, amelyet már gyakorlatilag távolsági felderítéssel megszerez, amelyeket ma, ilyen mélységben, sok esetben egy helyszíni felderítés során sem tud teljes mértékben megszerezni. A fentiek miatt, továbbá a döntést támogató rendszereknek köszönhetően kész tervek állnának rendelkezésére, amelyeket kombinálva, vagy a legmegfelelőbbet kiválasztva a beavatkozás gyorsasága jelentősen megnőne, azaz a tűz fejlődésének egy olyan korábbi szakaszában meg tud kezdődni a tűzoltás, amikor még nem

fejlődik ki a teljes tér égése. Így jelentősen csökkenne a benntartózkodók veszélyeztetettsége és a tűzkár. A beavatkozó tűzoltó állomány biztonsága jelentős mértékben nőne, és az oltóanyag felhasználás is optimalizálódna. Összességében tehát jelentős mértékben nőne a tűzoltói beavatkozás hatékonysága, emellett egyenes arányban nőne a biztonság is. Az okos eszközök alkalmazásán túl a beavatkozó tűzoltó egyéni védőeszközeit is el lehetne látni érzékelőkkel, amely folyamatosan vizsgálná a tűzoltó életfunkcióit és a közvetlen környezetének állapotát. Így a személyes biztonság az épületekbe beépített rendszereken túl jelentős mértékben fokozódna. Az épület és az egyéni védőeszköz a kompatibilitás elvén automatikusan szinkronizálódhat, ezáltal egy kölcsönös szimbiózis alakulhat ki a tűzhelyszín és a beavatkozó állomány között, amely komplex biztonságot nyújtana a tűzoltó állomány részére. Továbbá jelentős mennyiségű információt rögzítene a rendszer, amelyet a tűzvizsgálat során fel lehetne használni. A tűzvizsgálati eljárás során a beavatkozó állománytól megszerezhető információ, amelyet ma meghallgatás, elmondás útján hajthatunk végre, egy egészen új minőségben jelenne meg, egzakt adatokkal.

5.3. Ellenőrzési lehetőség

A tűzvédelmi hálóval nőne az ellenőrzések minősége és hatékonysága is. Egyrészről a rendszerek ellenőrzése digitális módon is elvégezhető lenne, akár az e-építésnapló, akár egy aktív tűzvédelmi berendezés működőképességének ellenőrzéséről legyen szó. Ez természetesen nem helyettesíti a helyszíni élő ellenőrzéseket, de az azokra történő felkészülést lehetővé teszi, a folytonosság meglétét nyomon követhetővé teszi, és az ellenőrzések lehetőségét kiterjeszti, azaz összességében jelentős mértékben növeli a kontroll hatékonyságát. Igaz ez mind az üzemeltetői, mind a hatósági terület szakemberei részére.

5.4. Komplex tűzvédelem a komplex tűzvédelmi hálóban

A komplex tűzvédelem tekintetében körbezár a folyamat, és kialakul a teljes kölcsönhatás, gyakorlatilag megvalósul a komplex tűzvédelem. A példaként hozott aktívan alkalmazott passzív tűzgátló alapszerkezet információt meghatározzák a tervezésnél, majd értékelik, végül a kialakult adatok alapján egy rendszer részeként engedélyezik. Az információt tovább használják a kivitelezés, a termékgyártás során, ahol már nyújthatnak visszajelzéseket a tervezők felé. Mindenről informálódik a hivatásos szakterület is, ellenőrizhet, vizsgálódhat,

amely során szintén visszajelzéseket adhat a gyártónak, tervezőnek. A használat során az üzemeltető szakemberei is alkalmazzák az információt, és megteszik a szükséges intézkedéseket, karbantartást, felülvizsgálatot, illetve visszajelzéseket adnak a hatóság, szakhatóság, a gyártó és a tervező részére is. Végül ugyanezt az információt képes alkalmazni a beavatkozó tűzoltó és a tűzvizsgáló szakember is egy-egy tűzeset során és azt követően. A tapasztalataikat pedig a tűzvédelmi háló segítségével ugyanarra a műszaki megoldásra vissza tudják jelezni valamennyi korábbi szakterület, szakember részére. Gyakorlatilag egy teljes egymásra hatás alakul ki, amely dinamikusan képes a tűzvédelem fejlesztésére, a tűzbiztonság jelentős és hatékony növelésére, egy-egy épület teljes életciklusán átívelve.

6. Okos város és a katasztrófavédelem

6.1. Smart city

A 2017. március 20-i Magyar Közlönyben megjelent az 56/2017. (III. 20.) Korm. rendelet az egyes kormányrendeleteknek az „okos város", „okos város módszertan" fogalom meghatározásával összefüggő módosításáról. A kormányrendelet hivatalosan is meghatározza mit értünk okos város alatt:

Az okos város olyan település vagy település csoport, amely természeti és épített környezetét, digitális infrastruktúráját, valamint a területén elérhető szolgáltatások minőségét és gazdasági hatékonyságát korszerű és innovatív információtechnológiák alkalmazásával, fenntartható módon, lakosainak fokozott bevonásával fejleszti.

A módszertan szerint véghezvitt, fenntartható városfejlesztés horizontális szempontokat – magas minőség és hatékonyság, környezeti és gazdasági fenntarthatóság, lakosság fokozott bevonása – érvényesít a szolgáltatások és az infrastruktúra fejlesztésében egyaránt. A fejlesztés és működtetés eszköztárába integrált információtechnológiák ezek eléréséhez és a fejlődés nyomon követéséhez nyújtanak segítséget. (http://okosvaros.lechnerkozpont.hu/hu)

Az okos város az EU Smart City Ranking és a Smart Cities Council index rendszerén alapszik, melyek 6 alrendszert jelölnek meg:

1. Okos kormányzás
2. Okos közlekedés
3. Okos környezet
4. Okos gazdaság
5. Okos életkörülmények
6. Okos emberek

Az Okos életkörülmények alrendszer alatt értjük az élhető várost, a **személyes biztonságot és az egészségügyi kondíciókat** javító intézkedéseket.

Ezen alrendszer részhalmazát képzi a katasztrófavédelem.

6.2. Okos életkörülmények biztonsága a katasztrófavédelem által

Az okos város képes katasztrófavédelem biztonsági komponenseinek kiterjesztésére, amely biztosítja, hogy az egyes BIM alapon tervezett és üzemeltetett épületek csoportja az adott településszövetben biztonsági zónákként jelenjen meg. A különböző digitálisan rendelkezésre álló településszerkezeti tervek különböző övezetei a BIM rendszer által biztonsági minőségekkel ruházhatók fel, amelyek csoportosítva övezeti biztonsági szinteket képeznek.
A különböző biztonsági szintekhez rendelhető kockázatok határozzák meg a veszélyességi övezetek mérhető határait, amelyeket a településrendezési eszközöknél figyelembe kellene venni. A BIM rendszernek köszönhetően, a térinformatika alkalmazásával, a teljes ország lefedettségét el lehet érni, és elérhetővé lehet tenni a digitális állam keretében valamennyi szereplő számára. Ez a rendszer szolgálná az okos életkörülmények biztonságát a legalapvetőbb szinten, a településrendezés szintjén a katasztrófavédelem szempontjából. Itt már nem csak digitalizált 2D-s platformról beszélhetünk, hanem egy kiterjesztett valóságot megjelenítő és használó alkalmazások segítségével egy virtuális valóságról, amely az eddig ismert legmagasabb biztonsági szintet képes létrehozni.

6.3. Okos város fejlesztési modell és monitoring rendszer

Az okos város fejlesztési modell az adott település integrált településfejlesztési stratégiájának részét képzi a stratégia megalkotás szempontjából, továbbá lefekteti a monitoring a rendszer kereteit. Ezáltal az intelligens megoldások bevezetésével egy hosszú távú fenntarthatóság építhető fel. (http://lechnerkozpont.hu/doc/okos-varos/okos-varos-fejlesztesi-modell-tervezesi-utmutato-170405.pdf)
A biztonság kérdésének fenntarthatóságát is ezek az intelligens megoldások alapozzák meg. A hosszú távú fenntarthatóság elvén tervezett épületek rendszerelemei, intelligens épületinformációkkal modellezve a tervezett kockázatok elemzésével racionizálható és optimalizálható a védekezés kiépítésének mértéke. A stratégiai szinten kezelt biztonságra tervezett intelligens épített környezet monitoringozható, így az esetleges kockázatnövekedések már a kezdeti fázisokban észlelhetővé válnak, és a szükséges biztonsági intézkedések korai szakaszban kezelhetők lesznek. Ezzel a metodikával a megvalósul a biztonságos hosszútávú fenntarthatóság.
Másik fontos aspektusa a monitoring rendszer által nyert információk adatbázisban történő gyűjtésének, hogy az eredmények értékelésével az elkövetkező tervezések során a tapasztalt,

mért, egzakt eredmények figyelembevételével hatékonyabb megelőzés érhető el, amely folyamatosan az információs bázis növekedésével egyre hatékonyabbá válik.

6.4. Okos katasztrófavédelem az okos város struktúrában

A katasztrófavédelem megelőző és beavatkozó képességei az okos város rendszerben a hosszú távú fenntarthatóság szempontjából soha nem látott minőségre növelhetők. A térinformatikai modellek segítségével, dinamikus és digitális alaptérképek felhasználásával a településrendezés eszközeinek kialakításánál aktívan integrálható a katasztrófavédelem biztonsági szempontrendszere, amely a megelőzés első- és alappilléreként működhet.

A digitális településrendezési eszközök térinformatikai támogatottsággal egzakt veszélyességi zónákra bonthatók, amely településszövetekbe az egyes épületek egyedi módon azonosítva elhelyezhetők.

Az egyes épületek BIM alapon történő tervezésével a legkisebb védelmi egység is, pl.: egy tűzszakasz azonosítható, követhető, ellenőrizhető hosszú távon felhő alapú informatikai rendszereken alapuló monitoringozás útján. Ebben az infokommunikációs rendszerben különböző szereplők (hatóságok, tervezők, üzemeltetők, stb). egy térben és valós időben okos eszközök alkalmazásával bárhonnan naprakész információkkal rendelkeznek, amelyek birtokában a veszély legkorábban azonosított jelére a szükséges intézkedéseket képesek megtenni.

Az okos városba integrált biztonsági háló kiterjesztésével folyamatosan egyre nagyobb területek fedhetők le, míg végül Magyarország teljes területére kiterjedhet a lefedettség. A monitoringozás által készített adatbázisok, amelyek a megelőzési paramétereket eleve tartalmazzák, a beavatkozások és beavatkozásokat követő vizsgálatok adatival olyan visszacsatolási rendszert képeznek, amely a következő tervezések fejlesztését empirikus úton nyert eredményekkel támasztják alá. A mért adatok kiterjesztése a szimulációs eszközök nyújtotta tervezési lehetőségek során validált eredményként felhasználhatók a veszélyek prognosztizálásához.

A katasztrófavédelem hivatásos szervei az e-közigazgatás keretében eljárva hivatalos eljárások lefolytatására is képesek lesznek, amely már az okos városok platformján történhet, a digitális állam nyújtotta informatikai infrastruktúrában.

A fentiek alapján a legkisebb épített környezeti elem (pl.: egy épület) intelligens épületinformációs tervezésével a katasztrófavédelem a még virtuális modell születésénél

csatlakozik a megfelelő védelem kialakításában. Az egyes épületek településszövetei, övezeti az okos városban egységes, jól követhető és monitoringozható szisztémát alkotnak, amely az informatikai infrastruktúrának köszönhetően kiterjeszthető az egész ország területére. Adatbázisok szintjén pedig kiterjeszthető az EU azonos adatbázisaira is, amely már több száz milliós lakosság mélyen tagolt, ország határokon átívelő biztonságát szolgálja. A katasztrófák határokon átívelő hatásai miatt ez a megoldás szolgálná a leghatékonyabb védelmi rendszer kiépítését hosszútávon.

A robotika, mint a következő információs forradalom előképe a fenti rendszerbe összefüggésszerűen integrálható, így veszélyhelyzetben a kockázatos emberi beavatkozások mértéke csökkenthető lesz. Az okos épületeken keresztül az okos városok, okos ökoszisztémájába integrálható robotizált biztonsági rendszerek nagy mértékben újabb lépcsőfokkal növelik majd a biztonság szintjét a katasztrófavédelem területén.

6.5. Okos katasztrófavédelem és a közösségi háló

Az okos ökoszisztéma a lakosság életét és mindennapjait átszövő közösségi hálóban kiterjeszthető. A kiterjesztés eredményeként a biztonság új minősége közvetlenül eléri a lakosságot. A egy katasztrófa helyzetről, tűzvészről, veszélyhelyzetről, stb. a lakosság az okos ökoszisztéma rendszerén keresztül ellenőrzött és hiteles információkkal kerülhet ellátásra. A tájékoztatáson túl időben azonnal közölhetők a létfontosságú, majd egyén kiegészítő információk a szükséges teendőkről, a lehetséges veszélyekről. A közvetlen kommunikáció a veszélyhelyzettel érintett közösség biztonságát szolgálja, az adott észlelést követően, a monitoring rendszereknek köszönhetően, lehető legrövidebb időn belül. A hivatásos és az önkéntes beavatkozó állomány riasztásával egy időben a lakosságvédelmi intézkedések is már távolsági helyzetből megkezdhetők. (Endrődi, 2014) Megfelelő applikációkon keresztül a beavatkozó állomány visszajelzéseket kap a lakosság megkezdett tevékenységéről, így már a távolsági felderítés során információkat szerez a lakossági intézkedésekkel kapcsolatban, még a kárhelyszínre érkezés előtt. Ez az új távolsági, előzetes lakossági intézkedés a ma ismert és alkalmazott lakossági intézkedések új minőségét szolgáltatja. Időben jelentősen korábban megkezdhető, megfelelő applikációk alkalmazásával, már egy okos szüléken keresztül minden lakosságvédelmi tájékoztatás közölhető az észlelést követő 1-2 percen belül, a riasztással párhuzamosan. A lakosság megfelelő információt kaphat a felmerült veszélyhelyzetről, annak mértékéről, a szükséges teendőkről, a lakosságvédelmi helyek,

átmeneti elszállásolást biztosító helyek elhelyezkedéséről, az odajutás térképes elősegítéséről. Az esetleges kitelepítés menetét, a teendőket a térinformatikai rendszer támogatásával okos eszközökről követheti a lakosság, és egyszerűen visszajelezhet, hogy biztonságban megtörtént egyénenként az intézkedés végrehajtása. Az okos készülékekben található GPS hely/helyzet meghatározó- és navigációs rendszer információkkal szolgál mind a lakosság, mind a beavatkozó állomány részére. A védelmi igazgatásba integrálva az okos katasztrófavédelem rendszerét a veszélyhelyzeti központokból professzionális módon koordinálható és irányítható a veszélyelhárítás: a beavatkozás, a lakosságvédelem, később pedig a biztonságos rend visszaállítása. A teljes, átfogó védelmi igazgatás új minőségként jelenhet meg közvetlenül a lakosság köreiben. Ez a védelmi háló a kezdeti néhány perc előnyt a veszély fejlődésével szemben az idő múlásával órákra, szélsőséges esetekben napokra megnövelheti, amely által több emberi élet megmentése valósulhat meg.

7. Összegzés

7.1. Összefoglalás

A katasztrófavédelemben a komplex tűzvédelem a szereplők nagymértékű heterogenitása és az épület-ember-tűz paraméterek egymásra hatásának időbeli dinamikus változása olyan kritikus kockázatú fehér foltokat okoz egy épület teljes életciklusát tekintve, amelyek jelentős mértékben csökkentik az épület tűzbiztonságát. Megállapítható, hogy mérnöki módszerek innovatív és kombinált alkalmazásával – az egyedi tűzvédelmi kérdések megoldásán túl – a tűzvizsgálat mérnöki eredményei és tapasztalatai alapján kockázatos időszakok és helyek határozhatók meg, amelyekre egzakt módon tervezhető a használat. Ez a módszer az innovatív mérnöki módszer, amely egy szerteágazó, korszerű számítógéppel segített elemző, értékelő módszer. A BIM alapú tervezéssel és a felhő alapú korszerű infokommunikációs rendszerek alkalmazásával aktívvá tehetjük a passzív tűzvédelmi eszközeinket.

Így gyakorlatilag az aktív módon alkalmazott passzív tűzvédelmi rendszerek működtetésével egy új típusú dinamikus használati szabályrendszer alakul ki, amely folytonosan biztosítja egy épület teljes életciklusán át a biztonságot. A komplex tűzvédelem szereplői a digitális állam rendszerében virtuális módon egy térben és időben tevékenykedhetnek, homogén módon így egy új típusú, mérnöki szemléletű tűzvédelmi háló szolgálhatja a biztonságot a tervezés első lépésétől a tűzoltói beavatkozás szervezésén, az ellenőrzéseken át az épület végleges

elbontásáig. A mai felgyorsult világ tempóját követő tűzvédelem innovatív megvalósításához a már megkezdődött szemléletváltás kiszélesítésére és felgyorsítására, a tűzvédelmi képzés tudatos mérnöki szemléletű átalakítására van szükség.

Albert Einstein gondolata nyomán: a katasztrófavédelem és az általa nyújtott biztonság, amit létrehoztunk, gondolkodásunk eredménye. Nem lehet megváltoztatni, megújítani kizárólag jogszabályokkal, csak akkor, ha gondolkodásunkat, szemléletünket is megváltoztatjuk. Ennek egzakt módon járható útja a tudományos alapokon nyugvó megoldások keresése.

A katasztrófavédelem fejlesztésének lehetőségét az innovatív mérnöki módszereken alapuló komplex tűzvédelem fejlesztésében látom, amely létrehozható a digitális állam keretein belül a rendelkezésre álló infokommunikációs eszközök alkalmazásával. A komplex tűzvédelem megvalósulásával a katasztrófavédelem egy új minősége jönne létre, amely a biztonságot egy magasabb szintre emelné.
A rendszer okos városok programban történő megvalósítása és kiterjesztése egy átfogó, egységes katasztrófavédelmi háló kialakítását képezné, amely Magyarország teljes területén szolgálná a biztonságot. A digitális állam struktúrájában monitoringozás útján empirikus módon nyert egzakt adatbázisok megosztásával az Európai Unió teljes területére kiterjeszthető katasztrófavédelmi háló hozható létre.

7.2. Ajánlás

A tanulmány eredményei a katasztrófavédelem fejlesztését kívánják szolgálni, olyan módon, hogy az általános közigazgatási szférából a hangsúlyt áthelyezi az informatikai alapokon nyugvó e-közigazgatás síkjára. A digitális állam teljes megvalósulásakor a megújult, legkorszerűbb katasztrófavédelmi igazgatást szolgálja alátámasztani, mérnöki elveken alapuló módszerek segítségével.
A katasztrófavédelem ezen új védelmi jellege, és az ezáltal nyújtott biztonság új minősége kiterjeszthető és általánosítható a védelmi, biztonsági szektor teljes spektrumára. Az innovatív mérnöki módszereken digitális projektekkel intelligens folyamatok útján egy okos ökoszisztéma alakítható ki, amely nagymértékben szolgálja a fenntartható fejlődést.
A fenntartható fejlődés alapjaként, az átfogó védelmi igazgatás által nyújtott védelmi háló, megfelelő applikációk alkalmazásával, szolgálja a lakosság magas szintű biztonságát, amely közvetlenül eljuttatható mindenki számára.

Irodalomjegyzék

Beda L.: *Épületek tűzbiztonságának műszaki értékelése*, Doktori értekezés, ZMNE, KMDI, 2004.

Beda L.: *Tűzmodellezés, tűzkockázat elemzés*, Szent István Egyetem YMMFK, 1999. pp. 5-12.

Beda L.: Gondolatok az épületek tűzbiztonságáról, *Magyar Építőipar*, 2011 (3) pp. 94-98.

Beda L. – Kerekes Zs.: *Égés- és oltáselmélet II*, Budapest, Szent István Egyetem YMMFK, 2006. 118 p.

Buchanan A. H.: *Structural Design for Fire Safety*, ISBN: 13:978 0 471 88993 9 (H/B), John Wiley & Sons, New Zealand, 421 pp.

H. Ziebs: Erfolgreiches Schutzkonzept am Beispiel Allianz Arena, *Bundesverband Technischer Brandschutz e. V.* (bvfa), Feuerlöschanlagen (2014) 6-11.

Restás Á.: A tűzoltásvezetők döntései – elméleti szempontból, *Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle* 20: (3) pp. 5-10.

Haig Zs. – Várhegyi I.: A cybertér és a cyberhadviselés értelmezése http://mhtt.eu/hadtudomany/2008/2008 elektronikus/2008 e 2.pdf (A letöltés dátuma: 2015. 11. 17.)

Haig Zs.-Kovács L.-Munk S.-Ványa L., Szerk.: Kovács L., Szerk.: Tózsa I.: *Az infokommunikációs technológia hatása a hadtudományokra*, Budapest: Nemzeti Közszolgálati Egyetem, 173 p.

www.kozigazgatas.netenahivatal.gov.hu (A letöltés dátuma: 2016. 04. 12.)

Fritts M.: A BIM jövője, http://www.autodeskforum.hu/?p=2780 (A letöltés dátuma: 2016. 04. 30.)

Kerekes Zs.: Az építőanyagok új „Euroclass" szerinti tűzveszélyességi minősítése és hazai bevezetése, *Tudományos Közlemények*, Szent István Egyetem YMMFK 5:(1) pp. 47-57. (2008)

Szabó A., Beda L.: Modelltűz-választás valós méretű tűzoltási modellhez, *Védelem Katasztrófavédelmi Szemle* 21: (6) pp. 19-21.

Bérczi L.: A tűzoltói beavatkozás biztonsága – helyszínen beépítve. Védelem Online, 2012. www.vedelem.hu/letoltes/tanulmany/tan428.pdf (A letöltés dátuma: 2015. 09.03.)

Bérczi L.: Structure, organization and duties of fire services in Hungary, *Védelem Tudomány: Katasztrófavédelmi Online Tudományos Folyóirat* I. (2) pp. 3-18. (2016)

Ramachandran G.: Informative Fire Warning Systems, *Fire Technology*, 27, 1, 1991 pp. 66-81.

Maliosz M.: Felhő alapú hálózatok, http://www.tmit.bme.hu/vitmma02-2015 (A letöltés dátuma: 2016. 03.18.)

Bérczi L.: A tűzvédelem a katasztrófavédelem rendszerében, *Új Magyar Közigazgatás 5*: (6) pp. 2-8.

Zellei J.: Mérnöki módszerek – a tűzszimuláció alkalmazásának módszerei, *Katasztrófavédelmi Szemle*, 20 1 (2013) 23-24.

Badonszki Cs. – Szikra Cs. – Szilágyi Cs.: Tűzvédelmi mérnöki módszerek a világban – a szomszéd rétje, *Katasztrófavédelmi Szemle*, 20 4 (2013) 31-34.

Muhoray Á.: *Katasztrófamegelőzés I.* Nemzeti Közszolgálati Egyetem Szolgáltató Nonprofit Kft., pp.: 24-182. (2016)

Endrődi I.: Egy lehetséges új veszélyhelyzeti információs és tájékoztató rendszer bemutatása, jelentősége, helye, szerepe a katasztrófavédelem rendszerében, *Bolyai Szemle* XXIII: (3) pp. 109-122. (2014)

Pántya P.: Füsttel telített, zárt terekben történő tűzoltói beavatkozások vizsgálata a biztonság szempontjából, *Bolyai Szemle* XXII. évf. 3. 2013. pp. 47-58.

Érces G. – Restás Á.: Infocommunication Based Development Opportunities in the System of Complex Fire Protection, In: Branko Savić, Verica Milanko, Mirjana Laban, Eva Mračkova, Restás Ágoston, Branka Petrović (szerk.) Book of Preceedings: МЕЂУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА БЕЗБЕДНОСНИ ИНЖЕЊЕРИНГ. 530 p., ISBN:978-86-6211-106-7

Érces G. – Restás Á.: Importence and procedure of building life cycle assessment, *Ecoterra: Journal of environmental research and protection* 14:(2) pp. 2-9. (2017)

Érces G.: Aktívan alkalmazott passzív tűzvédelmi rendszerek hatása az épületek tűzvédelmi életciklusában, *Védelem Tudomány* 1:(4) pp. 13-29. (2016)

Érces G.: Tűzvédelmi háló, *Védelem Tudomány* 1:(2) pp. 472-496. (2016)

http://digitalismagyarorszag.kormany.hu/europai-digitalis-menetrend (A letöltés dátuma: 2017. 09.18.)

http://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (A letöltés dátuma: 2017. 09.20.)

http://www.kormany.hu/download/0/05/50000/E-k%C3%B6zigazgat%C3%A1si_keretrendszer_koncepci%C3%B3.pdf (A letöltés dátuma: 2017. 09. 20.)
http://okosvaros.lechnerkozpont.hu/hu (A letöltés dátuma: 2017. 09.30.)

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

ALMÁSI CSABA SÁNDOR – BÁRTFAI FANNI – DR. BONNYAI TÜNDE – DR. GYARAKI RÉKA ESZTER – KISS SÁNDOR – MARGITICS JÓZSEF

A FŐVÁROS IVÓVÍZ-ELLÁTÓ RENDSZERE ELLEN INTÉZETT INFORMATIKAI TÁMADÁS POTENCIÁLIS KÖVETKEZMÉNYEI ÉS AZOK FELSZÁMOLÁSÁNAK MEGOLDÁSI LEHETŐSÉGEI

Bevezetés

Az elmúlt évek eseményei azt mutatják, hogy egy adott nemzetet a legnagyobb veszélyek már nem csak fizikailag, hanem a kibertérben is fenyegetik. A technológiai fejlődés adta lehetőségeknek köszönhetően nem csak az ipari szférában jellemző az úgynevezett rendszerbe történő kapcsolódás, hanem a lakosság alapvető ellátását biztosító infrastruktúrák esetében is egyre gyakrabban fordul elő. Bár sok eszköz egy rendszerbe történő kapcsolása nagyban megkönnyíti a mindennapi munkát és javítja az adott szolgáltatás színvonalát, azonban az így létrejött komplex rendszer sérülékenysége is jelentősen nő.

Ebből adódóan mind nemzetközi, mind hazai vonatkozásban egyre nagyobb hangsúlyt kap az ún. kritikus infrastruktúrák informatikai biztonságának kérdésköre, éppen ezért szükségesnek éreztük azt, hogy elemezzük egy adott létfontosságú rendszerelem informatikai támadásának lehetséges hatásait, illetve a helyreállítás során felmerülő kérdéseket és problémákat. Választásunk a Fővárosi Vízművekre esett, mert hazánk egyik legnagyobb ellátási képességével rendelkező ivóvíz-szolgáltatója. A Vízművek honlapján elérhető 2015-ös jelentés szerint két millió főt látnak el naponta fogyasztásra alkalmas vízzel és kezelik az általuk termelt szennyvizet. Ez naponta egy millió m^3 kapacitást jelent, amelyet 5 200 km vízhálózat tesz lehetővé.[65]

[65] http://vizmuvek.hu/files/public/Fovarosi_vizmuvek/tarsasagi_informaciok/FVM_Eves_Jel_HUN.pdf p. 10. (letöltés ideje: 2017.08.12.)

A pályamunka első részében az általunk elméletben megalkotott támadás menetét ismertetjük, amely felépítésében elsőként az internetes és egyéb, bárki számára szabadon hozzáférhető információkra támaszkodtunk, hiszen egy ártó szándékú egyén, vagy csoport is nagy valószínűséggel ezekből a forrásokból szerezné meg azokat a szükséges adatokat, amelyek elengedhetetlen fontosságúak egy hasonló volumenű támadás sikeres kivitelezéséhez.

A második fejezetben bemutatjuk a kialakult helyzet kezelésének egyes dimenzióit. A tervezés elsődleges szempontja – a pályamű elkészítésekor hatályos jogszabályok betartása mellett – a minél gyorsabb és eredményesebb válaszlépések kivitelezése, annak érdekében, hogy a lakosság számára szükséges ivóvízkészlet elérése és a szennyezett víz fogyasztásából fakadó fertőzések megakadályozása a lehető leghamarabb biztosítható legyen.

Szeretnénk azonban hangsúlyozni azt, hogy csak elméleti síkon jelentjük ki a tanulmányban leírt támadási technikák sikerességét és ezért elméleti síkon elemeztük a lehetséges következményeket is. Nem állt és jelenleg sem áll szándékunkban ötleteket adni senkinek egy esetleges támadáshoz, pusztán az általunk feltárt hiányosságokra kívánjuk felhívni a figyelmet, illetve egy olyan „rendkívüli eseményre vonatkozó forgatókönyv" megalkotása volt a célunk, amely a jövőben alapot adhat egy hasonló krízishelyzet tényleges kezeléséhez. A szerzők abban bíznak, hogy az általuk megfogalmazott preventív javaslatok hozzájárulnak ahhoz, hogy hasonló esemény a jövőben ne történhessen meg.

A budapesti ivóvíz-ellátó rendszer ellen intézett támadás kivitelezésének lépései

A Budapest ivóvízellátását biztosító szolgáltató (a továbbiakban: Szolgáltató) elleni támadás során a cél a lehető legnagyobb károkozás, ezért annak egy forró, nyári estére történő időzítése több szempontból is célszerű. Az időpont kiválasztásánál nem csak az játszathat szerepet, hogy a város lakosságának megnő az ivóvíz-fogyasztása és a vezetékes víz felhasználása: a nyáron szükséges fejenként napi 2,5-3 liter közötti vízfogyasztás mellett mindenképp figyelembe kell venni azt, hogy egy 4 fős család átlagos napi ivóvíz tisztaságú víz felhasználása megközelítőleg 600 liter[66]. Mindehhez hozzáadódik a – hőség elleni

[66] http://okoenergia.hu/vizfogyasztasi-statisztika/ (letöltés ideje: 2017.10.05.)

védekezésként elrendelt – közúthálózat és kiemelt zöldterületek locsolása és hűtése[67], illetve a magánkertek öntözése.

Különösen kiemelendő, hogy csak 2017 júniusában 391 635 fő turista tartózkodott[68] a majdnem két millió lakoson kívül a fővárosban. A fenti adatokat figyelembe véve ez a létszám jelentős többlet terhet ró mind a vízszolgáltatóra, mind a közlekedési infrastruktúrára. Különösen fennáll az utóbb említett szegmens terheltsége, amikor a főváros ad otthont egy olyan nagyobb volumenű rendezvénynek – például a 2017 nyarán megrendezett FINA világbajnokság –, amely nem csak megnövekedett számú látogatót vonz, hanem esetleges forgalomelterelésekkel is járhat.

A fent említett turisztikai adatokon túl a nyári időszak a szabadságolásokat is magába foglalja. Feltételezhető tehát, hogy ekkor a vízszolgáltatónál is csökkentett számú dolgozói állomány áll rendelkezésre, mindamellett az emberi tényezőt figyelembe véve – a hőség hatására – a koncentrációs képesség is csökken, miközben a szolgáltatás igénybevétele hatványozottan nő. Ez az állapot kedvez az úgynevezett social engineering típusú, informatikai támadások végrehajtásának, amelyek főként a célszemély hiszékenységére, gyanútlanságára alapoznak és használják ki azt.

Figyelembe véve a fent ismertetett okokat, a nyári kánikula idejére időzített többlépcsős, fiktív támadási terv az alábbiak szerint épülhet fel.

1. Informatikai támadás

Az informatikai támadás megtervezésekor első lépésben a célpont informatikai infrastruktúrájáról próbáltunk meg minél több adatot elérni nyílt forrásból. Az első gyors keresés közben segítségünkre volt többek között a főváros vízszolgáltatójának jubileumi kiadású honlapja, ahol megemlítik, hogy *„Az elektronika átveszi az irányítást: a termelő berendezések szabályozását frekvenciaváltók végzik, a gépházakat komputervezérléssel irányítják, felügyelik, a köztéri munkák folyamatirányítottak, mindezt egy központi diszpécserszolgálat tartja kézben.”*[69] Az idézett szövegen kívül találtunk képeket a központi

[67] http://www.orientpress.hu/cikk/2017-08-02_a-fovaros-kuzd-a-hoseggel (letöltés ideje: 2017.10.05)

[68] https://www.budapestinfo.hu/hu/szallashely-statisztika---minden-mutato-emelkedett-2017-elso-feleveben-budapesten-is (letöltés ideje: 2017.08.26)

[69] http://vizmuvek.hu/jubileum/ (letöltés ideje: 2017.08.22.)

irányító központról, amelyek megalapozták azokat a felvetéseinket, hogy a sebezhető emberi tényezővel számolhatunk. Ez az információ elősegíti a rendszer elleni támadás eszközének megválasztását, amely két típusú, vírus által okozott károkban nyilvánul meg. Az első vírus egy úgynevezett ramsomware, amely a levelező rendszeren keresztül behatolva titkosítja a fájlállományokat és akadályoztatja a belső kommunikációt, ezáltal felerősíti és elnyújtja a második féreg okozta károkat.

2013-ban az interneten megjelent egy részletesebb cikk a Szolgáltató akkor modernizált termelésirányító rendszeréről (a továbbiakban: SCADA), ahol mind a routerek, mind a PLC[70] eszközök esetében a konkrét termékcsaládok kerültek megnevezésre.[71] A korszerűsítés közbeszerzési pályázat kiírásával kezdődött meg. Mivel 2013 óta nem találtunk nyílt forrású kereséssel olyan közbeszerzési pályázatot, ami ehhez hasonló, nagyobb volumenű informatikai beruházásról szól, illetve maga a rendszer is 20-30 éves élettartamot ígér, ezért nagy valószínűséggel feltételezhetjük, hogy az eszközök többsége napjainkban is a négy évvel ezelőtt beszerzett termékekből áll. Ez az adat azért jelentős, mert felveti két sebezhetőség lehetőségét is, amelyek összefügghetnek egymással. Az amerikai SANS intézet 2017-es, több száz IT-biztonságért felelős szakember bevonásával készített felméréséből[72] az derült ki, hogy a rengeteg, még mindig fel nem patch-elt[73] vagy az önálló védelemmel nem rendelkező hálózati eszköz súlyos veszélyt hordozhat magában. Ezeken a réseken keresztül pedig bejuthat egy olyan, a Stuxnethez[74] hasonló kártevő, amelyet előzőleg akár a Darkneten vásárolhattak meg.

---

[70] Programozható logikai vezérlő, amely olyan bonyolultabb munkafolyamatokat vezérel, amik több, önálló szabályozással is rendelkező egységből állnak.

[71] https://sg.hu/cikkek/it-tech/96470/lecsereli-informatikai-halozatat-a-fovarosi-vizmuvek (letöltés ideje: 2017.08.22.)

[72] http://www.information-age.com/risks-facing-industrial-control-systems-reach-all-time-high-123467315/ (letöltés ideje: 2017.10.07.)

[73] Az adott programhoz tartozó, utólag javított fájlok eltérését tartalmazó információcsomag.

[74] 2010 nyarán bukkant fel Fehéroroszországban az a kártevő, amely kifejezetten SCADA rendszerekben okozott károkat. A vírus képes volt felismerni a natanzi erőmű Siemens gyártmányú PLC eszközeit és annak alapértelmezett programját felülírva úgy tette tönkre az általuk vezérelt atomdúsító centrifugákat, hogy a státuszjelző üzeneteket meghamisította, így az operátorok nem észleltek semmi rendkívüli eseményt mindaddig, amíg hallható jelei nem voltak a felgyorsult centrifugáknak. http://hadmernok.hu/2010_4_kovacs_sipos.pdf (letöltés ideje: 2017.10.07.)

1.1. A bejuttatás módszerei

Számos, az emberi naivitásra és jóhiszeműségre alapozó social engineering technika létezik. Jelen támadás során a két legnépszerűbb módszer segítségével „juttattuk be” a két kártékony kódot a rendszerbe.

1.1.1. E-mailben történő vírusküldés

Napjainkban még mindig nagy sikerrel alkalmazható a social engineering trükkjeit használó, rosszindulatú elemeket tartalmazó levelekkel történő vírusterjesztés.

A gyanútlan felhasználó megnyit egy fertőzött e-mail csatolmányt (általában ismeretlen, vagy ismerősnek tűnő feladótól), vagy egy rosszindulatú linket egy közösségi oldalon, vagy beérkezett levélben. Sok támadó rövidített URL-eket használ a rosszindulatú linkek elfedésére, így még nehezebb észrevenni, hogy az útvonal például egy fertőző kódot tartalmazó (JavaScript fájl) oldalra mutat. Bár ez a legnépszerűbb módszer, egyre inkább kezd elterjedtebb lenni a TOR-hálózaton megtalálható RaaS (Ransomware as a Service) megoldás is, ahol a rosszakaró gyakorlatilag egy szolgáltatásként vásárolja meg a hackerektől a támadást, amelynek esetleges bevétele után bizonyos részesedést kap az "eladó"[75]. Szerverek közvetlen megtámadására is van lehetőség, ha a támadó távoli asztali kapcsolaton, vagy terminálon keresztül elkezdi brute force-olni[76] a gyenge jelszavakat[77]. Amint sikerül így belépnie a gépre, már képes titkosítani az ott található adatokat. A fertőzött gépre történő

[75] Ilyen RaaS platform a felhasználó barát Satan platform is, ahol egyszerűen lehet a notPetya-hoz vagy a WannaCry-hoz hasonló vírust szolgáltatásként venni.

(Cisco Midyear Cybersecurity Report p. 23.) https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2 letöltés ideje: 2017.10.07.)

[76] Nyers erő segítségével történő jelszó feltörés, amelynek lényege, hogy nagy teljesítményű számítógépek lehetséges jelszó karaktersorozatok nagyon nagy számú permutációját próbálják végig a támadáskor, viszonylag rövid időn belül.

[77] 2017 januárjában a Keeper Security jelentése szerint a három leggyakoribb jelszó 2016-ban az *„123456”,* az *„123456789”* és a *„qwerty”* voltak. (The Most Common Passwords of 2016. https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf letöltés ideje: 2017.10.05.)

településekor a zsarolóvírus általában praktikusan megkeresi a jpg, .xls, .xlsx, .png, .doc, .docx, .ppt, stb. kiterjesztésű fájlokat, mivel a személyes és szenzitív adatok[78] nagyrészt képek és dokumentumok formájában vannak tárolva. Ezen adatok enkriptálása után történik meg maga a zsarolás: pénz (általában Bitcoin) ellenében ígérik, hogy feloldják a titkosítást.

A fent ismertetett módszerek közül ebben az esetben a számlaként álcázott -pdf kiterjesztésű fájlban történt a zsarolóvírus bejuttatása. Annak érdekében, hogy a levelezőrendszer ne szűrje ki automatikusan a kártevőt tartalmazó levelet, úgynevezett megbízható e-mail címeket használtunk, amelyekhez a hozzáférést a gyenge jelszavak feltörése és a hozzájuk tartozó gyanútlan felhasználói magatartás biztosították[79].

1.1.2. Az ajándékba küldött vagy elhagyott adathordozó eszköz

A PLC eszközöket megtámadó kártevő pendrive-on történő bejuttatásához, az egyik alapvető emberi tulajdonság, a kíváncsiság adta lehetőségeket használtuk ki.

A parkolóban elhagyott pendrive ötlete elég egyszerűnek és kézenfekvőnek tűnhet, azonban pont ez az egyszerűség kérdőjelezi meg a módszer hatékonyságát. Az alapelv az, hogy a vírust egy adathordozó tartalmazza, amelyet „véletlenül" a kiszemelt dolgozó autójának közelében hagynak el, aki kíváncsiságból felveszi és csatlakoztatva a számítógépéhez a vírus észrevétlenül bejuthat a hálózatba. A módszer jelentős kockázatának tekintjük, hogy nem garantálható az, hogy a célszemély fogja megtalálni, vagy egyáltalán felvenni az eszközt.
A módszer továbbfejlesztett változata, az „ajándékba küldött" pendrive trükk azonban több sikerrel kecsegtethet, így a Szolgáltató elleni támadás során is ezt a bejuttatási technikát

[78] Ebben az esetben a szenzitív adat lehet minden, a személyügyi osztály által kezelt személyes adat vagy a munkavállaláshoz elengedhetetlen szükségességű orvosi alkalmassági és vizsgálati dokumentumok), amelyeket a törvény fokozottabban véd – az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény 3. § (3) alapján.

[79] Az IBM Security 2016-os tanulmánya szerint a ransomware-ek által fertőzött e-mail-ek száma 6000%-kal növekedett az előző évhez képest. A támadók egyre keményebben próbálkoznak azzal, hogy a felhasználókat a saját levelezésükön keresztül fertőzzék meg. Ezek az e-mail-ek általában számlákat, kimutatásokat, jegyzeteket és egyéb, fontosnak tűnő tartalmú csatolmányokat tartalmaznak. (http://invenioit.com/security/ransomware-statistics-2016/ letöltés ideje: 2017.10.09.)

választottuk. Ebben az esetben egy konkrét személynek kézbesítik a fertőzött eszközt, egy olyan legendával övezve, amely szerint az adathordozót vagy valamilyen nyereményjátékon nyerte, esetleg egy partnercég, vagy más szolgáltató vállalat küldte ajándékba. Még hihetőbbé lehet tenni a történetet, ha egy bizonyos eseményhez kötjük a küldött eszközt.

A közösségi oldalon előzetesen leinformált[80] személynek küldött adathordozó esetében bármelyik történet hihető lehet, főleg akkor, ha az valamilyen cég, vagy olyan esemény emblémájával díszített, amely a közelmúltban került megrendezésre és tudjuk, hogy a címzett biztosan részt vett rajta. Anyagi vonzatát tekintve kimondottan könnyen kivitelezhető módszer, hisz pár ezer forintért szinte bárhol lehet logóztatni ilyen tárgyakat. Apró mozzanat, ám rendkívüli mértékben el tudja altatni a gyanakvást.

1.2. Az informatikai rendszerekben okozott károk

A Szolgáltató informatikai rendszerének alaprendeltetése, hogy a főváros ivóvíz-ellátását biztosító komplex rendszer folyamatosan működjön. Budapest vízellátását kettő vízbázis biztosítja:

→ az Északi vízbázis (Szentendrei-sziget), amely a város ellátásának 70%-átt biztosítja, valamint

→ a Déli vízbázis (Csepel-sziget), amely a maradék 30%-ot szolgáltatja.

A víztermelés módja azonban mind a két területen egyforma: a parti szűrésű vizet csápos kutak nyerik ki a Dunából. A kitermelt vízből elsőként a vas- és mangántartalmat vonják ki oxidációs eljárás folytán ózon segítségével. Ezt követően a szerves anyagokat távolítják el, végül pedig klórral fertőtlenítik az ivóvizet, hogy a mikrobák és férgek is elpusztuljanak a vízből[81]. A tisztítás után a víz egy tározó medencébe kerül (a Gellért-hegy

[80] A célszemély digitális lábnyomának felkutatására például remek eszköz lehet a http://www.uk-osint.net/ honlap. Ennek segítségével többek között az adott felhasználó összes Facebookos tevékenységét listázni lehet: elsőként a felhasználó adatlapjának URL címének bemásolásával egy numerikus azonosítót generálunk, majd annak segítségével megkapjuk például azt, hogy hány fényképen szerepelt, illetve milyen eseményeken vett részt. Mivel a legtöbb konferencia rendelkezik ún. Facebook-os eseménnyel, ahol a részvétel visszaigazolható, könnyen kaphatunk valós képet arról, mely rendezvények „reklámajándékaként" tudjuk a vírushordozó eszközt célba juttatni.

[81] http://budapest.hu/Documents/varosfejlesztesi_koncepcio_2011dec/11_Kozmuvek_jav.pdf (letöltés ideje: 2017.10.08.)

oldalában lévő szabadon látogatható) néhány órára, ahol keverőlapátokkal áramoltatják, így folyamatosan friss oxigénhez jut.

Feltételezzük, hogy a levelező rendszeren keresztül bejuttatott ramsomware és a PLC eszközöket célzó kártevő az informatikai rendszerben – egymástól függetlenül – ellehetetleníti működést. A zsaroló vírus esetében a kártevő, amely a fentebb említett – e-mailen történő – bejuttatási módnak köszönhetően került az informatikai rendszerbe, hozzáfér a hálózati meghajtókon tárolt fájlokhoz, azokat titkosítja és csak 900 dollár értékű Bitcoin megfizetése után bocsájtja rendelkezésre a feloldó kulcsot. Ennek köszönhetően a belső kommunikáció akadozik, valamint a munkavégzés ellehetetlenül.

Szinte a bejuttatott zsarolóvírussal egy időben a másik kártevő sikeresen felülírta a SCADA rendszer eszközei logikai vezérlőegységeinek alap programjait, aminek következtében a klóradagolás megszűnt, a keverőlapátok is leálltak, de a vízminőséget ellenőrző eszközök a szokásos 0,5 mg/liter klórértéket mutatják. Az áramoltatás hiányában az előzetesen nem tisztított vízben néhány óra alatt elszaporodnak a baktériumok és vírusok, amelyeknek jelentős az egészségre gyakorolt negatív hatásuk. Ennek kivitelezésére az éjszakai idősáv tűnt a legmegfelelőbbnek, mert reggelre szaporodnak el a vízben a baktériumok annyira, hogy tömeges megbetegedéssel lehessen számolni a délelőtti órákban, valamint a lakosság ivóvíz-felhasználása a reggeli, illetve az esti időszakban emelkedik meg jelentősen.

1.3. A lakosságra gyakorolt élettani hatások

Az ivóvízhálózatba került, az ivóvízminőségi követelményeknek nem megfelelő tisztaságú víz használata következtében számolni lehet tömeges emésztőrendszeri megbetegedéssel, amelynek hatását a 2006-ban történt miskolci esethez lehet hasonlítani, amikor tömegesen fordultak orvoshoz meg E. coli és calici fertőzés miatt[82]. Mindez elsősorban és kezdetben hányással, hasmenéssel járó tüneteket okoz, de közvetetten láz, tartósan pedig kiszáradás állapotába sodorhatja a beteget.

[82]Epidemiológiai Információs Hetilap – 13. évf. 23. sz. 2006. június 16. pp. 291-296. http://epa.oszk.hu/00300/00398/00208/pdf/00208.pdf (letöltés ideje: 2017.10.07.)

Elsősorban a kisgyermekek és idősek vannak kitéve a fertőzés miatti kiszáradás veszélyeinek. A fertőzés a beteg és idős, legyengült szervezetet jelentősen befolyásolhatja, valamint azokat a betegeket érintheti súlyosan, akik speciális kórházi ellátásra szorulnak. Az ő ápolási feladataikat nehezíti az, hogy a tömeges fertőzések miatt számos gyermek, illetve felnőtt jelentkezik kórházi ellátásra, ezért az egészségügyi intézményekben a betegek feltorlódnak, ezáltal növelve a továbbfertőzés lehetőségét és valószínűségét.

2. Fizikai támadás

Annak érdekében, hogy az okozott károk szélesebb körben fejtsék ki hatásukat és a kezelés/elhárítás nehezebben legyen kivitelezhető, elengedhetetlen lépésként ítéltük meg a fizikai támadás szükségét.

A külföldi, illetve sajnos a hazánkban is előforduló mintát alapul véve a Budapesti Közlekedési Zártkörűen Működő Részvénytársaság (a továbbiakban: BKV Zrt.) autóbusz garázsainak közelében, valamint egy metróvonalon, a reggeli csúcsidőszakban történő bombatámadás végrehajtása adja a támadássorozat második fázisát, amelynek következében a kialakuló közlekedési káosz akadályozni fogja az alternatív vízkészletek eljuttatását a város különböző pontjaiba, ezáltal a krízishelyzet tovább eszkalálódhat.

A művelet megtervezésekor, ahogyan az előbbiekben, nyílt forrású információkat használtunk fel, amelyhez a városban történő életvitelszerű tartózkodásból fakadó ismeretek, illetve az interneten fellelhető adatok szolgáltak támpontul.

2.1. A fővárosi tömegközlekedési csomópontokról elérhető nyilvános információk elemzése

Elsőként a két legnépszerűbb metróvonalat összehasonlítva kiválasztottuk azt az állomást, ahol a robbanószert tartalmazó táska elhelyezésre kerül. A forgalmi adatok elemzése az M2 és az M3 vonalat szállítási kapacitására, napi utas-számára, legnagyobb forgalmú állomására, valamint ennek csúcsforgalmára terjedt ki:

M2 vonal		M3 vonal	
Legnagyobb szállítási kapacitás (utas/h/ir.)	2 3 000	Legnagyobb szállítási kapacitás (utas/h/ir.)	2 8 200
Napi utasszám (munkanapokon)	4 51 627	Napi utasszám (munkanapokon)	6 26 179
Legnagyobb forgalmú állomás napi utasforgalma (fő)	7 7 521	Legnagyobb forgalmú állomás napi utasforgalma (fő)	7 5 976
Legnagyobb forgalmú állomás csúcsórai utasforgalma (felszállók)	1 1 297	Legnagyobb forgalmú állomás csúcsórai utasforgalma (felszállók)	9 792

1. sz. ábra: A vizsgált metróvonalak forgalmi adatai[83]

A két metróvonal közös pontja az, hogy mindkét esetben a Deák Ferenc téri megálló a legnépszerűbb és a leginkább terhelt, a reggeli csúcsidőben körülbelül százezer fő halad át a területen, ezért a robbanószerkezetet a legnagyobb pusztítás érdekében ott célszerű elhelyezni reggel 8 óra körül, mert a nagy tömegben egy-egy elhagyott táska kevésbé kelt nagy feltűnést.

Az interneten – jelenleg bárki számára – elérhető információk szerint Budapesten öt autóbusz garázst üzemeltet a BKV Zrt., amelyek pontos címe szintén nyilvános, így a kész robbanó csomagok könnyen célba juttathatók, legegyszerűbben hajléktalanok közreműködésével, akik szerepe abban merül ki, hogy az általuk nem ismert tartalmú táskákat a kijelölt helyekre leteszik bizonyos pénzösszeg fejében.

Feltételezzük, hogy a két, egymást követő robbantás-sorozat a helyszínek alapos megválasztásával a maximálishoz közeli rombolási hatásfokot érte el.

2.2. A bombák készítésének módszere, az alapanyagok beszerzésének lehetőségei

A 2016-os Teréz körúti robbantás[84] kapcsán vetődött fel ismét, hogy hazánkban milyen „hatékonysággal” lehet a bűnüldöző szervek figyelmének felkeltése nélkül robbanószerkezeteket előállítani. Az interneten számos módszer fellelhető a házilag

[83] A táblázat forrásai: http://metros.hu/vonal/jellemzok_m2.html; http://metros.hu/vonal/jellemzok_m3.html (letöltés ideje: 2017.10.01.)

[84] 2016. szeptember 24-én este a Teréz körúton egy üres üzlethelyiség bejáratánál robbant fel az a hátizsákba rejtett bomba, amely súlyosan megsebesített két rendőrt. Bár számos járókelő haladt el a csomag előtt, a támadó célpontjai kifejezetten rendőrök voltak. A robbantás nagysága, illetve az, hogy a támadó közvetlen közelről hozta működésbe a szerkezetet, arra enged következtetni, hogy már korábban is készíthetett hasonló pokolgépeket, annyira pontosan voltak az összetevők kimérve, illetve többször is ki kellett próbálnia a szerkezetet, ami alapján meg tudta azt állapítani, hogyan lehet úgy legközelebb a robbantáshoz, hogy ő azt sértetlenül ússza meg. http://hvg.hu/itthon/20160926_Hidegverrel_lepett_at_aldozatain_a_robbanto (letöltés ideje: 2017.10.01.)

elkészíthető pokolgépekről. A két leghíresebb mű az *Anarchist Cookbook*[85] és az Iszlám Állam Inspire nevű magazinjában megjelent *Make a bomb in the kitchen of your Mom*[86]. Az itt szereplő robbanószerkezetek vegyi összetételét tekintve megegyeznek abban, hogy olyan, szinte bárhol beszerezhető alapanyagokból állnak, mint például az aceton, a hidrogén-peroxid és sósav. Ezeken kívül az időzített és/vagy késleltetett működtetésű, házi készítésű robbanószerkezetek szerkezeti felépítésüket tekintve egy zárt áramkörből, gyújtási láncból állnak, az időzítő, késleltető szerkezetnél megszakítva[87]. Az elektromos indító szerkezet alapja is lehet egyszerű használati tárgy, mint például egy karóra, vagy akár egy mobiltelefon.

A megszerzett ismeretek birtokában elkészített távvezérlésű pokolgépeket ezek után már csak egy hátizsákba kell helyezni, majd azokat a hajléktalanok által eljuttatni az alapos mérlegelést követően kiválasztásra került pontokra. A hátizsákok beszerzésénél arra kell ügyelni, hogy azok nehezen lekövethető, a lehető legátlagosabb darabok legyenek, amelyek bármelyik aluljáróban vagy kínai üzletben készpénzes fizetés során megvásárolhatóak.

2.3. A robbantások által okozott károk összegzése, hatása a lakosságra

A fent említett módszerekkel elhelyezett bombák robbanásakor nem csak a kiesett metróvonal pótlására szolgáló buszok üzembe állítása lehetetlenül el. A robbantások helyszínét – várhatóan nagy sugarú körben – teljesen lezárják, a helyszínekre vezető útvonalakon jelentős mértékben korlátozzák a gyalogos és gépjárműves közlekedést, különös tekintettel a mentők és a tűzoltó egységek számára biztosítandó felvonulási utak érdekében. A robbantási helyszíneken tartózkodók menekülése és pánikreakciója várhatóan negatívan befolyásolja a mentési tevékenységet, míg a város távolabbi pontjain feltorlódott tömegek a

---

[85] 1970-ben William Powell írta, tiltakozva az USA vietnámi háborúban aktívan részvevő kormányzata ellen. Bár a könyv lassan 50 éves lesz, a mai napig fellelhető az interneten, illetve folyamatosan bővítik azt. https://uniteyouthdublin.files.wordpress.com/2015/01/anarchist-cookbook-william-powell.pdf (letöltés ideje: 2017.08.22.)

[86] 2010 nyarán jelent meg a magazin, amelynek 33. oldalán a mai napig elérhető a tartalom. https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf (letöltés ideje: 2017.08.27)

[87] Daruka Norbert: A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei, különös tekintettel a tűzszerész feladatok ellátására. Doktori (PhD) értekezés p. 40. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2014/daruka_norbert.pdf (letöltés ideje: 2017.08.26.)

mindennapos, reggeli forgalmi dugók méretét duzzasztják tovább. A helyzetet leginkább az az már megtörtént esemény szemlélteti, amikor 2016 decemberében az M2 metró Pillangó utcai megállójánál két szerelvény összeütközött[88]. A baleset következtében a reggeli csúcsforgalom egyik csomópontjától (Örs vezér tér) a Puskás Ferenc Stadion metróállomásig csak pótló buszok közlekedtek, amelyek kapacitása eleve nem volt elegendő az utasok száma tekintetében. Az ezzel párhuzamosan kialakult, jelentős forgalmi dugót tovább súlyosbította, hogy az utasok a gyorsabb utazás reményében a taxi társaságokhoz fordultak. Aznap reggel 9 órára a XIV. kerületben egyik személyszállítást végző társaság autója sem volt elérhető, így a város más pontjairól érkezőkre is átlagosan 40 percet kellett várni.

Ilyen körülmények között belátható az, hogy az ivóvíz-ellátás pótlására tett intézkedések keretében történő vízosztás azokon a helyeken is akadályokba fog ütközni, ahol leginkább szükség van emberi fogyasztásra alkalmas vízre (pl.: elsősorban egészségügyi és szociális intézmények).

Az ismertetett következmények mellett nem elhanyagolható az utazó közönség általános elégedetlensége, ami negatív irányba fogja befolyásolni a közhangulatot, ez pedig a támadás harmadik lépésének kivitelezésékor elengedhetetlen fontossággal bír.

3. Mesterségesen szított megmozdulások a fővárosban

A Szolgáltató ellen intézett informatikai támadás, illetve a város több pontján történt robbantás rövid időn belül a médiaszolgáltatók vezető hírei között szerepel, folyamatos és több oldalról érkező tudósításokra lehet számítani. A kezdeti zűrzavar miatt a dezinformáció ez esetben is komoly veszélyforrásnak számít, amely a lakosság viselkedését és a közvéleményt jelentősen befolyásolhatja. Az álhírek felbukkanását egy ideig lehetetlen kiszűrni, valamint a sajtóhoz eljuttatott információk valódiságát – elsősorban idő hiányában – szinte lehetetlen ellenőrizni. A szenzációhajhászás időszakában (az első egy órában) megindulnak a találgatások, illetve a fél információk alapján az egymást generáló hamis, vagy csak féligazságot tartalmazó hírek villámgyors terjedése.

[88] http://hvg.hu/itthon/20161205_baleset_miatt_nem_jar_a_2es_metro (letöltés ideje: 2017.08.12.)

Mindez a fővárosban várhatóan kisebb-nagyobb csoportok „összeverődéséhez” vezethet, vagy megmozdulásokat generálhat, amelyek a „kritikus tömeg elmélet” mentén akár tüntetés jellegű problémagócokká nőhetik ki magukat.

Ezt az általános tömegviselkedést kívánjuk felhasználni arra, hogy a Szolgáltató informatikai és a tömegközlekedés fizikai támadását követően, a rendvédelmi szerveket túlterheljük, aminek köszönhetően a kárelhárítás akadályoztatva lesz.

3.1. A közösségi oldalak és a média szerepe

Ahogyan arra Kovács László és Krasznay Csaba is rámutatott a Digitális Mohács című műben: *„már komoly befolyásoló tényezőként számolhatunk ezekkel a hírportálokkal a lakosság egészét tekintve. Itt következik a pszichológiai hadviselés következő fázisa. Ha nem is könnyű feladat, mégis lehetséges hamis híreket elhelyezni a különböző hírportálokon, azok meglévő és többször bizonyított sebezhetősége és sérülékenysége miatt. Amennyiben ezek a hamis hírek egymással összefüggnek, illetve a különböző blogokon is megjelennek, már komoly mértékű pánikot is okozhatnak.”*[89]

Az úgynevezett „médiahack” több irányból történő, célzott manipulálása biztosítja a lakosság egységességének megbontását. A robbantásokat követően a bulvársajtónak eljutatott, megbízhatónak beállított, neve elhallgatását kérő, rendvédelmi szervekhez közel álló forrásoktól kapott információk azt sugallják, hogy a támadássorozat mögött az Iszlám Állam[90] áll, amelynek tagjai a magyarországi muszlim közösségben rejtőznek. Ez az információ, illetve hamis profilokkal történő gyűlöletkeltés a közösségi oldalakon hamar fellobbantja a muszlim kisebbség iránti ellenszenvet, amelynek következtében fizikai atrocitásokkal is lehet számolni.

Feltételezhető, hogy a robbantások után a lakosság inkább bezárkózik, ezért az egyetlen mód, amellyel nagyobb tömegeket az utcára lehet szólítani, a reggeli robbantásokban elhunyt áldozatokra való nyilvános megemlékezés kezdeményezése. Ahhoz, hogy ez a legszélesebb

[89] Kovács László, Krasznay Csaba: A digital Mohács. p. 49.

[90] Az elmúlt hónapokban, Európában elkövetett terrortámadásokért azonnal vállalt felelősség, valamint az, hogy a szervezet kísérletet tett arra, hogy magára vállalja a 2017 októberének első napjaiban elkövetett Las Vegas-i merényletet, még inkább hihetővé teszi az Iszlám Államhoz fűzhető kapcsolódás tényét.

közönséghez elérjen[91], célszerű Facebookon meghirdetni egy eseményt, figyelemmel arra is, hogy a terrorveszélyhelyzet kihirdetése után az előre bejelentett tüntetéseket a gyülekezési jog korlátozásával valószínűleg nem fogják engedélyezni. Így azonban tűnhet egy „spontán" összegyűlésnek.

Célszerűnek tartjuk azt is, hogy a megemlékezés időpontjában a muszlim közösségnek is szervezzünk egy megemlékezést a „Not in my name[92]" jegyében azért, hogy kifejezhessék részvétüket és hangot adhassanak annak, hogy nem osztják a radikális muszlim nézeteket.

3.2. A tömeges megmozdulásokból eredő kockázatok vizsgálata

Az előzőekben felvázolt szerveződések – az álhíreknek köszönhetően – hamar fordulhatnak tömeges, elégedetlen, akár politikailag is átitatott, ellenséges demonstrációba.

A terrortámadás alapvető traumája és az egész nap közösségi oldalakon hergelt, valamint bulvársajtóban megjelent ellenséges és megosztó cikkek hatására a résztvevők egy eleve felfokozott lelki állapotban érkeznek a helyszínekre. Mindezt egy-két „beépített személy" könnyen kiaknázhatja pár elejtett megjegyzéssel, gondolunk itt a muszlim tömegben egy hangosan elkiáltott „megérdemelték sorsukat a hitetlenek", vagy a gyászoló tömegben a muszlim közösséget okoló mondatokra. A tömegben elvegyülő, konfliktust szító egyének szinte láthatatlanok maradnak, de a két csoport összeütközése gyakorlatilag elkerülhetetlen. Az ilyen jellegű tömeges rendbontás nemcsak az ivóvíz általi fertőzés további terjedését segítheti elő, hanem a kialakuló konfliktushelyzetben esetlegesen megsérült emberek ellátásával is tovább terheli az amúgy is kapacitása végén járó egészségügyi ellátó rendszert.

Rendvédelmi szempontból azonban felmerülhet az is, hogy a tömeg potenciális célpontot nyújt egy újabb merényletre, így a rendőrség a feloszlatás vagy a biztosítás dilemmájába kerül.

---

[91]Okkal feltételezhető a részvételi hajlandóság az alapján, hogy a más országokban elkövetett terrorcselekmények kapcsán – együttérzésük kifejezésére – emberek ezrei változtatják meg a közösségi oldalakon szereplő profilképeiket az érintett ország zászlajára.

[92]http://www.thehindu.com/news/national/what-is-not-in-my-name-all-about/article19194499.ece (letöltés ideje: 2017.10.07.)

A biztosítás újabb erőket von el a hatóságoktól, akik a nyomozáson és a krízishelyzet felszámolásán dolgoznak, azonban ha a feloszlatás mellett döntenek, sajnos fennáll annak a veszélye, hogy a demonstrálók/megemlékezők a rendőrökre támadnak, akik a testi kényszer alkalmazása miatt ellenszenvet váltanak ki a lakosságból, amely akár ismételten akadályozhatja a szakszerű intézkedéseket. Bármely változatot is választják, a támadók elérték céljukat: az alkotmányos rend felborult, illetve a lakosság egységessége is, amely tovább súlyosbítja a következménykezelés nehézségeit.

A kialakult krízis kezelésének dimenziói

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete[93] a kritikus infrastruktúrák között nevesíti az ivóvíz-szolgáltatás létesítményeit. A kritikus infrastruktúrák a lakosság alapvető ellátásában nélkülözhetetlen szerepet töltenek be, ezért védelmüket állami és üzemeltetői szempontból is prioritásként kell kezelni.

A tanulmány második részében a fővárosban uralkodó helyzet felszámolásához szükséges intézkedéseket, illetve a meghatározott jogszabályok alkalmazása által teendő válaszlépéseket ismertetjük. Megvizsgáljuk továbbá a magánszektor bevonásának egyes lehetőségeit, amelyek a beavatkozói, a kárelhárításért felelős, a nyomozati és a rendfenntartásra rendelt szervek tevékenységét segíthetik.

1. Az eseménysor kezelésének katasztrófavédelmi szempontú összefoglalása

Tárgyalt helyzetben terrortámadás történt, tehát az Országgyűlés a kormány kezdeményezésére meghatározott időre terrorveszélyhelyzetet hirdethet ki az Alaptörvény 51/A. cikk értelmében, amelynek kihirdetéséhez, meghosszabbításához a jelen lévő országgyűlési képviselők kétharmadának szavazata szükséges.

[93] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete

„(4) A Kormány a terrorveszélyhelyzet idején rendeletet alkothat, amellyel - sarkalatos törvényben meghatározottak szerint - egyes törvények alkalmazását felfüggeszthetti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat.

(5) A Magyar Honvédséget a (3) bekezdés szerinti intézkedések hatályossága és a terrorveszélyhelyzet idején akkor lehet felhasználni, ha a rendőrség és a nemzetbiztonsági szolgálatok alkalmazása nem elegendő."[94]

A Kormány első intézkedései között azonnal kirendeli a rendvédelmi szervek megerősítésére a Magyar Honvédséget (a Magyar Honvédség *belföldi* alkalmazása), elsősorban a kiemelt létesítmények (például kritikus infrastruktúrák) védelmére. A helyzet kezelésére a katasztrófavédelem alaprendeltetését és működését tekintve a veszélyhelyzeti (Magyarország Alaptörvénye, 53. cikk) állapotnak megfelelő intézkedések történnek. A beavatkozás jogszabályi alapját és hátterét Magyarország Alaptörvényéből következően

→ a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény, valamint

→ a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvények jelentik.

Rendkívüli esemény során kettő, kifejezetten a Kormány döntéseit előkészítő kormányszerv láthat el javaslattevő, véleményező, illetve szakmai tanácsadó tevékenységet a védelmi-, illetve a honvédelmi igazgatás területein:

→ a Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoport (a továbbiakban: HIKOM), valamint

→ a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság (a továbbiakban: KKB).

A HIKOM alaprendeltetése a Honvédelmi Tanács[95] és a Kormány speciális működési feltételeinek biztosításával összefüggő feladatok tárcaközi egyeztetése. Feltételezett helyzet belbiztonsági természetéből adódóan nem indokolja fenti munkacsoport működtetését,

[94] Magyarország Alaptörvénye *51/A. cikk*

[95] A Honvédelmi Tanács összehívása a honvédelmi típusú különleges jogrendben (hadiállapot kinyilvánítása vagy idegen hatalom fegyveres támadásának közvetlen veszélye, rendkívüli állapot) esetén lehetséges.

azonban a Honvédelmi Minisztérium létre hozhat a KKB munkáját támogató, szakértő munkatörzset.

A KKB a katasztrófavédelemmel összefüggésben döntés-előkészítő, valamint a katasztrófák elleni felkészüléssel, megelőzéssel, védekezéssel és helyreállítással kapcsolatban koordinációs feladatokat lát el. A KKB, a katasztrófák elleni védekezéssel kapcsolatos tudományos, elemző- és értékelő tevékenysége mellett – operatív munkaszerve útján – koordinálja a védekezésben részt vevő központi államigazgatási szervek védekezéssel kapcsolatos szakmai tevékenységét, javaslatot tesz a felmerült védekezési költségek biztosítására, és a rendelkezésre álló, illetve vis maior pénzeszközök felhasználására.

A feltételezett esemény következtében kihirdetett terrorveszélyhelyzet a veszélyhelyzetnél magasabb szintű jogrendi tényállás, azonban a KKB-t a veszélyhelyzeti különleges jogrendi állapotnak megfelelően alkalmazzák, amellyel a kiemelt létesítmények üzemzavara, működési elégtelensége, működésképtelensége és a lakosság alapvető ellátásában keletkező üzemfolytonosság akadozása/szünetelése kezelhető. Az 1824/2015. (XI. 19.) Korm. határozat alapján továbbá kritikus szintre emelik a terrorfokozatot, a védelmi igazgatás rendszere összességében tehát terrorelhárítási prioritással működik, míg a katasztrófahelyzet elhárítása és kezelése a veszélyhelyzeti állapotnak megfelelően szerveződik.

A katasztrófaveszély időszakában és a veszélyhelyzet során ellátandó feladatokat, valamint a veszélyhelyzetre vonatkozó sajátos irányítás szabályait a Katasztrófavédelmi törvény végrehajtási rendelete[96] tartalmazza, amely részletezi a területi és helyi védelmi igazgatási szintek katasztrófák elleni védekezéssel összefüggő feladatait. A magyar védelmi igazgatási rendszer hierarchiája alulról építkezik az alábbiakban részletezett formában.

[96] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. tv. végrehajtásáról szóló 234/2011. (XI. 10.) Korm. rendelet.

Települési szint (főpolgármester, polgármester)

A Katasztrófavédelmi törvény alapján – veszélyhelyzet időszakában – a hivatásos katasztrófavédelmi szerv által kijelölt tiszt segíti a polgármester védekezéssel/beavatkozással kapcsolatos tevékenységét és közreműködik az okozott károk felmérésében.

Egyeztetve más rendvédelmi, közigazgatási és a gazdálkodó szervek kijelölt kapcsolattartóival, összegzik a károsult eszközrendszert (például buszok, lakóingatlanok, egyéb létesítmények), hogy abból meghatározhatók legyenek a helyreállításhoz szükséges erőforrások. A polgármester részt vesz továbbá a védekezésben részt vevő erők váltásának, pihentetésének és ellátásának szervezésében is. Erre a célra kijelölhetők például sportlétesítmények tornacsarnokai, vagy konferenciatermek, amelyről – szükség esetén – hatósági határozatot kell hozni (katasztrófavédelmi célú gazdasági és anyagi szolgáltatások fővárosi szintű igénybevétele). Jelen esemény kezelése kapcsán, gazdálkodó szervezetek meghatározott körét érintően, igénybe kell venni például ivóvíz/élelmiszer/takarmány szállítására alkalmas szállítóeszközöket, szerelvényeket, tartályokat, mobil mosdóhelyeket és fertőtlenítő szereket, valamint ezek szállítókapacitását, a szállításukra alkalmas járműveket.

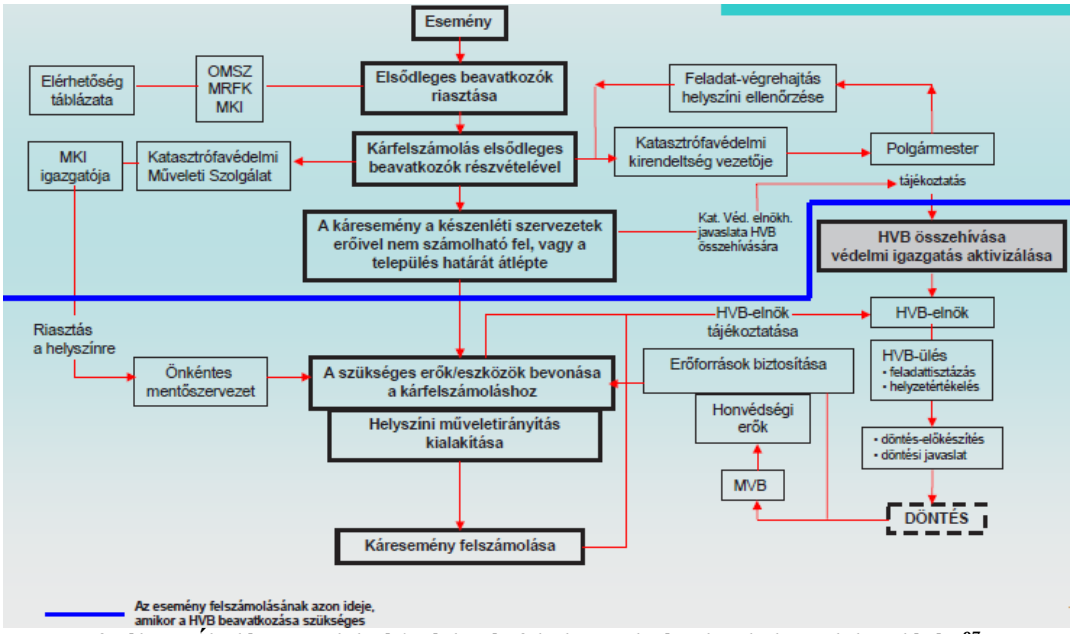
A polgármester a katasztrófavédelmi szempontból I. és II. veszélyességi osztályba sorolt településen (a katasztrófák elleni védekezésre való felkészülési, védekezési és helyreállítási szakmai feladataiban, továbbá a rendvédelmi és honvédelmi feladataiban közreműködő) közbiztonsági referenst jelöl ki. A felvázolt terrortámadás által érintett kerületek jelentős része az I. és a II. kategóriákba van sorolva *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény IV. fejezetének* hatálya alá tartozó üzemek általi veszélyeztetettség alapján. Ebből adódóan a kijelölt referens feladatai a tárgyalt cselekmény időszakában:

- → előkészíteni a polgármester védekezéssel kapcsolatos szakmai döntéseit a lakosság és a létfenntartáshoz szükséges anyagi javak védelme érdekében,
- → kapcsolatot tartani a védekezést irányító és a védekezésben közreműködő szervekkel, erről tájékoztatni a polgármestert,
- → részt venni a kitelepítés, kimenekítés, befogadás és visszatelepítés feladataiban, amennyiben szükséges.

Helyi szint (Helyi Védelmi Bizottság, a továbbiakban: HVB)

A HVB a Megyei Védelmi Bizottság irányítása alatt működik, meghatározza a beavatkozás/védekezés helyi feladatait, ellenőrzi azok végrehajtását, illetve elrendeli a települési polgári védelmi erők bevonását, koordinálja a védekezésben részt vevő polgármesterek védekezési tevékenységét. A HVB elnöke a katasztrófavédelmi feladatok ellátásával kapcsolatos döntésekről tájékoztatja a Fővárosi Katasztrófavédelmi Igazgatóság igazgatóját, felelős továbbá a lakosság veszélyhelyzeti tájékoztatásáért. A fővárosi kerületekben is HVB működik, amelyek illetékességi területe a fővárosi kerületekhez igazodik. Tevékenysége keretében gondoskodik a helyreállítás meghatározott sorrendjének és ütemének megvalósításáról, folyamatos kapcsolatot tart az érintett létesítményekkel. Intézkedik továbbá a védekezéshez igénybe vehető állomány és eszközök átcsoportosításáról és bevonásáról, illetve a lakosság alapvető ellátásának biztosításáról a normál életkörülmények helyreállításáig.

Feltételezett esemény kapcsán a robbantás-sorozat elsősorban és időbeliségét tekintve a katasztrófavédelem tűzoltó erőinek beavatkozását igényli. Az első robbantást követően exponenciálisan emelkedik a Fővárosi Katasztrófavédelmi Igazgatóság főügyeletére beérkező, a robbanásokról szóló hívások száma, illetve később a szennyezett, bűzös ivóvízzel kapcsolatban is egyre több lakossági bejelentés érkezik, ami jelentősen leterheli a Tevékenység-irányítási Központot (a továbbiakban: TIK) és nagymértékben megnehezíti az egységes segélyhívás-fogadást a 112-es telefonszámon. A TIK hamarosan tömeges jelzésként fogja kezelni az esemény bejelentéseit, hogy biztosítsa a fővárosi erők, eszközök és események átláthatóságát, ezzel egy időben, a jelentési rendnek megfelelően, értesítik a fővárosi katasztrófavédelmi igazgatót. Az első bejelentést követő egy órán belül az illetékes polgármesterek tájékoztatása megtörténik, összeülnek az érintett helyi védelmi bizottságok, majd a fővárosi védelmi bizottság is. Eközben a Kormány az Országgyűlés összehívására intézkedik. Az alábbi ábra szemlélteti az eseménysor eszkalálódásának kezelését területi szintig.



2. ábra: Általános cselekvési vázlat és feladatrend váratlan helyzetek kezelésére[97]

Területi szint (Megyei Védelmi Bizottság, tárgyalt estben Fővárosi Védelmi Bizottság, a továbbiakban: FVB)

Az FVB a KKB operatív munkaszerve – közvetetten a kormány – irányítása alatt működik, meghatározza a védekezés területi feladatait, ellenőrzi azok végrehajtását, elrendeli a területi polgári védelmi erők bevonását, a hatáskörét meghaladó esetekben kormánydöntést kezdeményez, koordinálja a védekezésben részt vevő helyi védelmi bizottságok, polgármesterek tevékenységét.

A felvázolt helyzetben az FVB legfontosabb feladata a lakosság tájékoztatása mellett (későbbiekben kifejtve) fenntartani a tűzoltóvíz-utánpótlást és megszervezni ennek kivitelezését. Erre alkalmas lehet a Dunából történő felszívásos táplálás láncolatának kialakítása. Ezzel párhuzamosan a veszélyes anyagokkal foglalkozó üzemeket haladéktalanul tájékoztatni kell a víz összetételének megváltozásáról, és intézkedni szükséges a visszafordíthatatlan vegyi reakciók megelőzésére. Ha indokolt, az érintett üzemi és létesítményi kör működését határozatlan időre be kell szüntetni.

[97] Baán Mihály, Bors István, Csifféry Tamás, Hári László, Kocsis Lajos, Szentes László: Magyarország védelmi igazgatása a közigazgatás új környezetében

Tekintettel az ivóvíz fertőzés miatti megbetegedések, a terrorcselekményben megsérült, valamint az egyéb tömeges megmozdulások során sérüléseket szenvedett személyek számára, egészségügyi szakállományt kell vezényelni a területileg illetékes kórházakba, elsősorban a további fertőzéses megbetegedések kezelésére történő felkészülés céljából. Budapest Főváros Kormányhivatala Népegészségügyi Főosztályának bevonásával fel kell készülni a járványokra és a szükséges ellenanyag-mennyiségre, megfelelő típusú és mennyiségű fertőtlenítőszerek beszerzésére. Szintén gazdálkodó szervezetek útján kell megszervezni ideiglenes mosdóhelyek kihelyezését, fertőtlenítését, illetve az ott keletkező szennyvíz folyamatos gyűjtését és szállítását. A fertőtlenítőszerek nagy mennyiségű szállítására és kijuttatására a honvédség szállító-, és mentesítő eszközei a legalkalmasabbak. Biológiai veszély esetén fent kell tartani a mentesítés és fertőtlenítés folytonosságát, a folyamatos utánpótlást, illetve számításba véve a behatási időt.

A Nemzeti Közlekedési Hatóság bevonásával le kell állítani a főváros területére belépő járműforgalmat és meg kell tervezni annak elkerülhetőségét, számolva az utak és hidak befogadó kapacitásával.

Fenti feladatok kiemelt létszámú rendőri biztosítást igényelnek, ezért további rendőri erőket kell vezényelni a fővárosba, a honvédség erre nem elegendő és nincs felkészítve kifejezetten rendvédelmi feladatok ellátására. A rendőri erők átcsoportosítása során kiemelt figyelmet kell szentelni a Rendőrség határvédelmi feladatainak ellátására is.

Az FVB elnöke a katasztrófavédelmi operatív feladatok ellátásához – a Fővárosi Katasztrófavédelmi Igazgatóság közreműködésével – a célnak megfelelően kialakított és felszerelt, folyamatosan üzemképes állapotban tartott vezetési pontot és annak támogatása érdekében operatív munkaszervet működtet. A védekezési feladatok végrehajtását (az FVB döntésének megfelelően) a Fővárosi Katasztrófavédelmi Igazgatóság igazgatója, vagy az által kijelölt személy hangolja össze. A fővárosi védelmi bizottság területi operatív munkaszervével folyamatosan együttműködik valamennyi érintett helyi védelmi bizottság mellett működő helyi operatív munkaszerv.

A lakosság védelmének alapvető módszerei a helyi és a távolsági védelem (kimenekítés, kitelepítés, átmeneti jellegű elhelyezés befogadó helyen, elzárkózás). Vizsgált esemény során a lakosságvédelem legindokoltabb módszere a helyben megszervezett ellátás, az alábbi feladatok végrehajtásával:

→ folyamatos ivóvíz és élelmiszer biztosítása,

→ lemosó- és fertőtlenítő anyagok biztosítása,

→ mosdó- és fertőtlenítő helyek telepítése.

Kizárólag az önellátásra képtelen, vagy különösen veszélyeztetett személyeket (például várandós, vagy csecsemőjét gondozó nők) célszerű erre a célra kialakított befogadó helyeken – a megfelelő szakellátás biztosítása mellett – elhelyezni. A főváros összes érintett vízfogyasztójának kimenekítése akadályozná a veszélyhelyzeti szolgálatok beavatkozó- és logisztikai tevékenységét, valamint lassítaná a helyreállítást is.

A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) készíti elő a közszolgálati műsorszolgáltatók által végzett lakosság tájékoztatási háttéranyagokat, a veszély jellegére vonatkozó tájékoztatót és a követendő magatartási szabályokat tartalmazó közleményeket. A Fővárosi Katasztrófavédelmi Igazgatóság szervezi a lakosság közvetlen – helyben szokásos módon történő – tájékoztatásával kapcsolatos területi és helyi feladatokat, folyamatosan együttműködve és egyeztetve az üzemzavarban érintett kritikus infrastruktúra üzemeltetőjével, a rendőrséggel, a honvédséggel és az országos tiszti főorvossal. A veszélyhelyzeti tájékoztatás tartalma ez esetben:

→ a bekövetkezett esemény, a helyzetkezelés részcselekményei;

→ a megtett és tervezett lakosságvédelmi intézkedések;

→ az elrendelt korlátozások és az irányadó magatartási szabályok;

→ a további tájékozódási lehetőségek.[98]

[98] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

Központi szint (Országgyűlés, Kormány, KKB)

Ahogy az már említésre került, a vizsgált esetben az Országgyűlés a Kormány kezdeményezésére terrorveszélyhelyzetet hirdet ki és felhatalmazza azt rendkívüli intézkedések bevezetésére. A terrorcselekmény létfontosságú rendszerek és létesítmények működésének megzavarásával közvetlenül veszélyezteti az élet- és vagyonbiztonságot, tárgyalt helyzetben humán járvánnyal, vagy járványveszéllyel, állatjárvánnyal, a felszíni és felszín alatti vizek haváriaszerű szennyezésével, amelyek elhárítása érdekében a Kormány – a fent bemutatott védelmi igazgatási struktúrán keresztül – rendkívüli intézkedéseket vezet be. A védekezés/beavatkozás időszakában a KKB látja el a Kormány számára történő döntés-előkészítési feladatokat. Jelen terrorcselekmény vonatkozásában a kialakult helyzet kezelése szempontjából különösen fontos a KKB jogszabály szerinti összetétele:

Elnök	belügyminiszter		
Elnökhelyettes	az elnök által kijelölt tag		
Tagok	honvédelmi miniszter	igazságügyi miniszter	
	külgazdasági és külügyminiszter	nemzetgazdasági miniszter	
	emberi erőforrások minisztere	nemzeti fejlesztési miniszter	
	földművelésügyi miniszter	Miniszterelnökséget vezető miniszter	
	miniszterelnök kabinetfőnöke által kijelölt állami vezető	belügyminiszter rendészeti államtitkára	
Állandó, tanácskozási jogú tagok	BM OKF főigazgatója	országos rendőrfőkapitány	Honvéd Vezérkar főnöke
	KKB Tudományos Tanácsának elnöke		
	KKB NVK vezetője		
	KKB adminisztratív feladatait ellátó szervezeti egység vezetője		
Elnök	Bevándorlási és Menekültügyi Hivatal főigazgatója		

döntése és meghívása alapján, tanácskozási jogú tagok	büntetés-végrehajtás országos parancsnoka
	polgári nemzetbiztonsági szolgálatok főigazgatói
	KKB NVK vezetőjének szakmai helyettese
	Országos Atomenergia Hivatal főigazgatója
	országos főállatorvos
	Országos Meteorológiai Szolgálat elnöke
	Országos Mentőszolgálat főigazgatója
	Nemzeti Adó- és Vámhivatal elnöke
	Nemzeti Média- és Hírközlési Hatóság elnöke
	Állami Egészségügyi Ellátó Központ főigazgatója,
	az Országos Vízügyi Főigazgatóság főigazgatója
	Pest Megyei Kormányhivatal kormánymegbízottja
	annak az MVB-nek az elnöke, akit a napirenden szereplő kérdés érint

3. sz. ábra: A KKB összetétele[99]

A 3. sz. ábrán szürke hátterű cellák mutatják, hogy az eseménykezelés során meghatározó szerepet betöltő szervek magasszintű képviselete biztosított. Ugyanakkor a felvázolt esemény sajátosságaira való tekintettel indokolt lenne megvizsgálni annak szükségességét, hogy a KKB ülésén állandó jelleggel, tanácskozási joggal részt vevők körébe delegálják – legalább terrorveszélyhelyzet kihirdetett időszakában – a Terrorelhárítási Központ főigazgatóját és a Nemzeti Nyomozó Iroda igazgatóját (vagy a Készenléti Rendőrség, mint felettes szerv parancsnokát).

Országos szintű koordinációt, az érintett és közreműködő szervek hatékony és eredményes együttműködését igényli az alábbi – a területi és helyi szervek által megkezdett, azok képességeit és kapacitásait feltételezhetően meghaladó – feladatok végrehajtása:
→ a csatornázási művek összes szivattyújának leállítása, a rendszer „leengedése”;

[99] A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság létrehozásáról, valamint szervezeti és működési rendjének meghatározásáról szóló 1150/2012. (V. 15.) Korm. hat.

→ lakosság folyamatos és hiteles tájékoztatása, társszervek tájékoztatása a végrehajtott feladatokról, nemzetközi média valós információkkal történő ellátása;
→ tűzoltóvíz biztosítása felszívásos táplálás módszerével a Dunából több, folytonos csatornát fenntartva, vízszállítók vezénylése a főváros kerületeibe;
→ ivóvíz és élelmiszer (a kitelepítésben/kimenekítésben érintettek) biztosítása a lakosság számára, vízszállításra és kiosztásra alkalmas eszközök, tartányjárművek bevonása (élelmiszeriparból pl. tejszállítók kb. 24 tonna kapacitással);
→ kórházi ügyeletek megerősítése, felkészülés az emésztőrendszeri betegségek és fertőzések tömeges kezelésére, ellenanyag-készletek megerősítése, nemzetközi segítségnyújtás igénybevétele (UN OCHA, EU polgári védelmi mechanizmus);
→ lakossági mobil mosdó- és fertőtlenítő helyek telepítése;
→ fenti feladatok kiemelt rendőri (nem honvédségi) biztosítása;
→ fertőtlenítőszer-készletek beszerzése és kijuttatása, volumen tekintetében a dekontaminálásra csak a Magyar Honvédség képes;
→ a fővárosba belépő (civil) járműforgalom korlátozása, szükség esetén leállítása.

2. A bűnüldöző szervek feladatai

Jelen szituációban egy olyan rendkívüli eseményt kell felszámolnia a hatóságoknak, amely a folyamatos rendelkezésre állást ellehetetleníti úgy, hogy az informatikai támadás sikeres végrehajtásával okkal feltételezhetővé válik, hogy bármely ivóvíz-szolgáltatásért felelős rendszer sérülékenysége jelentős mértékben megnövekedett. A nyomozás szempontjából fontos tisztázni, hogy a kritikus infrastruktúra védelem rendszerében nevesített víz ágazaton belül, az 5 alágazatból egyet érintett közvetlenül a támadás, mégpedig az ivóvíz-szolgáltatás alágazathoz tartozó létesítményeket. Közvetetten azonban akár a felszín és felszín alatti vizek minőségének ellenőrzése, összességében pedig a vízbázisok védelme alágazatokhoz tartozó rendszerek is érintettek lehetnek.

Víz	**ivóvíz-szolgáltatás**
	felszíni és felszín alatti vizek minőségének ellenőrzése
	szennyvízelvezetés és -tisztítás
	vízbázisok védelme
	árvízi védművek, gátak

4. ábra: A víz ágazat struktúrája a magyar kritikus infrastruktúra védelmi rendszerben[100]

Egy ilyen volumenű támadássorozat szoros és hatékony együttműködést tesz szükségessé a bűnüldöző szervektől. A kialakult helyzet – a kibertámadástól kezdődően, a reggeli robbantásokon át, a károk helyreállításáig – a Rendőrség (elsősorban az Országos Rendőr-főkapitányság és a Terrorelhárítási Központ), a BM OKF és fővárosi illetékességű területi szerve, a Magyar Honvédség, a Kormányzati Eseménykezelő Központ, illetve a polgári nemzetbiztonsági szolgálatok (elsősorban a Nemzetbiztonsági Szakszolgálat és az Alkotmányvédelmi Hivatal) gyors, hatékony, szervezett és eredményes helyzetkezelését igényli, ami akár nemzetközi szervezetekkel történő együttműködésre is kiterjedhet.

A kibertámadás bekövetkezése után, a Szolgáltató IT biztonsági csoportjának jelentési kötelezettsége van a BM Ügyelet felé a 33/2011. (XII. 2.) BM utasítás[101] alapján. A nyomozást hivatalból, a Budapesti Rendőr-főkapitányság rendeli el[102], bűncselekmény elkövetésének gyanújával, a BM Ügyeletre[103] érkezett bejelentés alapján. A bűncselekmény egyediségét tekintve, az ügyet az országos rendőrfőkapitány a Készenléti Rendőrség Nemzeti

[100] a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 3. melléklete

[101] a Belügyminisztérium és a belügyminiszter irányítása alá tartozó szervek ügyeleti szolgálatai által teljesítendő tájékoztatási kötelezettség rendjéről, valamint a Kormányügyelet működéséről szóló 33 /2011. (XII. 2.) BM utasítás 4. pontja

[102] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 1. mellékletének 12.5 pontja

[103] A 33/2011. (XII. 2.) BM utasítás alapján az Országos Vízügyi Főigazgatóság bejelentést tesz a BM Ügyeleti Osztályon a rendkívüli eseményről, ezekkel összefüggő szükséges és halaszthatatlan intézkedések megtételéről.

Nyomozó Iroda (a továbbiakban: KR NNI) Kiberbűnözés Elleni Főosztálya hatáskörébe utalhatja, illetve a KR NNI vezetője szóban előterjesztést tehet az ügy átvételére[104].

2.1. Rendőrségi intézkedések

Jelen helyzetben a főváros ivóvíz-ellátását biztosító rendszerben történt kettős kibertámadás után, a rendőrség a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) a terrorcselekményre vonatkozó rendelkezéseit – kiemelt biztonsági intézkedés, csapaterő, bírói engedélyhez kötött titkos információgyűjtés – alkalmazhatja.

A helyszínen a Rendőrség az Rtv. által meghatározott kiemelt biztonsági intézkedéseket vezeti be. Eszerint a terrorcselekmény által érintett területet lezárják, ellenőrző-átengedő pontokat jelölnek ki, az oda belépőket, ott tartózkodókat ellenőrizik, ruházatukat átvizsgálják, vagy az ott tartózkodókat távozásra kötelezhetik. A hatásterületet érintő közúti, illetve tömegközlekedést irányítás alá vonják, korlátozhatják, szüneteltethetik, az ott álló járműveket elszállíttathatják, ha a kialakult helyzet indokolttá teszi[105]. Azt Rtv. 54. § szerint terrorcselekmény megakadályozására, megszakítására a rendőr lőfegyvert használhat[106]. A rendőrök továbbá csapaterőben alkalmazhatók terrorcselekmény felszámolására. A csapatszolgálat alkalmazásának szabályairól, lehetőségeiről bővebben a 11/1998. (IV. 23.) ORFK utasítás[107] rendelkezik.

A nyomozást – a hatásköri és illetékességi szabályokat figyelembe véve, tekintettel arra, hogy a tárgyalt eset terrorcselekmény – a KR NNI végzi[108]. A Rendőrség terrorizmus elleni harccal kapcsolatos feladatait ellátó szervének (Terrorelhárítási Központ) nincs nyomozati jogköre, a terrorcselekmények felderítése, megszakítása, megakadályozása mellett a

[104] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 9. §

[105] Rtv. 37/A. §

[106] Rtv. 54. § (1) c)

[107] a Magyar Köztársaság Rendőrségének Csapatszolgálati Szabályzata kiadásáról szóló 11/1998. (IV. 23.) ORFK utasítás

[108] a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 13.1. és 13.2. pontjai

terrorcselekménnyel összefüggésben elkövetett más bűncselekmények megelőzéséért, felderítéséért, megszakításáért, illetve az elkövetők elfogásáért felelős[109].

2.2. A nyomozás előkészítése, információgyűjtés

A nyomozati tevékenységet alapvetően meghatározza az, hogy a felvázolt bűncselekmény szervezett módon történt elkövetése alkalmas arra, hogy a lakosságot megfélemlítse, illetve az ország társadalmi, gazdasági rendjét megzavarja, hiszen nemcsak a főváros ivóvíz-ellátását zavarták meg az elkövetők, hanem a robbantásokkal pánikot keltettek a főváros és közvetetten az egész ország lakosságában.

2.2.1. Kibertámadás

A KR NNI Kiberbűnözés Elleni Főosztály nyomozói a helyszínen megkezdik az információgyűjtést. A rendelkezésre álló információk szerint megállapítható, hogy kettős támadást történt.

→ Az első, egy számlaként álcázott pdf fájlkiterjesztésű dokumentumban egy zsarolóvírus jutott be az infrastruktúra belső levelező rendszerébe**.** Az üzenetet nem szűrte ki a biztonsági rendszer, mivel megbízható e-mail címről érkezett. A nyomozás során feltételezni kell, hogy a megbízható címhez történő hozzáférést a gyenge jelszavak feltörése és a hozzájuk tartozó gyanútlan felhasználói magatartás is eredményezhette.

→ A támadás másik eleme az emberi könnyelműséget kihasználó ajándékba küldött pendrive volt. A nyomozás megállapítja, hogy az elkövetők jól felépített legendával küldték ki az eszközt, amely szerint a címzett az adathordozót egy szakmai konferencián történő részvételét követő sorsoláson nyerte.

Összességében megállapítást nyer, hogy az ajándékként bejuttatott pendriveon egy olyan malware található, amely a Microsoft Windows operációs rendszert futtató gépeket fertőzi meg, és azokon terjed, de hatását végső soron a SCADA rendszeren fejti ki: nem csak kémkedik a célzott ipari rendszer után, hanem át is programozza azt.

[109] Rtv. 7/E. §

Bizonyítottá válik továbbá, hogy a megbízható e-mail címről kapott üzenet egy álszámlát tartalmazott, amelyet megnyitva egy ransomware került a rendszerbe. A ransomware e-mail segítségével terjed, amely mellékletként tartalmaz egy tömörített file-t (zip/rar/docm), valamint makrókat is magába foglal. Amennyiben ez megnyitásra kerül és a káros kód sikeresen lefut a rendszeren, egy távoli szerverről letöltődő ransomware kód titkosítja a dokumentumokat és más fájlokat a helyi és hálózati mappákban.[110] A zsarolóvírus titkosította a hálózati meghajtókon tárolt fájlokat és meggátolta a belső kommunikációt. A program felajánlotta, hogy 900 $ értékű Bitcoin megfizetése után szoftverhez tartozó dekódolást a felhasználó rendelkezésére bocsájtja, de ez nem teljes mértékben megbízható megoldás.

2.2.2. Fizikai támadások

A kibertámadás mellett a reggeli órákban fizikai támadások (bombarobbanások) érték a fővárost: a BKV Központ Zrt. autóbusz garázsainak közelében, valamint egy metróvonal megállójában, a reggeli csúcsforgalomban.

A fizikai támadásokról történő információszerzés érdekében azonnal intézkedni kell az érintett területek lezárására, majd vizsgálni kell a hatásterületeket. A Fővárosi Önkormányzat Rendészeti Igazgatóságtól be kell szerezni a térfigyelő kamerák felvételeit[111], majd elemezni kell azokat. A robbanás hatásfokát és károkozását vizsgálva meg kell állapítani, hogy milyen robbanószerkezetet használtak az elkövetők, illetve a bomba származási helyét, összetételét vizsgálva következtetni lehet a feltételezett elkövetőre is. Házilag készített bombák esetében az Iszlám Állam elnevezésű terrorszervezet által fenntartott Inspire és www.jihadology.net/ weboldalakat, illetve a Dabiq, vagy a Rumiyah című iszlám propaganda magazint, amelyek rendszeresen közreadnak ilyen típusú tartalmakat.

[110] http://neih.gov.hu/locky (letöltés ideje: 2017.10.03.)

[111] http://www.kozterulet-felugyelet.hu/sites/default/files/kepek/kozutkezeloi_kamerak_lista_.pdf (letöltés ideje: 2017.10.03.)

A rendőrség az érintett infrastruktúra központjában, illetőleg a városban keletkezett kaotikus állapotokra tekintettel, a Budapesti Rendőr-főkapitányság (a továbbiakban: BRFK) teljes állományát készenlétbe helyezi. Az Rtv. rendelkezései szerint a rendőrök csapaterőben alkalmazhatóak terrorcselekmény felszámolására[112], erre tekintettel intézkedéseket tehetnek a testi épséghez, a személyi szabadsághoz, a magánlakás, a magántitok és a levéltitok sérthetetlenségéhez, a személyes adatokhoz, valamint a tulajdonhoz fűződő jogok törvényben foglaltak szerinti korlátozására[113].

Terrorcselekmény elkövetése esetén a nemzetközi együttműködés keretében az Rtv. lehetőséget ad arra, hogy Magyarország területén az Európai Unió más tagállamának különleges intervenciós egysége intézkedjen. Ez az intervenciós egység egy olyan, más EU tagállam bűnüldöző egysége, amelynek speciális szakterülete a válságkezelés[114]. A rendfenntartás terrorveszélyhelyzet elrendelésekor a Magyar Honvédség (a továbbiakban: MH) egységeinek bevonásával történik. A MH egységeinek szakirányításáért és a készenlét szintjeinek fokozásáért a Honvéd Vezérkar főnöke felelős[115].

2.3. A kiberbűncselekmények nyomozási aspektusai

Európai Uniós szinten a tagállamok részéről is megfogalmazódott az igény egy megbízható, biztonságos kibertér létrehozására. Szükség volt egy közös terv megalkotására, amely a hálózati és információs rendszerek biztonsága mellett, garantálja a bűncselekmények megakadályozását, felderítését. Az Európai Unió kiberbiztonsági stratégiája[116] nemzeti szinten minimumkövetelményeket fogalmazott meg egy biztonságos kibertér létrehozása érdekében. E stratégia a követelmények között leírja a hálózati információs rendszerben illetékes nemzeti hatóságok kijelölésének szükségét, jól működő, hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT – Computer Emergency Response Team) létrehozását

[112] Rtv. 58. § (1) d)

[113] Rtv.58. § (2)

[114] Rtv.62/C. §

[115] a Magyar Honvédség készenléte fenntartásának és fokozásának rendjéről szóló 30/2012. (V. 8.) HM utasítás

[116] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér

és a hálózat- és információbiztonságra vonatkozó nemzeti stratégia és nemzeti együttműködési terv elfogadását.

Az EU kiberbiztonsági stratégiája és a hozzá kapcsolódó irányelv[117] jogharmonizációja keretében létrejött a Kormányzati Eseménykezelő Központ[118] (GovCERT-Hungary), amely Magyarország információ-megosztó és incidens-kezelő szerve lett. Fő feladata a preventív információ-megosztás és operatív incidens-kezelés[119]. Fontos megemlíteni, hogy a Kormányzati Eseménykezelő Központ nem hatóság, nem rendelkezik nyomozati jogkörrel sem, de a nemzetgazdaság és az állami működőképesség szempontjából kritikus fontosságú informatikai rendszerek védelmében, elkövetett támadás felderítésében együttműködik a nyomozó hatóságokkal. Az azonnali reagálás képességének biztosítása érdekében a GovCert 7/24 ügyeleti szolgálatot működtet.

2.3.1. Nyomozati tevékenység és eredményei

Az elkövetők első lépésként feltehetőleg a ransomware szoftvert vásárolták meg a Darkneten. A fizetést kizárólag Bitcoinnal hajthatták végre, így valamilyen platformon kriptovalutához kellett jutniuk, amelyhez elengedhetetlen létrehozni egy Bitcoin pénztárcát. A Bitcoint átválthatjuk bármilyen nemzetközi tőzsdén, vagy akár a Budapesten található Bitcoin ATM használatával is. A nyomozás során feltárásra kerül, hogy Budapesten egyetlen ilyen ATM található a 1065. Budapest, Anker köz 1-3. szám alatt. A nyomozás keretében tehát az Anker Klubban lévő ATM elmúlt 6 havi tranzakciós listáját is elemezni szükséges[120].

A különböző innovatív és csúcstechnológiai eljárások mellett a rendőrség a kiberbűncselekmények nyomozása során alkalmazza a klasszikus nyomozati eljárásokat is. A Büntetőeljárásról szóló törvény szerint a nyomozás megindulásától kezdődően a

[117] 460/2004/EK rendelet Az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról

[118] az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

[119] Nemzeti Kibervédelmi Intézet GovCert. http://www.cert-hungary.hu/node/1 (letöltés ideje: 2017.10.03.)

[120] Bitcoin ATM Forgalmazó (https://www.mrcoin.eu/hu/atm)

nyomozóhatóság tanú minőségben kihallgathatja az osztályon dolgozó személyeket[121], különös tekintettel azokat, akiknek sikerült feltörni az e-mail címét, illetve azt, aki megnyitotta a ransomware fájlt, továbbá azt is, aki az „ajándék" pendrive-t kapta. Ezzel a kihallgatás során a cselekményt megelőző idővonal állapítható meg.

A nyomozás keretében személyi szabadságot nem korlátozó kényszerintézkedések alkalmazhatóak, nevezetesen a lefoglalás[122] és a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés[123]. A bűncselekmény végrehajtására használt pendrive-ot, továbbá az érintett számítógépeket lefoglalhatják, továbbá az érintett infrastruktúra információs részlegét kötelezhetik a megőrzésre, ami a bűncselekmény felderítése és a bizonyítás érdekében az információs rendszerben tárolt adat birtokosának, feldolgozójának, illetőleg kezelőjének az információs rendszerben tárolt meghatározott adat feletti rendelkezési jogának ideiglenes korlátozását jelenti.

A kiberbűncselekmények felderítésében nagy szerepet játszik IP (Internet Protocol) Cím beazonosítása. Ezt tulajdonképpen tekinthetjük a virtuális világban lévő ujjnyomnak is. Az internetszolgáltató folyamatosan tárolja a beazonosításhoz szükséges adatokat, amelyeket a nyomozó hatóság a felderítés sikere érdekében megkérhet a szolgáltatótól[124]. Az IP cím alapján történő nyomozást leginkább orientáló nyomként[125] alkalmazzák, mivel a hackercsoportok nyíltforrású WiFi használatával is elkövethetik bűncselekményüket.

Feltételezhető, hogy bizonyos körökben, az elkövetők egy ilyen sikeres kiber- és fizikai támadást nem fognak eltitkolni. A „bűnözői alvilágban" feltehetően nagy visszhangot kavar egy ilyen nagy volumenű támadás végrehajtása, ami hírnevet szerezhet az elkövetőknek. Az

[121] 1998. évi XIX. tv. a Büntetőeljárásról 79. §

[122] uo. 151. §

[123] uo. 158/A. §

[124] http://arsboni.hu/a-kiberbuncselekmenyek-nyomozasanak-uj-eszkozei/ (letöltés ideje: 2017.10.03.)

[125] A nyomozás során a hatóságok tudomására jutott IP címen keresztül nem juthatunk el közvetlenül a bűncselekmény elkövetőjéhez, mivel az adott eszközhöz több személy is hozzá férhet, illetve más helyszínen nyílt forrású internethez is csatlakozhatnak. Közvetett információként szolgálhat azonban, hogy ki, mikor és hol használhatja az adott informatikai eszközt.

ilyen forrásból származó információk megszerzésére a 2012. évi C. törvény a Büntető Törvénykönyvről, illetve a büntetőeljárásról szóló 1998. évi XIX. törvény ad felhatalmazást, az egyéb adatszerző tevékenységet, a bírói engedélyhez nem kötött, illetve bírói engedélyhez kötött titkos információgyűjtés intézménye útján. Ilyen esetekben a rendőrség a felderítés sikere érdekében fedett nyomozót alkalmazhat. A nyomozó hatóság a büntetőeljárás megindítása után bizonyítási eszközök felkutatására adatszerzést végezhet. Ennek során az ügyész engedélyével a nyomozó hatóság olyan tagját is igénybe veheti, aki e minőségét leplezi, továbbá más, bírói engedélyhez nem kötött titkos információgyűjtést is végezhet[126].

A rendőrség a bűncselekmények elkövetésének megakadályozására, felderítésére, az elkövető kilétének megállapítására, továbbá bűnmegelőzési, bűnfelderítési célok érdekében titokban információt gyűjthet[127]. A feladat teljesítése érdekében a rendőrség informátort, bizalmi személyt vagy titkosan együttműködő más személyt vehet igénybe, a nyomozás során az eljárás célját leplezheti, továbbá a rendőri jelleg leplezésére fedőokiratot állíthat ki. A rendőrség bírói engedélyhez kötött titkos információgyűjtést, titkos adatszerzést folytathat bűnüldözési célból, illetve súlyos bűncselekmények felderítésének érdekében. A tevékenység során a magánlakást titokban átkutathatja, technikai eszközök segítségével megfigyelheti, postai küldeményt ellenőrizhet, elektronikus hírközlés útján továbbított kommunikáció tartalmát megismerheti, rögzítheti, továbbá számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerheti, rögzítheti és felhasználhatja[128]. A titkos adatszerzést a bíró 90 napra engedélyezi, ez egy alkalommal, indítványra 90 nappal meghosszabbítható. Bár nyomozati jogkörrel nem rendelkezik, az információgyűjtésben részt vesz, továbbá speciális felderítési feladatokat lát el az Alkotmányvédelmi Hivatal. A terrorcselekmény felderítése során az államellenes vonalat keresi a tényállásban. Fontos, hogy az Alkotmányvédelmi Hivatal főigazgatója konkrét információ esetében 72 óráig engedélyezheti a titkos információgyűjtést is[129].

[126] 1998. évi XIX. tv. a büntetőeljárásról 178. §

[127] Rtv. 63. §

[128] Rtv. 69. §

[129] a Nemzetbiztonsági Szolgálatokról szóló 1995. évi CXXV. tv. 59. §

2.4. Robbantásokkal kapcsolatos nyomozati irányok

A robbantásokkal kapcsolatos nyomozás során a legfontosabb tényezők a tanúkutatás, a helyszínen rögzített anyagmaradványok, a kamerafelvételek beszerzése, a bombát elhelyező személyek felkutatása, illetve a bomba szakértői vizsgálata. Emellett a rendőrség bűncselekmények felderítése érdekében a lakosság segítségét kérheti. A robbanás helyszínének közelében lévő személyek jelentkezésére felhívást tehet, illetve a robbantó személyazonosságának felderítése érdekében nyilvánosan díjat tűzhet ki[130]. A nyomozás során azonban szelektálni kell a kapott információkat. Sok hamis/téves bejelentés és álhír is érkezhet a rendőrséghez, egyrészt a nyomravezetői díj miatt, másrészt az elkövetők védelme miatt próbálhatják meg álhírrel elterelni a nyomozást.

A hermetikusan lezárt területeken a rendőrség helyszínelői azonnal megkezdik a nyomrögzítést. A nyomrögzítés során feltételezhető, hogy DNS minta alapján azonosítható az a személy, aki a bombákat a helyszínekre helyezte.

A térfigyelő kamerák felvételeit a nyomozó hatóság az információgyűjtés során beszerzi és elemzi. A kerületi önkormányzati térfigyelő kamerákon túl, az egyéb adatszerző tevékenység során beszerezheti és megvizsgálhatja a környéken lévő hivatalok, intézmények, egyéb létesítmények tulajdonában álló biztonsági kamera felvételeit is[131]. A kamerák felvételeit használva megállapítható a bombát elhelyező személy személyazonossága, végigkövethető a haladási és távozási útvonala.

A szakértői vizsgálat megállapítja, hogy egy háztartásban elkészíthető, saját kezűleg összeállított szerkezetről van szó, amely Kínából, interneten rendelhető működési elektronikával és áramkörrel rendelkezik. A nyomozás fő irányvonalát ezek az információk adják meg: a rendelés során az elkövetőknek meg kell adniuk e-mail címüket, postai címüket, esetleg a nyomozás során a fizetési tranzakcióról is található információ.

[130] Rtv. 26-27. §

[131] Rtv. 26. §

2.5. Nemzetközi aspektus

Az internet egy olyan globális, határokat nem ismerő platform, amely nem tartozik állami felügyelet, illetve szabályozás alá. Ezért a kiberbűncselekmények nyomozását tekintve az elkövetők jelentős előnyben vannak az állami hatóságokkal szemben. A kibertér egy olyan, egész bolygót felölelő platform, amelyben nem számítanak az államhatárok, illetve a különböző állami jogi szabályozások. A felhasználók nincsenek helyhez kötve, bármikor, bárhonnan képesek elérni az adott weboldalt, illetve szervezett és fedett módon tudnak egymással kommunikálni.

2004-ben az Európai Unió a tagországok felhasználóinak védelme érdekében – a 460/2004/EK rendelet alapján – létrehozta az Európai Unió Hálózat- és Információbiztonsági Ügynökséget (ENISA – European Union Agency for Network and Information Security). Az ENISA a hálózat- és információbiztonság európai szakértői központja, amely segít az EU-nak és tagországainak abban, hogy jobban fel legyenek készülve az információbiztonsági kihívások felderítésére és kezelésére, illetve megelőzésére, továbbá kapcsolódó koordinációs feladatokat is ellát[132].

A koordinációs együttműködés az Európai Unió intézményeit is érinti. 2012-ben állandó, hálózatbiztonsági vészhelyzeteket elhárító csoportot ún. „CERT-EU”-t hoztak létre, amely az uniós intézmények, ügynökségek és szervek informatikai rendszereinek biztonságáért felel[133]. A bűnügyi szervek együttműködését európai szinten az Europol és az Eurojust koordinálja, előbbi a nyomozó hatóság, utóbbi az ügyészség szintjén. 2013-ban további Európai Uniós együttműködési megállapodások születtek, amelyek tovább segítik a nemzetközi bűnügyi szervek együttműködését. Az Európai Bizottság az Europolon belül 2013. január 1-jével létrehozta a számítástechnikai bűnözés elleni európai központot[134] (European Cybercrime Centre), amelynek feladata az Európai Unió tagállamain belül elkövetett kiberbűncselekmények gyors és hatékony felderítése.

---

[132] az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendelet

[133] Cert-EU https://cert.europa.eu/cert/plainedition/en/cert_about.html, (letöltés ideje: 2017.10.03.)

[134] Európai Unió Sajtóközlemény – Január 11-én megnyílik a számítástechnikai bűnözés elleni európai központ http://europa.eu/rapid/press-release_IP-13-13_hu.htm (letöltés ideje: 2017.10.03.)

Az Európai Unió kiberbiztonsági stratégiájában megfogalmazottak szerint, mind nemzetközi szinten, mind állami és privát szektorban tenni kell a kibertér biztonságáért, ezért az Európai Parlament és a Tanács 2016-ban kiadta a 2016/1148. irányelvet[135]. Ez útmutatást ad a tagállamok számára a minimumkövetelmények teljesítésére, mind az információs rendszerek biztonsági kihívásainak kezelésére, mind információcserére, együttműködésre vonatkozóan. E minimumkövetelmények nem csak a nemzetközi együttműködés kötelességét rögzítik, de minden tagállamnak kötelessége elfogadni egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát. Ez az a dokumentum, amely meghatározza a stratégiai célokat, valamint a biztonság megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket az információbiztonság tekintetében[136]. Továbbá minden tagállamnak kötelessége létrehozni egy, vagy több hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot[137], illetve számítógép-biztonsági eseményekre reagáló csoportot (CSIRT), amelynek főfeladata a biztonsági események meghatározott eljárással összhangban történő hatékony kezelése[138].

Az állami hatóságoknak szükséges volt létrehozni egy új nyilvántartási rendszert, amelyben a különböző büntetőítéletekről szóló információk cseréje egységes és gyors formában történik, továbbá útmutatást ad a jogalkalmazásban.

E szükségleteket tekintve bűnügyi nyilvántartást hoztak létre a hatóságok részére, nevezetesen az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS). A nyilvántartás, a büntetőjogi felelősséget megállapító ítéletekre vonatkozó gyors adatcserét teszi lehetővé az államok között. A 2016-os fejlesztéseknek hála, az ECRIS nem csupán az Unión belüli állampolgárokra, hanem harmadik ország állampolgárai vonatkozóan is tárol adatot.[139].

---

[135] Az Európai Parlament és a Tanács 2016/1148. irányelve, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[136] uo. 7. cikk

[137] uo. 8. cikk

[138] uo. 9. cikk

[139] ECRIS – European Criminal Records Information System http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm
(letöltés ideje: 2017.10.03.)

2.6. Ransomware – Kell-e fizetni a zsarolóvírusnak?

Miután a helyi és hálózati meghajtókat megfertőzte a ransomware, felmerül a kérdés, érdemes-e kifizetni a 900 $ értékű dekódolást és bízni az egyszerű megoldásban, vagy célszerű-e más megoldásokat keresni.

A Symantech, internetbiztonsággal foglalkozó cég javaslatai alapján a fizetés abszolút nem célravezető. A Bitcoin elutalása ugyanis nem jelent biztosítékot arra, hogy a ransomware dekódolja saját magát. Ez eredhet szándékos beállításból, vagy programozási hibából is. Továbbá a fizetéssel az áldozatok jelzik a kiberbűnözők számára, hogy egy kiváló módszert találtak a pénzszerzésre, bátorítóan hat további támadások indítására, illetve tőkét biztosíthatnak számukra a további fejlesztésekre[140].

3. A magánszektor és önkormányzati szereplők helyzetkezelésbe történő bevonásának lehetőségei

A kialakult helyzetet elsősorban az erre rendelt, illetve a különleges jogrend által felhatalmazott hivatásos állományú szervek számolják fel, a helyzet összetettsége miatt ez valószínűleg meghaladja az állomány kapacitását, így érdemes mérlegelni azt, hogy más, önkormányzati- és magánszereplők bevonásával hogyan lehetne tehermentesíteni őket, illetve a lakosság ellátását több ponton-több módon biztosítani.

Jelen alfejezetben elsősorban ajánlásokat szeretnénk megfogalmazni, amelyek a hatékony elhárítást, a további problémák eszkalálódását ellensúlyozhatják.

3.1. A Polgárőrség és a Fővárosi Önkormányzati Rendészet bevonása

Tekintettel arra, hogy a Rendőrség állományának a helyszíni biztosítás, a felderítés és a különleges jogrendben foglalt feladatainak teljesítése miatt már nem jut elég kapacitása arra, hogy a lakosság körében pontos felmérést készítsen arra vonatkozóan, hogy mindenki hozzájut-e a szükséges ivóvízmennyiséghez, célszerű egyéb szerveket bevonni a helyzet

[140]Ransomware removal and protection with Symantec Endpoint Protection https://support.symantec.com/en_US/article.HOWTO124710.html (letöltés ideje 2017.10.03.)

kezelésébe. Erre a Polgárőrség és a Fővárosi Önkormányzati Rendészet tökéletesen alkalmas lehet, hiszen kerületi szintű járőrözések során fel tudják azt mérni, hol tartózkodnak olyan idős, beteg személyek vagy kiskorú gyermekek, továbbá hajléktalanok, akik akadályoztatva vannak abban, hogy az ivóvizet biztosító pontokra eljussanak. Az önkormányzati rendészek gépjárműveikkel és alapos helyismeretükkel segíthetik az ivóvíz hatékonyabb szétosztását, illetve a mentőszolgálatot tájékoztathatják olyan súlyos betegek tartózkodási helyéről is, akik valamilyen oknál fogva nem tudtak egészségügyi intézményekbe eljutni.

A Polgárőrség és a Fővárosi Önkormányzati Rendészet fent említett feladata közé érdemes beépíteni az állatmenhelyek látogatását is, hiszen nem csak az emberek, az állatok is tömegesen betegedhetnek meg, és a jelentős számú elhullásuk ismételten egy járványügyi kockázat lehet, ezért ezen szervezetek számára is biztosítani kell a tiszta ivóvizet, illetve célszerű fokozottabban figyelni, szükség szerint begyűjteni a kóbor állatokat, ami gátat szabhat a fertőzések további terjedésének.

3.2. A Szolgáltató informatikai rendszerének izolálása, a károk helyreállítása

A támadást észlelve a Szolgáltató – bejelentési kötelezettségeinek eleget téve[141] – azonnal megkezdi a károk felmérését és a rendszer izolációját a GovCERT szakmai koordinációjával. A Szolgáltató megfertőzött rendszerének teljes hálózati leválasztása szükséges, ami után párhuzamosan meg kell kezdeni az azonnali biztonsági mentésből való visszaállítást és rendszerelemzést. Ez a lépés feltárja, milyen mélységben érintette a kibertámadás a rendszereket, így csökkentve a lefedetlen időszakot. A biztonsági mentés helyreállítása előtt mindenféleképpen meg kell vizsgálni, hogy fertőzött állomány került-e eltárolásra, ezáltal elkerülhető a visszafertőzés veszélye.

Javasoljuk egy független internetkapcsolat biztosítását (akár önálló modemmel rendelkező mobil internet) is, amelyhez a felhasználói hozzáférést korlátozni kell, tehát csak meghatározott vezetői szinten túl lehet azt kapcsolattartásra használni. A dolgozók internethasználatát az izoláció során korlátozni kell, amely elejét veheti a vírusok további terjesztésének, illetve a belső, bizalmas információk kiszivárogtatásának egyaránt.

[141] A GovCert 7/24 órás ügyelete, az Országos Vízügyi Főigazgatóság, illetve a BM Ügyelet felé.

A Szolgáltató azon rendszereinél, ahol még nincs a támadásnak nyoma, szintén célszerű egy rendszerelemzést végrehajtani megelőzésképpen, biztonsági intézkedésként. Ha nem található vírus, a biztonsági mentéseket haladéktalanul meg kell kezdeni, valamint azok külső, hálózatról leválasztott meghajtókon való tárolásával, duplikálásával az adatokat biztosítani. Erre a célra bár különösen költséges, de a legalkalmasabb a szalagos mentőegység lehet, amelyeket fokozott figyelemmel és körültekintéssel kell tárolni, valamint kezelni.

3.3. A médiaszolgáltatókra háruló feladat

Azon túl, hogy terrorveszélyhelyzet lehetővé teszi azt, hogy a Kormány ellenőrizheti az internet-, levél-, és postaforgalmat, valamint az állami médiát kötelezheti a kormányzati állásfoglalások kiadására, a pánikhelyzet kialakulásában nagy szerepe van a bulvársajtó és a médiaszolgáltatók egyéni felelősségének is.

A támadások vezető hírként fognak szerepelni és az idő előrehaladtával egyre több és több adat fog napvilágot látni az eseményekről, mert a lakosság folyamatos információs igényét a gyors cikkmegjelentetésekkel szeretnék kielégíteni. Ez a támadás harmadik lépésének, az álhírek terjesztésének és a dezinformációs műveleteknek kedvez.

Az állami médián keresztül közölt állásfoglalásokon, a sajtótájékoztatók tartásán túl érdemes lenne fontolóra venni azt, hogy a közösségi oldalakat is fel lehet használni, mint a hivatalos, megbízható hírek minél nagyobb közönséghez történő eljuttatási fórumát, hiszen mind a BM OKF, mind az ORFK rendelkezik Facebook oldallal, amelyen a hírek – felhasználói megosztások által – gyorsan, de mégis hiteles formában terjedhetnek.

Összegzés

A fenti helyzetet, valamint megoldási dimenziókat látva megállapítást nyert az, hogy bár Magyarország terrorfenyegetettsége alacsonyabb, mint más, nyugat-európai országoké[142], egy ilyen típusú támadás kivitelezésének valószínűsége – részint a viszonylag „könnyű" kivitelezésnek, részint pedig az informatikai támadási lehetőségek sebezhetőségekből eredő térnyerésének köszönhetően – nem elhanyagolható.

A XXI. század információs társadalmában látnunk kell a mindennapos életvitelünket veszélyeztető tényezőket. Számolnunk kell az emberi tényezővel mind az elkövetők, mind az elszenvedők vonatkozásában. A kibertérben rejlő lehetőségek ártó szándékú felhasználása a modern kor egyik legnagyobb kihívásává fogja kinőni magát. Ennek ellensúlyozása érdekében – ahogy a felvázolt eseménysorozat is mutatja – nem csak az állami szféra, a beavatkozó, elhárító és nyomozó hatóságok felkészültségét kell a lehető legmagasabb szintre fejleszteni, hanem a hétköznapi emberek gondolkodásmódját is. A tudatosítás, az „informatikai önvédelmi képesség" kialakítása és fokozása kiemelt célként kell, hogy szerepeljen az olyan stratégiai szintű dokumentumokban például, mint Magyarország Kiberbiztonsági Stratégiája. Mind állami, mind magánszektor vonatkozásában erősíteni – ha szükséges, akkor kötelezni – kell az informatikai tudatosító kampányok során az eszközök napi használatából fakadó veszélyekre vonatkozó ismereteket. Az emberi hiszékenység, a tájékozatlanság csökkentésére irányuló kezdeményezések útján el kell érni, hogy a következő években csökkenjen a szcenárióban bemutatott helyzetek kivitelezhetősége.

Természetesen a szerzők is tisztában vannak azzal, hogy nem egy-egy tudatosító előadás hozza meg az eredményt, éppen ezért olyan egyszerű, közérthető, kis anyagi vonzattal járó informatika biztonsági oktatási koncepciót ajánlunk mind az állami, mind a magánszektor számára, amelyek egyszerűen beépíthetők minden munkatárs napi rutinjába és amelyeket a magánéletükben is sikerrel és könnyedén alkalmazhatnak. Ezt azért tartjuk fontosnak, mert – ahogyan a tanulmányunkból is kiderült – az ártó szándékú fél sem munkaidőben fogja támadni a célpontot, úgy, mint az adott szervezethez vagy céghez tartozó kollégát, hanem az

[142] A brit külügy 2017 májusában készült fenyegetettség felmérése alapján. http://www.telegraph.co.uk/travel/maps-and-graphics/Mapped-Terror-threat-around-the-world/ (letöltés ideje: 2017.10.10.)

egyénhez, a magánemberhez próbál minél közelebb kerülni, hogy aztán azt kiismerve fel tudja használni céljai eléréséhez.

Célszerűnek tartjuk azt is, hogy a munkavállalókat a kötelező dolgozói oktatásokon túl véletlenszerűen ellenőrizzék akár az IT biztonsági osztályhoz tartozó kollégák, akár a felettesek, annak tekintetében, hogy a megtévesztésre mennyire hajlamosak, illetve mennyire fogékonyak akár a jelen tanulmányban ismertetett social engineering technikák tekintetében.

A levezetett feltételezés alapján áttekintettük a beavatkozó és nyomozati szervek reagáló-képességét biztosító jogszabályi környezetet is. Ez alapján megállapítottuk, hogy a különleges jogrend általi felhatalmazások érvényesítésével és a rendkívüli intézkedések bevezetésével a lakosság alapellátásának biztosítása megoldottnak tűnik, ugyanakkor számolni kell azzal, hogy egy ilyen komplex támadás meghaladhatja az erre rendelt erők képességeit. Különösen igaz lehet ez abban az esetben, amikor az általános rendőrségi feladatok ellátására létrehozott szerv eleve rendkívüli leterheltségnek van kitéve a tömeges bevándorlás okozta válsághelyzetből fakadó, folyamatosan végrehajtandó feladatok által. Mindez jelentősen befolyásolhatja az ilyen mértékű támadás kezelésével járó, elsősorban a közrend fenntartása érdekében előirányzott erőátcsoportosítási lehetőségeket, tekintettel arra, hogy a közbiztonság garantálása – a határvédelmi és a terrorcselekménnyel kapcsolatos feladatok mellett is – alaprendeltetésből fakadó kötelezettség az egész ország területére vonatkozóan.

A jogszabályi környezet elemzése során felmerült, hogy az ivóvíz-ellátás szabotálása miatt kialakuló helyzet következményeinek kezelésére az Alaptörvény veszélyhelyzeti tényállásának kihirdetése lehet a válasz, annak érdekében, hogy a gyors és hatékony döntéshozatal, illetve az azonnali intézkedések bevezetése megvalósítható legyen. Ugyanakkor a „klasszikus” terrorcselekmények (robbantások) elkövetése automatikusan feltételezi az Alaptörvény terrorveszélyhelyzeti tényállásának kihirdetését. Ahogy az a kialakult krízis kezelésének dimenziói c. fejezetben említésre került, fennáll a lehetősége, hogy a helyzetet két különleges jogrendi állapotra jellemző közigazgatási eszközökkel kezelik. Érdemes lenne emiatt megvizsgálni az ehhez hasonló, sajátos körülmények között szerveződő döntés-előkészítő és döntéshozó mechanizmust, valamint a rendvédelmi szervek hatáskör-telepítésének és az így kialakulható kollíziók feloldásának jogi és gyakorlati megoldásait, a párhuzamok és duplikációk elkerülése érdekében. Szintén a jogszabályi környezet vizsgálata közben állapítottuk meg, hogy a jelenlegi szabályozás szerint a KKB

ülésein résztvevők közvetetten rendelkeznek a terrorelhárítással kapcsolatos információkkal (belügyminiszter, országos rendőrfőkapitány, polgári nemzetbiztonsági szolgálatok főigazgatói). A pontos és szükség esetén részletekbe menő információk rendelkezésre állása érdekében megfontolandónak tartjuk terrorveszélyhelyzet kihirdetett időszakában legalább a TEK főigazgatójának jelenlétét jogszabályi úton is biztosítani.

Tanulmányunk forgatókönyvének döntő tényezőjeként azonosítottuk a pánik kialakulását, amelynek elsődleges táptalaját az álhírek, valamint a nem megbízható, ellenőrizetlen forrásból származó információk adják. A folyamatos, hivatalos forrásokból származó lakosságtájékoztatás megakadályozhatja ezt, valamint az ebből fakadó tömeges atrocitásokat, amely összességében az elkövetők végső célkitűzéseként aposztrofálható: a belső rend, a közbizalomba vetett hit megingatása. Meglátásunk szerint ennek felelősségét a médiaszolgáltatóknak is kell magukra vállalni és – bár a minél többet olvasott cikkek és eladott lapszámok jelentik bevételük fő forrását, amelyet a figyelemfelkeltő cikkekkel lehet elérni – mérlegelniük azt, hogy ebben a rendkívüli helyzetben a tényszerű, lényegre törő, a lakosság számára hiteles tények közlését helyezzék előtérbe.

Összességében megállapítottuk, hogy a hatályos jogszabályi környezet és a hatóságok rendelkezésére álló képességek alapján a feltételezett támadás következményeinek kezelése – feszített tempóban, a nemzetgazdaság tartalékainak igénybe vétele mellett, a magánszektor bizonyos mértékű bevonásával – eredményesen kezelhető. Bár az önkormányzati rendészeti szervek, valamint a rendőrség közti együttműködésre az elmúlt évek során egyre több példát látunk, véleményünk során a jövőben célszerű lenne hasonló gyakorlatokba belevonni őket is.

Irodalomjegyzék

Nemzetközi szabályozók

1. Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságának és a Régiók Bizottságának – Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001 (letöltés ideje: 2017.10.03.)
2. 460/2004/EK rendelet az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML (letöltés ideje: 2017.10.03.)
3. Az Európai Parlament és a Tanács 2016/1148. Irányelve, a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm (letöltés ideje: 2017.10.03.)

Jogszabályok

4. Magyarország Alaptörvénye
5. 1994. évi XXXIV. törvény a Rendőrségről
6. 1995. évi CXXV. törvény a Nemzetbiztonsági Szolgálatokról
7. 1998. évi XIX. törvény a büntetőeljárásról
8. 1999. évi LIV. törvény az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről
9. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

10. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
11. 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról
12. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
13. 33/2011. (XII. 2.) BM utasítás a Belügyminisztérium és a belügyminiszter irányítása alá tartozó szervek ügyeleti szolgálatai által teljesítendő tájékoztatási kötelezettség rendjéről, valamint a Kormányügyelet működéséről
14. 30/2012. (V. 8.) HM utasítás a Magyar Honvédség készenléte fenntartásának és fokozásának rendjéről
15. A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 1/2016. (IV.29.) határozata a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság ügyrendjének és a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság Nemzeti Veszélyhelyzet-kezelési Központ ügyrendjének elfogadásáról.

Tanulmányok

16. BAÁN Mihály, BORS István, CSIFFÁRY Tamás, HÁRI László, KOCSIS Lajos, szerk. SZENTES László: Magyarország védelmi igazgatása a közigazgatás új környezetében. Zrínyi Kiadó, Budapest, 2014.
17. Cisco 2017 Midyear Cybersecurity Report. Published July 2017. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2 (letöltés ideje: 2017.10.07.)
18. DARUKA Norbert: A bűnös célú/terror jellegű robbantások és az ellenük való védekezés lehetőségei, különös tekintettel a tűzszerész feladatok ellátására. Doktori (PhD) értekezés, http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2014/daruka_norbert.pdf (letöltés ideje: 2017.08.26.)

19. Keep Security The Most Common Passwords of 2016.
https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf
(letöltés ideje: 2017.10.05.)

20. KOVÁCS László–KRASZNAY Csaba: A digital Mohács - IN: Nemzet és Biztonság: Biztonságpolitikai szemle (Spec. Issue Winter) pp. 49-59
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf
(letöltés ideje: 2017.09.30.)

21. KOVÁCS László–SIPOS Marianna: A Stuxnet és ami mögötte van – Tények és a cyberháború hajnala. IN: Hadmérnök V. Évfolyam 4. szám pp. 163-172. (2010.)
http://hadmernok.hu/2010_4_kovacs_sipos.pdf
(letöltés ideje: 2017.10.07.)

22. William Powel: The Anarchist Cookbook, Barricade Books Inc. (1971.)
https://uniteyouthdublin.files.wordpress.com/2015/01/anarchist-cookbook-william-powell.pdf
(letöltés ideje: 2017.08.22)

Internetes források

23. http://vizmuvek.hu/files/public/Fovarosi_vizmuvek/tarsasagi_informaciok/FVM_Eves_Jel_HUN.pdf
(letöltés ideje: 2017.08.12.)

24. http://okoenergia.hu/vizfogyasztasi-statisztika/
(letöltés ideje: 2017.10.05.)

25. http://www.orientpress.hu/cikk/2017-08-02_a-fovaros-kuzd-a-hoseggel
(letöltés ideje: 2017.10.05)

26. https://www.budapestinfo.hu/hu/szallashely-statisztika---minden-mutato-emelkedett-2017-elso-feleveben-budapesten-is
(letöltés ideje: 2017.08.26)

27. http://vizmuvek.hu/jubileum/
(letöltés ideje: 2017.08.22.)
28. https://sg.hu/cikkek/it-tech/96470/lecsereli-informatikai-halozatat-a-fovarosi-vizmuvek
(letöltés ideje: 2017.08.22.)
29. http://www.information-age.com/risks-facing-industrial-control-systems-reach-all-time-high-123467315/
(letöltés ideje: 2017.10.07.)
30. http://invenioit.com/security/ransomware-statistics-2016/
(letöltés ideje: 2017.10.09.)
31. http://budapest.hu/Documents/varosfejlesztesi_koncepcio_2011dec/11_Kozmuvek_jav.pdf
(letöltés ideje: 2017.10.08.)
32. Epidemiológiai Információs Hetilap (2006. 23. szám pp. 291-296.) http://epa.oszk.hu/00300/00398/00208/pdf/00208.pdf
(letöltés ideje: 2017.10.07.)
33. http://metros.hu/vonal/jellemzok_m2.html
(letöltés ideje: 2017.10.01.)
34. http://hvg.hu/itthon/20160926_Hidegverrel_lepett_at_aldozatain_a_robbanto (letöltés ideje: 2017.10.01.)
35. http://metros.hu/vonal/jellemzok_m3.html
(letöltés ideje: 2017.10.01.)
36. https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf
(letöltés ideje: 2017.08.27)
37. http://hvg.hu/itthon/20161205_baleset_miatt_nem_jar_a_2es_metro
(letöltés ideje: 2017.08.12.)
38. http://www.thehindu.com/news/national/what-is-not-in-my-name-all-about/article19194499.ece
(letöltés ideje: 2017.10.07.)
39. http://neih.gov.hu/locky
(letöltés ideje: 2017. 10. 03.)

40. http://www.kozterulet-felugyelet.hu/sites/default/files/kepek/kozutkezeloi_kamerak_lista_.pdf
(letöltés ideje: 2017.10.04.)
41. http://jihadology.net/category/inspire-magazine/
(letöltés ideje: 2017.10.08.)
42. http://jihadology.net/
(letöltés ideje: 2017.10.08.)
43. https://clarionproject.org/docs/islamic-state-dabiq-magazine-issue-7-from-hypocrisy-to-apostasy.pdf
(letöltés ideje: 2017.10.08.)
44. https://clarionproject.org/factsheets-files/Rumiyah-ISIS-Magazine-1st-issue.pdf (letöltés ideje: 2017.10.08.)
45. https://www.mrcoin.eu/hu/atm
(letöltés ideje: 2017.10.03.)
46. https://cert.europa.eu/cert/plainedition/en/cert_about.html
(letöltés ideje: 2017.10.03)
47. http://europa.eu/rapid/press-release_IP-13-13_hu.htm
(letöltés ideje: 2017.10.03.)
48. https://support.symantec.com/en_US/article.HOWTO124710.html
(letöltés ideje: 2017.10.03.)
49. http://www.telegraph.co.uk/travel/maps-and-graphics/Mapped-Terror-threat-around-the-world/
(letöltés ideje: 2017.10.10.)

TÓTH TAMÁS

HUMÁN KOCKÁZATOK A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁBAN

Bevezetés

A releváns információk ismerete elengedhetetlen a hatékony feladat-végrehajtáshoz, kellő minőségű és mennyiségű specifikus adat birtoklása nélkül nem lehet megfelelő döntéseket hozni. Mérhetetlen számú információ egyidejű, folyamatos áramlására van ahhoz szükség, hogy a „need to know" és a „need to share" elv érvényesülhessen a közszolgálati és magánszféra területén egyaránt. Ehhez kulcsfontosságú a kommunikációs képességek, csatornák komplex rendszerének, azaz az infokommunikációs infrastruktúrának a fenntartása és védelme. Az infokommunikációs rendszeren[143] belül pedig különös figyelmet kell fordítani a szenzitív, különösen fontos adatok áramoltatásának alrendszereire, azaz a kritikus információs infrastruktúra biztosítására (NATO Polgári Vészhelyzeti Tervezés, NATO Civil Emergency Planning – CEP, 2006).

Információs társadalomban élünk, ahol az adatok lehető leggyorsabb továbbításának fontossága kulcskérdés, legyen az honvédelmi, rendvédelmi, nemzetbiztonsági, gazdasági vagy egyéb jellegű adat. Egy megfelelő pillanatban érkező információ emberéleteket menthet, gazdasági érdekeket befolyásolhat, szavatolhatja a nemzetbiztonságot. A végtelenségig lehetne sorolni a pontos és időben érkező információ rendkívüli jelentőségét. Ugyanakkor ez fordítva is igaz, ha sikerül blokkolni az ellenérdekelt fél tér- vagy időbeli, digitális vagy analóg, verbális vagy nonverbális kommunikációs csatornáit, a jelentkező adathiány okán

[143] Infokommunikációs rendszer alatt az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközök, eljárások, valamint az üzemeltető és a felhasználó személyek együttesét értem. *(.(Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, 16. o. Budapest, 2007)*

lépéselőnybe kerülhetünk, mi több, akár vissza nem fordítható folyamatokat generálhatunk a támadott fél részére.

Manapság az információk legtöbb esetben elektronikus jel, rádiófrekvenciás hullámok formájában, technikai úton terjednek, mivel ezek gyorsaságával a papír alapú kézbesítés nem veheti fel a versenyt. Ezen csatornák biztosítása a fentiek alapján kézenfekvő és indokolt, magában rejti az elvárást a védelem és biztonság iránt. (*Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.)* De a leglényegesebb dolgot, miszerint ezeket humánerő, azaz személyek tervezik, alkalmazzák, üzemeltetik és tartják karban, nagyon nagy felelőtlenség lenne figyelmen kívül hagyni. Lehet egy digitális infokommunikációs csatorna akármennyire védett informatikai, fizikai szempontból, ha az azt alkalmazó személyek feladataik ellátása során nem elég körültekintőek, nem rendelkeznek a megfelelő biztonságtudatos magatartással, illetve alkalmasak ellenérdekelt befolyás hatására, ezen hálózatok szabotálására.
A lehető legjobban üzemelő, komplex biztonsággal rendelkező információs infrastruktúra hatékony működésének szavatolásában elengedhetetlen a személyi állomány biztonságának kialakítása a fizikai, elektronikus és adminisztratív védelem területén. Az elektronikus információs rendszerek teljeskörű védelemének biztosítása jogszabályi kötelemként jelenik meg a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 5§-ának b*)* pontjában.

1. Tudományos hipotézisek

- Az kritikus információs infrastruktúra fogalma nem egységes, így nélkülözhetetlen annak megalkotása.

- A humán kockázatok jelentősége egyre nő az információbiztonság területén, ezért átfogó vizsgálata, csoportosítása elengedhetetlen a megelőzés érdekében.

- A helyi humán kockázatok eszkalációjában rejlő veszélyek kialakulása globális problémákat jelenthet, melyek megelőzése nélkülözhetetlen a nemzeti és nemzetközi komplex biztonság megteremtése érdekében.

2. Pályázati célkitűzések

Kutatásom során az alábbi célokat tűztem ki:

- Definiálni a kritikus információs infrastruktúra fogalmát, tartalmát és alkotóelemeit, illetve felhívni a figyelmet a benne rejlő humán kockázati elemekre.

- A humán kockázatokat csoportosítani, a csoportokat elemezni, valamint szemléltetni esetleges eszkalációjukat, gyakorlati példákon keresztül.

- Felállítani egy komplex képet a humán kockázatokban rejlő rendkívül nagy veszélyforrásra, az infokommunikációs rendszerek vonatkozásában.

- Kiindulási alapot teremteni a kritikus információs infrastruktúra védelem jogszabályi biztosítékainak, kockázat kezelésének, valamint megelőzésének későbbi kutatásához.

3. Kutatási módszerek

A pályázat elkészítése során kezdetben, a korábbi tanulmányaim alatt megszerzett ismereteim kibővítése céljából, a kritikus infrastruktúrával, valamint a humán kockázatokkal kapcsolatos tudományos, szakirodalmi források kerültek feldolgozásra, majd ezt követően nyílt forrásokban megjelenő publikációkat elemeztem és emeltem be a tanulmányba.
Felhasználtam szakmai konferenciákon elhangzott előadások elemeit is, melyek még komplexebbé, és hitelesebbé teszik a kutatást.

1. Fejezet

Humán kockázatok értelmezése a kritikus információs infrastruktúra tükrében

1.1. A kritikus információs infrastruktúra meghatározása

A fogalom maradéktalan meghatározásához lényeges az egyes elemek értelmezése. Elsőként az infrastruktúra fogalmát szükséges meghatározni, ezt különböző szakirodalmak próbálják definiálni.

A Magyar Larousse Enciklopédia definiálása szerint az infrastruktúra „*a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.). Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák).” (Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.)*

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése *„a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.” (Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.)*

Egy másik meghatározás szerint az infrastruktúra nem más, mint *„egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.” (*Haig Zsolt, *Várhegyi István ezredes: Hadviselés az információs hadszíntéren, Zrínyi, Budapest, 2005.)*

A fenti meghatározások alapján, az infrastruktúra a gazdaságtudományban megjelenő fogalom, amely magában foglalja azon gazdasági javakat, folyamatokat, melyek közvetlenül nem, de közvetve befolyásolják a nemzetgazdaság elemeinek fejlődését, mind termelési, mind innovációs szinten.

Az információ nem más, mint „bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.” *(2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 5§ 25)*)

A kritikusság lényegi megfogalmazása alapján, *„kritikus minden "dolog" amelyek megsemmisülése, működésének vagy szolgáltatásainak alacsonyabb szintje, elérhetőségének megszűnése vagy csökkenése valamilyen támogatott objektumra, folyamatra jelentős (ebben az esetben egyértelműen negatív) hatást gyakorol.” (Dr. Bognár Balázs PhD pv. őrnagy: A kritikus infrastruktúra, OKF Iparbiztonsági link, forrás: http://www.katasztrofavedelem.hu/index2.php?pageid=pvl_kritikus_infrastr-uktura (letöltés ideje: 2017.szeptember.12)*)
Mindezek alapján egy folyamat, vagy rendszer kritikusságát az határozza meg, hogy egy bekövetkező támadás, vagy kapacitáshiány, milyen negatív hatással lesz más, szorosan hozzá kapcsolódó rendszerekre, azaz a kármérték nagysága a viszonyítási alap.

Valójában értelmezési szempontból nem létezik kritikus információs infrastruktúra, hiszen e három szó összekapcsolása egy igen nehezen értelmezhető fogalmat alkotna.
„Már a kritikus jelző használata sem a legjobb, hiszen nem az infrastruktúra a kritikus, hanem annak elvesztése, sérülése válhat kritikussá, ezért célszerűbb lenne a – néhány fordításban használt – létfontosságú kifejezést használni. Az információs infrastruktúra sem igazán szabatos kifejezés magyarul, mert abba például a könyvtárakat is bele kell érteni, holott mindenki érti és érzi, hogy itt nem információs, hanem elektronikus információs infrastruktúrákról van szó.”(Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007. 11. o.) Ennek ellenére a kritikus információs infrastruktúra fogalom honosodott meg mind a köznyelvezetben, mind a tudományos nyelvezetben egyaránt, pedig szövegkohéziós szempontból a *„létfontosságú elektronikus információs infrastruktúra”* kifejezés alkalmazása lenne nyelvtanilag helyes. A tudományos nyelvezet használata okán továbbra is a kritikus információs infrastruktúra használatára kerül sor a pályázat további fejezeteiben is.

A fentiekből levezetve a kritikus információs infrastruktúra nem más, mint nemzeti vagy nemzetközi szinten, az általánosan értelmezett biztonság elemei számára, a szellemi és tárgyi életfeltételekhez szükséges információk áramlását biztosító szervezetek, létesítmények, hálózatok, információs-technológiai berendezések összessége, melyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése negatív hatással járhat.
Ez esetben a kármértéket, az információs infrastruktúra nem megfelelő működéséből adódó károk fogják meghatározni. Tehát azt kell vizsgálni, hogy az adat hiánya milyen kimenetelű döntések akadályozását, illetve ellehetetlenítését eredményezheti.

1.2. A humán kockázat meghatározása

Az információs infrastruktúrát vizsgálva, elsődleges humán kockázatokat a felhasználók, azaz a kommunikációs felek, valamint az üzemeltető-szakszemélyzet, vagyis a rendszergazdák, karbantartók, illetve a beszállítók jelenthetnek. A személyi állománynak tisztában kell lennie, milyen jelentőségű információk és döntési lehetőségek birtokába kerülhet, melyek privilegizált célpontjává tehetik őket bűnszervezetek vagy ellenérdekelt szolgálatok számára.

A humán kockázat fogalmi meghatározásához, meg kell vizsgálnunk a „humán” szó jelentését, illetve definiálni kell a kockázat fogalmat, mint biztonságot veszélyeztető tényezőt. Érdemes megvizsgálni a kockázat általános és nemzetbiztonsági meghatározását.
A kockázat általános megfogalmazása: *„a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.” (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1§ 28)*)
A kockázat meghatározása nemzetbiztonsági aspektusból nem mást, mint *„az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek.” (Dr. Resperger István mk. alezredes: Nemzetbiztonsági alapismeretek, 2. Fejezet Biztonsági kihívások, kockázatok és fenyegetések 2030-ig, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 31. o.)*

Mind a két fogalomban megjelenik a veszélyeztetettség lehetősége. Abban az esetben, ha ezeknek a kockázati tényezőknek a forrása, valamely személyhez köthető magatartás, humán kockázatokról beszélhetünk.
Humán kockázatnak minősülnek azok, a személyi állománynál fennálló körülmények, - különösen a negatív személyiségjegyek, konfliktusokkal terhelt környezeti vagy élethelyzetekből származó fenyegetettségek, életviteli és mentális problémák - amelyek fennállása önmagában nem, de az adott, fokozott kockázatú munkakörökben végzett feladattal összefüggésben, fenyegetettséget jelenthetnek az általánosan értelmezett biztonság egyes összetevőire.

Ilyen kockázati tényezőt jelenthet a nem megfelelő informatika-biztonsági ismeretek és a szabályozók hiánya, amelyek következtében a felhasználók magas kockázatú adatokat tárolhatnak, nem megfelelő biztonsági elemekkel ellátott adathordozón. A hordozóeszköz megszerzése esetén, az ellenérdekelt fél könnyen hozzájuthat az infokommunikációs rendszer titkosságát veszélyeztető adatokhoz, például felhasználó nevekhez, jelszavakhoz, kriptográfiai adatokhoz.
Egy megsértett, kiábrándult beosztott, szintén magában hordozza a kockázati tényezőt. Az ilyen alkalmazott elkeseredettségében, dühében a vezetővel szembeni személyes konfliktus okán, képes blokkolni az információáramlást, így nem jutnak el vagy téves adatok érkeznek a döntési folyamatban résztvevő személyekhez, elindítva akár mérhetetlen károkkal járó, egy rossz felsővezetői döntéshez vezető folyamatot.
Nem szabad megfeledkezni a bűnszervezetek és idegen titkosszolgálatok által egyre jobban kedvelt pszichológiai manipuláció módszeréről, azaz a social enginering alkalmazásáról sem. A folyamat célja, kiválasztani egy releváns adatokkal rendelkező, vagy ilyen adatokhoz hozzáférő beosztottat, vagy vezetőt a megtámadni kívánt szervezet állományából, majd a bizalmába férkőzve, ezen adatokat kiszivárogatni a támadás végrehajtásához, esetleg felhasználni a beszervezett egyént a végrehajtási folyamatokba is. *(Alissa Torres: A pszichológiai manipuláció (social engineering), OUCH, The SANS Instute 2014, 2014. 11. forrás: https://securingthehuman.sans.org/newsletters/ouch/ issues/OUCH-201411_hu.pdf (letöltés ideje: 2017. szeptember. 12)*

Ahhoz, hogy komplexen lássuk a kockázati amplitúdót és fel lehessen állítani egy kockázati rátát, szükséges a folyamat kiindulópontjaként az információ áramoltatás rendszerébe való bekerülést, azaz a humán „in-put”-ot meghatározni.

Ez annyit jelent, hogy ellenőrizni kell a kockázati tényezők meglétét minden olyan személynél, aki a kritikus információs infrastruktúra rendszerében kíván feladatot ellátni, még a munkakör betöltése előtti előszűrés végrehajtásával. Azaz, az információs infrastruktúra szemszögéből vizsgálva, közvetett kockázat monitoring zajlik. Ez lényegében annyit jelent, hogy egy hatalmas kockázati halmazból ki kell szűrni azokat az elemeket, amelyek nem rendelkeznek kockázati tényezővel. A rendvédelmi szervek esetében, erre szolgál például a nemzetbiztonsági ellenőrzés *(1995. évi CXXV. törvény - a nemzetbiztonsági szolgálatokról 4§ 9) 5§ f) 6§ r) 8§ f)*), illetve a Nemzeti Védelmi Szolgálat által végrehajtott kifogástalan életvitel ellenőrzés *(293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról 7§ (1) d)*). A rendvédelmi szervek állományába kerüléshez, az egészségügyi, pszichológiai alkalmassági vizsgálatokon történő megfelelés, szintén törvényi kötelem. *(2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról 33§ c)*). A szűrések végrehajtása során a munkakört betöltő személynél vizsgálják, hogy előélete során, milyen kockázatot jelentő élethelyzetbe került, milyen kapcsolati hálóval rendelkezik, megfelel-e a szenzitív adatok biztonságát biztosító markerek szintjének, nincsenek esetleges szervi, személyiségbeli, pszichés betegségei, amelyek alkalmatlanná teszik a beosztás betöltéséhez.

Az előszűrés végrehajtásának negatív eredménye előtt (pozitív kockázati tényező esetében alkalmatlan az „in-put”), a teljes folyamatot vizsgálva rendkívül magas a kockázati arány, ami persze leredukálódik a legoptimálisabb esetet vizsgálva, hiszen kockázati tényezőt nem tartalmazó humánerő kerül az információs infrastruktúra rendszerébe. Sajnos egyre nagyobb problémát jelent a nem kellő biztonságtudatos magatartás megléte, és továbbfejlesztésének lehetősége a potenciális munkaerő körében. Ennek szűrésére bizonyos rendvédelmi szervek kivételével, már a felvételi vizsgálatok alkalmával sem fordítanak kellő figyelmet a közigazgatási szervek, valamint a magánszektor elemei.

A felvételt megelőző időintervallumban a lehetséges kármérték igen alacsony, ami annak köszönhető, hogy a felvételiző nem rendelkezik valós ismeretekkel a kritikus információs infrastruktúra működésével kapcsolatban.

A következő szinten, a tényleges feladat-végrehajtás során felmerülő közvetlen kockázatok helyezkednek el. Ebben a szakaszban hajtódnak végre az információ létrehozásával, továbbításával, feldolgozásával kapcsolatos feladatok. Tényleges adatok birtokába kerül a humánerő, ez a legszenzitívebb része az információs rendszer működésének, hiszen ekkor van a legnagyobb relevanciája károsítani az infrastruktúra valamely elemét az alkalmazottnak. Ugyanakkor, egy megfelelően működő előszűrő rendszer esetén ekkor kellene a legalacsonyabb szintűnek lennie a kockázat fenyegetéssé alakulásának, mivel olyan személy került be a rendszerbe, aki nem rendelkezik biztonsági kockázattal. A munkáltató által a biztonságtudatos magatartás tovább fejlesztése, a közbenső szűrő és elhárító tevékenység is folyamatos kell, hogy legyen.
A kockázati ráta viszont nem redukálható le nullára, mivel az információkhoz való hozzáférés növeli a humán kockázat mértékét. Ebben a folyamatban van lehetőség az információ áram blokkolására, adatok kiszivárogtatására, a rendszer működésének akadályozására. A humán kockázat, ha az aktív munkavégzése során válik valós fenyegetéssé, vagy tényleges károkozássá, a kármérték ekkor lesz a legmagasabb. Ezen szakaszban van lehetőség a döntéshozó számára szükséges adat elérhetetlenné tételére, illetve a jogosulatlan szervezetek számára való hozzáférhetővé tevésére, akár aktív, akár passzív módon. A humán kockázat általi károkozás lehetősége, a tényleges munkafeladat végrehajtása során fenyeget a legnagyobb károkozással.

A harmadik fázis az „out-put” oldal, ekkor a munkaerő kikerül a kritikus információs infrastruktúra működtetésének rendszeréből. Ennek legoptimálisabb szakasza a nyugállományba vonulás. A kockázat egyik oldalról csökken, hiszen nem kerül a volt humánerő újabb aktuális információk birtokába, illetve a legoptimálisabb helyzetben a kialakult, magas szintű biztonságtudatos magatartás okán, nem is szivárogtathat ki korábban megszerzett adatokat, így a lehetséges kármérték újra leredukálódik.

Másik oldalról viszont nő a kockázat, hiszen a rezsimszabályok alóli kikerülés és egyéb, később vizsgált változó személyiség jegyek miatt, a biztonságtudatos magatartás csökken, megjelenhet az új környezet előtti megfelelési kényszer, ebből fakadóan a túlzott közlékenység. A teljes kockázati amplitúdót vizsgálva viszont megállapítható, hogy a károkozás mértéke szintén alacsony, akár csak az „in-put" szakaszban, hiszen a volt dolgozó nem rendelkezik töménytelen, aktuális döntési folyamatokat befolyásoló információval, illetve tényleges támadást nem tud végrehajtani a kritikus információs infrastruktúra ellen. *(1. számú melléklet)*

Kilépés, felmondás és elbocsájtás esetén a kockázatok nem redukálódnak ilyen alacsony szintre, inkább adott pillanatban jelentősek, hiszen a munkaviszony megszűnésének ezen eseteit kiválthatja valamilyen negatív érzés (sértődés, féltékenység, ellenszenv), amit kockázati tényezőnek kell értékelni.

A fentiek alapján kijelenthető, hogy vannak a kockázatot befolyásoló tényezők. Ilyen lehet az egyén biztonságtudatossága, a rendelkezésére álló információk mennyisége és minősége, a lehetséges károkozás mértéke, valamint egyéb külső ingerek. *(Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 73. o.)* A humánkockázat mértékét leghatásosabban személyi oldalról lehet csökkenteni, mivel a kármértéket nem egyedi tényezők, hanem komplex elemek alkotják. Ezért érdemes a személyi állomány oldaláról elemezni, majd csoportosítani a kockázatok jellemzőit, későbbi minimalizálásuk érdekében.

2. Fejezet
Humán kockázatok csoportosítása

Ahhoz, hogy a legátfogóbban ismerjük a humán kockázatok jellemzőit, és a leghatékonyabban lehessen fellépni ellenük, érdemes csoportosítani őket alanyi oldalról bűnösség szerint, a kockázatokat meg kell határozni eredet szerint, továbbá meg kell vizsgálni, hogy a kockázat milyen célzattal alakulhat ki.
A csoportosítás szempontjai az elemek bizonyos tulajdonságai alapján kerültek felállításra, de a csoportok között rendszerint átfedés van. Például attól, hogy valamely kockázati tényező szándékos magatartást feltételez, még lehet külső vagy belső tényező.

2.1. Bűnösség szerint

Először alanyi oldalról vizsgálva, meg kell különböztetni a kockázati magatartást szándékos illetve gondatlan végrehajtási lehetőségek alapján. Kockázati tényező lehet nem megfelelő körültekintés eredményeként bekövetkező, hanyagul, gondatlanul elkövetett cselekmény, illetve akaratlagos, tettleges, azaz szándékos elkövetési magatartás is. *(Balogh Ágnes, Tóth Mihály: Magyar büntetőjog. Általános rész, TAMOP 4.2.5 Pályázat, Osiris Kiadó, Budapest, 2010, forrás: http://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_520_magyar_buntetojog/ch03s06.html (letöltés ideje: 2017.szeptember 15.)*

2.1.1. Gondatlan magatartás

A gondatlan kockázati tényezők legfőbb generálója, a nem megfelelő biztonságtudatos magatartás eredményezte hanyagság, mely következtében az infrastruktúra biztonságát hivatott szabályozók figyelmen kívül hagyása történik. Ilyen esetek lehetnek például a rendszer működtetéséhez szükséges adatok nem megfelelő kezelése, szenzitív információkat tartalmazó jegyzetek megsemmisítésének elmulasztása, mások számára is hozzáférhetővé tevése. Elektronikus adatok nem megfelelő hordozón történő tárolása, amely által könnyen megismerhetővé válnak inkompetens személyek számára. (Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013. 26. o.)

Rendkívül nagy problémát jelent a túlzott közlékenység, amely során szenzitív információk szivároghatnak ki. A minősített adatkezelésben nincs bizalom, soha nem tudhatjuk, hogy hobbink, magánéletünk során kikkel kerülhetünk kapcsolatba. Igen felelőtlen dolog lenne azt hinni, hogy értékes információk birtokába lévő személyt leplezett módon nem kereshet fel ellenérdekelt szolgálat fedett alkalmazottja. Biztonsági kockázatként kell értékelni minden új kapcsolatot, aki túlzott bizalmaskodást és támogatást kínál, még ha eleinte ezt ellenszolgáltatás fejében is teszi.

Rendkívüli módon sértheti a biztonságot, a jó szándékból elkövetett normák megsértése. Az objektumokba való belépési feltételeket meghatározó szabályozók figyelmen kívül hagyása igen nagy kockázati elem, például egy kollégának kiadó személy belépésének biztosítása saját belépőkártyánkkal, belépő ponton keresztül, mivel arra hivatkozik, hogy otthon felejtette a sajátját. Ez a helyzet ellenőrző-áteresztő pontokon való áthaladáskor is igen nagy problémát jelenthet, mivel illetéktelen személyek védett objektumon belüli mozgását biztosítjuk, ami által blokkolhatják az infokommunikációs rendszert. Így az elkövetők mozgása nem lesz nyomonkövethető és dokumentált, amely által a védett információk könnyen megismerhetővé válnak inkompetens személyek számára.

Hatalmas kockázat rejlik a tudatmódosító szerek fogyasztásában is. Az ezek által előidézett kontrolálatlan pszichés állapotot, igen nagy hatékonysággal ki tudják használni az erre szakosodott személyek, így érzékeny adatokhoz jutva a kommunikációs rendszerről. Nem véletlenül szükséges az efféle kockázatokkal rendelkező humánerőt, már a szervezethez kerülés előtt kiszűrni, hiszen magas veszélyekkel járhat az adatszivárogtatás lehetősége.

A fenti példák jól mutatják, hogy nem károkozási céllal szegte meg a humánerő a biztonsági normákat, hanem hanyagságból, következetlenségből, mely abból ered, hogy nincs tisztában magatartásának esetleges biztonságot veszélyeztető következményeivel. Rendkívül fontos ez esetben a biztonságtudatos magatartás folyamatos fejlesztése, oktatása és szavatolása a munkáltató részéről, hisz másképp nem sikerülhet a mulasztás eredményezte humán kockázati elemeket leredukálni. *(Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 74-78. o.)*

2.1.2. Szándékos magatartás

A szándékos elkövetés büntetőjogi szankcionálása a legsúlyosabb, hiszen itt a károkozás bekövetkezése akaratlagos tevékenység útján valósulhat meg. (*2012. évi C. törvény a Büntető Törvénykönyvről/1998. évi XIX. törvény a büntetőeljárásról)*. A humánerő szándékos károkozásának kockázati lehetősége, mindig valamilyen inger hatására jön létre. Az előszűrések elvileg megakadályozzák a rendszerbe kerülését, olyan elemeknek, akik anyagi, ideológiai vagy pszichés okokból, károkozási szándékkal kívánnak az információs infrastruktúra rendszerébe bekerülni, de a hatalmas személyi állomány feladatának végrehajtása során, nagy kihívást jelent a folyamatos szűrés.
Kialakulhat olyan helyzet, amikor a munkavállaló munkáltatóval szembeni sértettsége, a rendszerbe való csalódottsága, kiábrándulása, esetleges bűnözői csoportokkal való kapcsolatba kerülése, magában hordozza a szándékos károkozás lehetőségét. Ilyen ok lehet az extrém munkahelyi stressz, a vezető nem megfelelő irányítási, személyügyi módszerei, az egyénben rejlő innovációs lehetőségek elfojtása, a munkatevékenység nem megfelelő értékelése.

Igen nagy kockázat rejlik már az előszűréskor is vizsgált függőségekben és szenvedélyekben egyaránt, akár legyen az az alkohol, a kábítószer, a szerencsejáték, valamint a nagy vagyoni hátteret kívánó luxus hobbik. A függőségét, szenvedélyét a dolgozó minden áron ki akarja elégíteni, ehhez nem sajnálva időt, anyagi fedezetet, amit egy idő után csak a munkabérén felüli forrásokból tud pótolni, így adósságcsapdába kerülhet. Amennyiben a kapott összeget nem tudja törleszteni a dolgozó, információkat kérhetnek tőle a „hitelezői", esetleg kereskedni kezdhet a birtokába lévő adatokkal, adathordozókkal. A közelmúltban a Brit Királyi Haditengerészet egy fegyvermérnöke, a rendszeresített rakétákra vonatkozó adatokkal teli laptopokat adott el ismeretleneknek, aminek bevételeit hatalmas kaszinó tartozásainak törlesztésére fordította. *(Humán kockázatok: a leggyengébb láncszem, Crisma, forrás*: *http://www.carisma.hu/cikkek/human_kockazatok.html. (letöltés ideje: 2017. szeptember. 17.)*

Nagy figyelmet igényel az is, ha a humánerő magánélete során szimpatizálni kezd ellenérdekelt szervezetek tevékenységével, esetleg bűnszervezet tagja lesz. A rendszerbe való passzív csalódottságát egyfajta aktív cselekvésre való akarat váltja fel, például ellenérdekelt hírszerző tevékenység támogatása során. Vallási radikalizálódás esetén, fennáll a lehetősége

egy terrortámadás támogatására a támadott fél kommunikációjának blokkolásával, mely hatására a reagáló erők nem lesznek képesek az információcserére, így meghiúsítva az elhárítás és mentesítés folyamatát. *(Dr. Kis-Benedek József: Célkeresztben az Iszlám Állam, Ludovika Szabadegyetem, Budapest. 2015.11.10.)*

2.2. Eredet szerint

A kockázatokat vizsgálni kell forrásuk szerint, vagyis meg kell határozni, hogy milyen eredetűek. Eszerint a kockázat lehet külső forrás, egy potenciális dolgozó jelölt, valamint lehet belső humán forrás, miszerint a kockázati tényezőt egy racionális munkatárs jelenti. A továbbiakban szétválasztásra kerül a külső támadó bejuttatása és a támadók által megtévesztett, vagy hanyag magatartást tanúsító humán kockázati elem fogalma, illetve köztes csoportként elemzésre kerül a menesztett alkalmazottak köre.

2.2.1. Külső forrás

Külső forrásként kell tekinteni azokra az elemekre, akik a kritikus információs infrastruktúrán kívülről érkező veszélyeztető tényezők, még akkor is, ha egyes tagjaikat sikerült a rendszerbe betelepíteniük. Fontos a külső humán kockázati tényezők kategorizálása az információs infrastruktúrához viszonyított elhelyezkedésük alapján.

Legtávolabb állnak a passzív közvetett tényezők. Ezek az elemek azok a bűnszervezetek, ellenérdekelt szolgálatok, akik veszélyeztethetnék a rendszer működését, de a vizsgált időszakban ilyen irányú szándék, vagy tevékenység nem jellemzi működésüket. Rendkívül nagy jelentősége van a hírszerző modulok működésének a számunkra negatív elemek feltérképezésében és lokalizálásában.
Őket követik az aktív közvetett tényezők, akik már tevőlegesen törekednek a szervezetbe férkőzni. Ez annyit jelent, hogy tagjaikat megpróbálják felvételiztetni, bejuttatni valamely részegység állományába, így előkészítve a műveleteikhez szükséges stratégiai pontokat. Ezen tényezők blokkolását az előszűrő rendszerek kifogástalan működésének kellene szavatolnia.
Következő szinten számolunk az igen nagy fenyegetést jelentő passzív közvetlen humán kockázati tényezőkkel, akik a nem megfelelően működő lokalizációs hírszerző tevékenység és előszűrő rendszerek okán bekerültek az infokommunikációt biztosító szervezetbe. Itt már a tényleges károkozás lehetőségével kell számolni, hiszen valós adatokhoz jutnak a kockázati

tényezők a rendszer működésével kapcsolatban, így azt blokkolhatják is. Ezen a szinten a szervezet belső elhárító mechanizmusai hivatottak az illegális szándék feltérképezésére és a rendszerből való kiemelésére a lehetséges károkozás megelőzése céljából.
A negyedik lépcső, amikor a humán kockázat a fenyegetésen túl tényleges károkozásként jelenik meg, vagyis aktív közvetlen kockázati tényező realizálódik a kritikus információs infrastruktúrában. Ekkor beszélhetünk racionális támadóról, aki ténylegesen információkat szolgáltat ki a rendszer működéséről, akadályozza a kommunikációt, háttértámogatást nyújt illegális tevékenységek végrehajtásához az ellenérdekelt küldő szerv részére. Ebben a szakaszban a belső elhárító egységek mellett a külső társszervek feladata a támadás lokalizálása és elhárítása. Abban az esetben, ha idáig képes egy bűnszervezet valamely tagját eljutatni, akkor a biztonsági elemek működése rendkívül sok kívánni valót hagy maga után, hiszen minimum három biztonsági lépcsőt sikerült deaktiválnia a támadó félnek.

2.2.2. Belső forrás

Belső kockázati tényezőként kell tekinteni az információs infrastruktúrát működtető személyi állományt és a hozzájuk köthető egyéb humán kapcsolataikat. Belső forrásnak számít a dolgozó abban az esetben is, ha egy külső kockázati forrás befolyásával, megtévesztésével hajt végre akciót, illetve ha fennáll a lehetősége, hogy mulasztással szivárogtat ki információkat.
A munkaviszony ideje alatt a munkavállaló magánéletében számos olyan esemény történhet, amely magatartását negatív irányba befolyásolhatja. Ebben az esetben azok a személyek, akik nem rendelkeznek kellő biztonságtudatos magatartással, és elég fegyelemmel a normák betartása iránt, sajnos könnyen megszeghetik az előírásokat. Nem tudnak magánéleti problémáik miatt kellően koncentrálni a munkafolyamatok kifogástalan végrehajtására, így károkat okoznak a rendszer működésében. Nem kellő odafigyeléssel kezelik a rájuk bízott adatokat, amelyek megsemmisülhetnek, megsérülhetnek vagy hiány keletkezhet bennük.
Például egy rendszergazda úgy telepít újra egy operációs rendszert, hogy nem mentett le minden adatot merevlemezre, így az újratelepítés során azok megsemmisülnek.
Magas kockázati elemeket hordoz magában az alkalmazott kiégése, sértettsége, kapzsisága. Ez esetben elég csak azt megvizsgálni, milyen károkkal járhat, ha egy dolgozó, hon- vagy rendvédelmi alakulatok által használt rádiójel átjátszó tornyoknak a pontos helyére, és védelmi fokára vonatkozó adatokat csempész ki anyagi ellenszolgáltatás fejében bűnözői

csoportok, vagy ellenséges államok számára. Így pontos ismeretek kerülhetnek a birtokukba a kommunikációs hálózat megbénításának végrehajtásához, egy esetleges katonai művelet során.
Ezen példák jól mutatják, hogy a humán „in-put”-ra jellemző kockázatok, a munkaviszony ideje alatt is kialakulhatnak.

Rendkívüli nagy kockázati tényező a világháló, azon belül is a közösségi oldalak, levelező rendszerek nem kellően körültekintő alkalmazása. Ezeken a humánerő, hanyag biztonságtudatos magatartásának következtében, mindenki számára hozzáférhető adatokat adhat meg magáról, családjáról, barátairól, hobbijáról, munkahelyéről és az ott végzett tevékenységéről.
Léteznek mindenki számára hozzáférhető adathalász programok, melyek segítségével bárki a számára érdekes személyről, mérhetetlen mennyiségű, az internetre feltöltött és hozzájuk kapcsolható információt gyűjthet össze. Ezeket számos bűnszervezet is alkalmazza, így szerezve megtévesztéshez, befolyásoláshoz, zsaroláshoz szükséges adatokat a ” leggyengébb láncszemről”. *(Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013. 36-66. o.)*

Az Egyesült Királyságbeli Sophos Group Plc. egy 2010-es jelentése szerint, a közösségi oldalakon robbanásszerűen megnőtt a kártékony programok és spamek száma. A jelentés szerint 2009-ben a közösségi oldalakat használók 57%-a számolt be arról, hogy profilját spamelték[144]. Ez 70%-os növekedést jelent 2008-hoz képest. A vizsgált 500 vállalat vezetőjének ¾-e úgy tartja, hogy alkalmazottai humán kockázatot jelentenek, hiszen munkaidőben látogatják a biztonsági szempontból nem megfelelő közösségi oldalakat. *(Durbák Ildikó: Ellopott céges információk, Profession, 2010, Forrás: https://www.profession.hu/cikk/20100722/ellopott-ceges-informaciok/401#, (letöltés ideje: 2017. szeptember 17.)*

[144] Spam: elektronikus úton továbbított kéretlen reklámlevél *(Dr. Dósa Imre: A Spam jogi szabályozása, 2004. 1. o. forrás: https://nws.niif.hu/ncd2004/docs/ehu/112.pdf (letöltés dátuma: 2017. szeptember 22.)*

A gondatlan eredetű humán kockázatok felhasználásával bűnözői csoportok, ellenérdekelt szervezetek, könnyen alakíthatnak ki szándékos károkozó magatartást az alkalmazottaknál.
A nem megfelelő biztonságtudatos magatartást kihasználva pszichológiai manipuláció, azaz Social Engineering (SE) alkalmazásával könnyen bűnszervezetek, vagy ellenérdekelt szolgálatok célpontjává válhat a humánerő. Itt mutatkozik meg leginkább a túlzott közlékenységben rejlő kockázat, hiszen a közösségi oldalak elemzésével, olyan személyes adatokhoz juthat a támadó, amelyek segítségével ki tudja választani melyik, az infrastruktúra egyik elemével munkaviszonyban álló személy lesz a legalkalmasabb a megkörnyékezésre. A kiválasztásnál szempont a személlyel kapcsolatos nyilvánosan elérhető adatok mennyisége. *(Christopher Hadnagy: Social Engineering: The Art of Human Hacking, John Wiley & Sons, USA, 2010. nov. 29)*
A kiválasztott személy profiljának elemzése során a támadó beszerzi a manipulálásához szükséges adatokat - hobbi, szórakozás, munkahelyi jellemzők, család, barátok vonatkozásában - majd felépíti a kapcsolatépítéshez szükséges legendát. Ezt követi a megkeresés, majd a bizalomba férkőzés fázisa. Amikor sikerült a külső személynek kialakítania a kellő bizalmi viszonyt az alkalmazottal, megkezdődhet a manipuláció végrehajtása az információk kiszivárogtatása érdekében. *(Tóth Tamás: Az új irány, üzleti hírszerzés és elhárítás, OTDK dolgozat, Budapest, 2017. 45-46. o.)*
Ebben az esetben a humán kockázat kialakulása a nem megfelelő biztonságtudatos magatartásnak köszönhetően fennálló, túlzott közlékenység kapcsán vált veszélyeztető tényezővé. Azaz a kockázat belső eredetű, hiszen a manipulált humánerő önként adott át bizalmasan kezelt információkat illetéktelen, harmadik fél részére, ezáltal realizálódott a humán kockázatban rejlő veszélyforrás.

A levelező rendszerek kockázata is igen magas, hiszen ha a vállalati dolgozók magán e-mail fiókjukat használják az információs infrastruktúra működése szempontjából fontos és érzékeny adatok fogadására vagy továbbítására, az ellenérdekelt felek könnyen hozzájuthatnak adathalász e-mailek segítségével. A magán e-mail fiókok munkahelyi számítógépeken történő használata is igen nagy veszélyeket rejt magában. A PishMe e-mailfigyelő szolgáltatás jelentése szerint, 2016 első negyedévében vizsgált spamek 93%-a ransomware terjesztésére volt hivatott, ez az arány 2015 utolsó negyedévéhez képest 789 %-os növekedést mutat. *(Csizmazia Darab István, Az adathalász levelek legalább 93%-a zsaroló*

vírus, Antivírus Blog, 2016.06.07. forrás: http://antivirus.blog.hu/2016/06/07/az_adathalasz_levelek_93_-a_zsarolo_virus (letöltés ideje: 2017. szeptember 27.)

2.2.3. Köztes csoport

Köztes csoportként definiálható az elbocsájtott, kilépett alkalmazottak köre. Ez a csoport a szervezetről való ismeretei segítségével, legyen a célzat bármi, igen jelentős károkat tud okozni az információs infrastruktúra számára. Az ilyen alkalmazottak célpontjai lehetnek külső veszélyforrásoknak, hiszen a menesztett humánerő birtokában lévő információk megszerzése, lényeges eleme lehet az infrastrukturális elem működésének megismerésében..

„A sértődött vagy elbocsájtott emberek, a rendszer-ismeretükkel nagy károkat okozhatnak. Az okok általában; irigység, sértettség, bosszú, vandál pusztítási vágy, rosszindulat, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása, információszerzés anyagi vagy egyéb előnyökért" (Schutzbatz Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004. 83. o.)

Elég, csak a biztonságvédelmi elemekkel kapcsolatos ismeretek átadása egy ellenérdekelt állam számára, így megkönnyítve a felkészülést egy csapásmérés végrehajtásához. A humánerő elcsábítása, illetve szolgálatokhoz történő beszervezése igen nagy kockázati tényező, hiszen a magasabb bér vagy a jobb munkakörülmények szavatolásának ígérete, a legtöbb alkalmazottban felkelti az érdeklődést. A kármértéket ebben az esetben az csökkenti, hogy a volt munkavállaló nem rendelkezik fizikális hozzáféréssel az infrastruktúra elemeihez, illetve nem jut újabb naprakész információkhoz.

2.3. Eszkalálódás alapján

A megfelelő védelem kialakításához, ismernünk kell a kockázatokat indukáló tevékenységek célját, vagyis, hogy milyen célzattal történik a humán kockázat eszkalációja. Alapvetően három nagy csoportra sikerült tagolni a kockázatokat végkimenet szempontjából, az első az anyagi haszonszerzés, ezt követi az ellenérdekelt információgyűjtés, végül pedig a károkozás. Azért lényeges vizsgálni a humán kockázatokat eszkaláció szempontjából, mivel így, még a kockázat kialakulása során tudunk következtetni arra, hogy esetlegesen milyen típusú fenyegetéssé terjedhet ki.

2.3.1. Egyéni anyagi haszonszerzés

Egyéni anyagi haszonszerzés alatt, a belső alkalmazottak részéről végrehajtott illegális akciókat értünk jogosulatlan profitszerzés céljából. Ebbe a csoportba csak az illegális, közvetlen haszonszerző tevékenységek kerülnek definiálásra, mint például a lopás, sikkasztás és egyéb vagyonelleni bűncselekmények, szabálysértések.

Kifejezetten az alkalmazott által végrehajtott, a saját szükségletei kielégítésére, önmagában generált igény alapján elvégzett akciókat vizsgál a kutatás.

A humánerő, saját célra történő haszonszerzését leggyakrabban az alábbi kockázati tényezők eredményezhetik, mint például az alacsony bérezés, valamely függőségének és pénzügyi tartozásának kielégítése. A legnagyobb csábító erőt az adatokkal való illegális kereskedelemre, jelenleg a „bérkiegészítés" teszi ki. Fontos kihangsúlyozni, hogy ebben az esetben nem az információk átadása, hanem az ellenszolgáltatás, azaz a jogtalan anyagi haszonszerzés a cél.

Ezt bizonyítja James Goodnow jogász CNBC-nek tett nyilatkozata is: *"Bár a külső, hackerektől érkező támadások száma a digitalizációval párhuzamosan 2007 óta az egekbe szökött, az alkalmazottak által elkövetett adatlopások inkább a gazdaság állapotával állnak összefüggésben: recesszió idején csúcsokat dönt, míg javuló gazdasági környezetben csökken az ilyen visszaélések száma. Amikor a gazdaság nem teljesít jól, az emberekre nagyobb nyomás nehezedik, hogy olyasmiből is profitáljanak, amiből nem kellene"* (Kerkuska Viktórira: Belső ellenségek Adatlopások és visszaélések, 2016. 06. 03. (XX/22), Hetek, forrás: http://www.hetek.hu/hatter/201606/belso_ellensegek, (letöltés ideje: 2017. október 02.)

Ebbe a kategóriába tartozik az információkereskedés mellett, az adathordózók, technikai berendezések feketepiacon történő forgalomba hozatala is, mely visszaszorítása, illetve megakadályozása a fizikai biztonság növelésével valósulhat meg. Nagy jelentőséget kell fordítani a technikai eszközöket használó alkalmazottak gépjármű és csomagátvizsgálására, így megakadályozva a hardverek kicsempészését a munkafolyamatok végrehajtására szolgáló létesítményekből. Az élőerős átvizsgálás mellett, tovább növelheti a biztonságot a fémdetektoros kapuk, a gépjármű átvilágító röntgenberendezések vagy más biztonságtechnikai berendezések telepítése. *(Kálmán László: A csomagvizsgálati röntgenberendezés alkalmazási lehetősége, Hadmérnök, X. Évfolyam 3. szám, 15. o., 2015. szeptember)*

2.3.2. Illegális információgyűjtés

Az illegális információgyűjtés, legyen szó ipari kémkedésről, vagy gazdasági hírszerzésről, túlmutat az egyéni anyagi haszonszerzés generálta ingeren, hiszen itt már egy csoport információ igényének kielégítésére kerül sor. Ezen a szinten általános információgyűjtő tevékenység zajlik, amely célja minél szélesebb körű adatok begyűjtése, elemzés és tárolás céljából.

A gazdasági társaságok és az állami szervek egy része a külső támadások kivédése mellett, nem fordít kellő figyelmet a belső mulasztások, adateltulajdonítások megelőzésére illetve elhárítására. Adatbiztonsági szempontból megengedhetetlen, hogy a munkatársak hozzáférhessenek az információs infrastruktúra működéséhez szükséges adatállományokhoz, valamint, hogy azokat módosítani tudják. Jelentős visszatartó ereje van az adatbázis kezelés naplózásának, a jogosultsági szintek, valamint a hozzájuk kapcsolódó műveletek megfelelő meghatározásának.

Abban az esetben, ha nincs ellátva az informatikai rendszer efféle biztonsági elemekkel, egy külső befolyás alatt álló alkalmazott segítségével könnyen juthatnak információkhoz ellenérdekelt szolgálatok, vagy konkurens szervezetek az infrastruktúra egy meghatározó eleméről.

Ezt az állítást támasztja alá Lengyel Csaba, a Hungard Kft. szakmai vezetőjének 2015-ben tett nyilatkozata is: *„A biztonsági vizsgálatok során számos alkalommal találkozunk azzal, hogy egy kívülről nehezen feltörhető rendszer a belülről érkező veszélyek ellen teljesen védtelen.*" (*Olyan a céges pajzs, mint a szita, 2015.08.08. P/AC & PROF/T forrás: http://www.piacesprofit.hu/infokom/it_biztonsag/olyan-a-ceges-pajzs-mint-a-szita/ (letöltés ideje: 2017. október 03.).*

Az adatlopások kapcsán nem feltétlenül a kész információkat kell csak védeni, hanem a hozzájuk kapcsolódó metaadatokat is, hiszen ezek az adott információra jellemző adatállományok, amelyekkel átfogóbb ismereteket szerezhetnek a célinformációról.

Rendkívül nagy problémát jelent az adatszivárogtatásban a humán „in-put" nem megfelelő előszűrésének végrehajtása. Igen magas a száma a Kínai Népköztársaság által telepített ügynököknek, például az Amerikai Egyesült Államok területén működő multinacionális vállalatoknál, melyek egy része az USA kritikus információs infrastruktúrájában jelen van. Ezek a személyek az oktatási rendszert kihasználva bekerülnek a célország egyetemeire. Tanulmányaikat elvégezve, a nem megfelelően működő biztonsági szűrőrendszerek folytán

munkaviszonyt létesítenek telekommunikációs vállalatoknál. Ezáltal hozzáférnek szenzitív információkhoz és hozzájuk kapcsolódó metaadatokhoz, amelyeket kicsempészhetnek a küldő országba. (*Csíki Ádám: Hogyan vigyázzunk a szellemi termékeinkre – avagy a kritikus digitális vagyontárgyak védelme. K+F és Innováció – 2016 Fókuszban az iparági fejlesztési trendek, Konferencia és kiállítás, 2016.12.06.)*

A leggyakoribb humán kockázati tényezők a nem megfelelő biztonságtudatos magatartás, mely következtében könnyen hozzájuthatnak védendő adatokhoz illetéktelen személyek, például a nem megfelelően kezelt e-mail fiókok tekintetében. Továbbá jelentős problémát okozhatnak a nem megfelelően működő előszűrő rendszerek, melyeket kihasználva külső humán kockázat kerülhet az infrastruktúra működésébe. Ezek eszkalációja vezethet az adatvesztéshez, adatszivárogtatáshoz.

2.3.3. Károkozás

Az egyéni anyagi haszonszerzésen, valamint az adattár létrehozásra és kibővítésére irányuló illegális információgyűjtésen kívül, számolni kell a tényleges károkozás generálta akciók végrehajtására is. Ezeket szinten indukálhatja ellenérdekelt hatalom, az infrastruktúrát alkotó szervezet konkurens vállalata, illetve maga a humánerő egyaránt.

A károkozás legszignifikánsabb kockázati tényezője a sértettség. Az aktív alkalmazottaknál kialakulhat a sértettség munkahelyi féltékenységből, rossz vezetői értékelésekből, döntésekből. Ekkor a legérzékenyebb a humánerő ellenérdekelt, külső megkeresésekre, amik vagy információ igényben, vagy fizikai károkozó akciók végrehajtásban realizálódnak.

Fontos megemlítetni, hogy ebben az esetben az eszkalálódott humán kockázat valós eredménye a károkozás, ami független a tartó szerv adat-felhasználási igényeitől.

Igen jól szemlélteti a humán kockázatokban rejlő veszélyt a 2017-ben Európán végigsöprő zsarolóvírussal végrehajtott támadás.

Az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) biztonsági réseket fedezett fel a Windows operációs rendszereiben. Ezek kihasználására megalkották az EnternalBlue elnevezésű exploitot[145]. Ezt az információt, és az exploitot, nagy

[145] Informatikai biztonsági fogalom: olyan forráskódban terjesztett vagy bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést. *(forrás: http://searchsecurity.techtarget.com/definition/exploit)*

valószínűséggel egy belső munkatárson keresztül, sikerült kicsempésznie a The Shadow Brokers nevű hackercsoportnak, akik a birtokukba került adatok felhasználásával megalkották, a WannaCry nevezetű ransomwar, leállító kód nélküli változatát. A zsarolóvírus felhasználta az EnternalBlue parancssorozat tulajdonságait, amely által blokkolni tudta a Windows alapú operációs rendszerrel rendelkező számítógépeket. Pár nap leforgása alatt, számos a nemzetközi szinten működő telekommunikációs vállalat adatállományát titkosította a vírus. Összesen 74 országban észlelet támadást a Kasperky Lab orosz számítógépes biztonsági cég. A támadott telekommunikációs vállalatok mindegyike része a kritikus információs infrastruktúra nemzeti, illetve nemzetközi platformjainak. Spanyolországban a Telefonica és a Vodafon, Portugáliában a Telecom, Oroszországban a MegaFon multinacionális távközlési vállalat számolt be arról, hogy kibertámadás érte a rendszereiket. A fenti esemény során adatállományok kerültek titkosításra, a kommunikációs csatornák csak azért nem omlottak össze, mert a vírus nem ilyen feladat végrehajtására volt megalkotva.

Ez a példa jól mutatja, hogy egy ellopott adatállomány, illegális felhasználása mekkora méretű veszélyforrás lehet egy globális kiterjedésű kibertámadás végrehajtása során. Ezt az egész eseménysorozat, nagy valószínűséggel egy eszkalálódott humán kockázati tényező indukálta. *(Nicole Perlroth, David E. Sangermay: Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool, The New York Times, 2017.05.12.)*

4. Konklúziók és eredmények

A pályázat során sikerült megvizsgálni a ’kritikus információs infrastruktúra’ kifejezés alkotóeleminek különböző szempontú meghatározásait, továbbá ezek alapján megalkotni egy általános és pontos definíciót a kritikus információs infrastruktúra vonatkozásában. Jól látható, hogy az infrastruktúra meghatározása ágazatonként más és más, ezért volt szükség a közös tartalmi elemek ismertetésére.

Ezt a gondolatmenetet követve bemutatásra került a ’humán kockázat’ kifejezés tartalmi eleminek meghatározása. Sikerült prezentálni a kockázat általános és a biztonság aspektusaiból történő megfogalmazását is.

Elsődlegesen a humán kockázatok, büntetőjogi ismérv alapján kerültek elemzésre, méghozzá a bűnösség szempontjából. E szerint a gondatlan és a szándékos magatartás, mint kiváltó ok volt a csoportosítás fő irányvonala. Sikerült szemléltetni a hanyagság következtében kialakuló

nem megfelelő biztonság tudatos magatartás kockázati elemeit, valamint a közvetlen és közvetett, aktív és passzív kockázati tényezőkben rejlő kihívásokat.

Ezt követte az eredet szerinti felbontás, miszerint sikerült infrastruktúrán belüli és külső forrásra tagolni a humán kockázatokat, valamint a volt alkalmazottak köre is vizsgálat tárgyát képezte. Ez a fajta szegmentálás segíti a megelőzést, és a kockázat felderítését az előszűrések és a folyamatos humán audit szempontjából.

Végső soron, a humán kockázatokon túlmutató kockázati eszkaláció szempontja volt a fő motívum, a csoportosításban. Ez alapján egyértelműen meghatározható az egyéni anyagi haszonszerzés, mely során a kockázat jogosulatlan haszonszerzés céljából eszkalálódik. A következő részhalmazt az illegális információgyűjtés alkotja, mely végrehajtása során az információigény biztosítása az eszkalációs folyamat indukáló tényezője. A legsúlyosabb következményekkel járó humán kockázati eszkaláció a károkozás, ekkor a kockázati tényező továbbfejlődését szándékos károkozás indukálja, aminek globális jelentőségét a 2017-es év során végrehajtott, nemzetközi zsarolóvírus támadás is alátámaszt.

A fentiek tükrében kijelenthetem, hogy a pályázati célkitűzések megvalósultak, miszerint elkészült egy kellő mélységű elemzés a humán kockázatok prezentálása céljából, ami jó alapot teremt későbbi kutatási folyamatok elvégzéséhez a kritikus információs infrastruktúra védelem jogszabályi biztosítékainak, kockázat kezelésének, valamint megelőzésének vonatkozásában.

Irodalomjegyzék

Szerzői művek

1. Christopher Hadnagy: Social Engineering: The Art of Human Hacking, John Wiley & Sons, USA, 2010. nov. 29

2. Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013.

3. Dr. Resperger István mk. alezredes: Nemzetbiztonsági alapismeretek, 2. Fejezet Biztonsági kihívások, kockázatok és fenyegetések 2030-ig, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013

4. Haig Zsolt, Várhegyi István ezredes: Hadviselés az információs hadszíntéren, Zrínyi, Budapest, 2005.

5. Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013.

6. Kálmán László: A csomagvizsgálati röntgenberendezés alkalmazási lehetősége, Hadmérnök, X. Évfolyam 3. szám, 15. o., 2015. szeptember.

7. Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

8. Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.

9. Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

10. Nicole Perlroth, David E. Sangermay: Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool, The New York Times, USA, 2017.05.12.

11. Schutzbatz Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004.

12. Tóth Tamás: Az új irány, üzleti hírszerzés és elhárítás, OTDK dolgozat, Budapest, 2017.

Konferenciák

1. Csíki Ádám: Hogyan vigyázzunk a szellemi termékeinkre – avagy a kritikus digitális vagyontárgyak védelme. K+F és Innováció – 2016 Fókuszban az iparági fejlesztési trendek, Konferencia és kiállítás, 2016.12.06.

2. Dr. Kis-Benedek József ezredes: Célkeresztben az Iszlám Állam, Ludovika Szabadegyetem, Budapest. 2015.11.10.

Jogszabályok

1. 1995. évi CXXV. törvény - a nemzetbiztonsági szolgálatokról

2. 1998. évi XIX. törvény a büntetőeljárásról

3. 2012. évi C. törvény a Büntető Törvénykönyvről

4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

5. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

6. 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról

7. 293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról

8. NATO Polgári Vészhelyzeti Tervezés, NATO Civil Emergency Planning – CEP, 2006

9. Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.

Internetről származó hivatkozások

5. Alissa Torres: A pszichológiai manipuláció (social engineering), OUCH, The SANS Instute 2014, 2014. 11. forrás: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH201411_hu.pdf (letöltés ideje: 2017. szeptember. 12)

6. Balogh Ágnes, Tóth Mihály: Magyar büntetőjog. Általános rész, TAMOP 4.2.5 Pályázat, Osiris Kiadó, Budapest, 2010, forrás: http://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_520_magyar_buntetojog/ch03s06.html (letöltés ideje: 2017.szeptember 15.)

7. Csizmnazia Darab István, Az adathalász levelek legalább 93%-a zsaroló vírus, Antivírus Blog, 2016.06.07. forrás: http://antivirus.blog.hu/2016/06/07/az_adathalasz_levelek_93_a_zsarolo_virus (letöltés ideje: 2017. szeptember 2.)

8. Dr. Bognár Balázs PhD pv. őrnagy: A kritikus infrastruktúra, OKF Iparbiztonsági link, forrás: http://www.katasztrofavedelem.hu/index2.php?_pageid=pvl_kritikus_infrastr-uktura (letöltés ideje: 2017.szeptember.12)

9. Durbák Ildikó: Ellopott céges információk, Profession, 2010, Forrás: https://www.profession.hu/cikk/20100722/ellopott-ceges-informaciok/401#, (letöltés ideje: 2017. szeptember 17.)

10. Humán kockázatok: a leggyengébb láncszem, Crisma, forrás: http://www.carisma.hu/cikkek/human_kockazatok.html (letöltés ideje: 2017. szeptember. 17.)

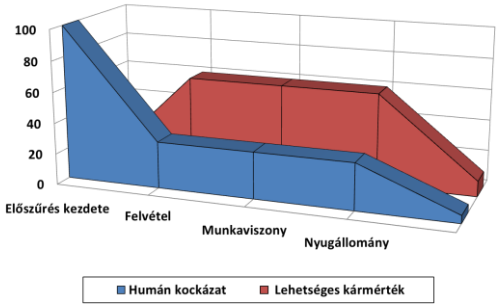
11. Kerkuska Viktórira: Belső ellenségek Adatlopások és visszaélések, 2016. 06. 03. (XX/22), Hetek, forrás: http://www.hetek.hu/hatter/201606/belso_ellensegek (letöltés ideje: 2017. október 02.)

12. Olyan a céges pajzs, mint a szita, 2015.08.08. P/AC & PROF/T forrás: http://www.piacesprofit.hu/infokom/it_biztonsag/olyan-a-ceges-pajzs-mint-a-szita/ (letöltés ideje: 2017. október 03.)

Mellékletek

1. számú melléklet:

A humán kockázatok és a lehetséges kármérték összefüggése



Forrás: „saját szerkesztés”

DR. KOVÁCS ISTVÁN

KIBERBIZTONSÁG? GYERMEKEK SZEXUÁLIS KIZSÁKMÁNYOLÁSA AZ INTERNETEN, AZAZ GYERMEKPORNOGRÁFIA MAGYARORSZÁGON, KÜLÖNÖS TEKINTETTEL A NEMZETKÖZI IOCTA, ÉS INHOPE ÉRTÉKELÉSEIRE

1. Bevezetés

1.1 Tudományos probléma megfogalmazása

Az internet olyan lenyűgöző, információkkal teli új világot hozott létre, ahová feltétel, és korlátozás nélkül a Földön élő összes ember beléphet, mindenki számára elérhető, aki online szolgáltatással rendelkezik. Egy virtuális autópálya, egy számítógépes mátrix, ahol az információ sebességkorlátozás nélkül száguld, és képes arra, hogy más számítógépekkel, mobiltelefonokkal, vagy más típusú technológiai eszközökkel a bolygó különböző sarkaiban élő embereket összekapcsolja.[146] Joggal hihetjük, hogy a gyermekek, és a felnőttek számára ez a technológiai egyedülálló lehetőségeket teremt (például: megismerhetjük az univerzum egészét, amelyben élünk), de sosem felejthetjük el, hogy - Janus kettős arcaként - sajnos a potenciál mellett, (ez a galaxis) visszaélések tekintetében is ugyan olyan veszélyforrás is egyben.[147] A senki földjén, egy olyan világban, ahol a valóság, és a virtualitás elmosódik, a személyek az identitásukat elrejtve, mosolygós hangulatjelek mögé bújva csak arra várnak, hogy áldozatokat szedjenek, kellően veszélyes ahhoz, hogy védekezzünk ellene: korlátozzuk,

[146] PETIT Miguel Juan: Rights of the Child. – United Nations: Economic and Social Council, 2004.

[147] Ianus (Janus) a római mitológiában a kezdet, és a vég kétarcú védőszelleme/istensége volt. Egyik arca a kezdetet, a jót, a másik arca a véget, a rosszat jelképezte. Bár álláspontom szerint a jó-, és rossz erkölcsi dilemmája sztereotíp, az egyén-, társadalomfüggő. In: BAGNALL Roger, BRODERSEN Kai, CHAMPION Craige, ERSKINE Andrew, HUEBNER Sabine: The Ecyclopedia of Ancient History. – United States: Wiley-Blackwell, 2012.

és szabályozzuk, hogy ennek a világméretű úthálózatnak ki válhat felhasználójává. A hálózat alapú-, és internetes technológiák, mint a hírfolyamok, chatprogramok, csevegőszobák, stb. a sztráda fő útvonalát jelentik, ahol a gyermekek szexuális kizsákmányolására szakosodott bűnözők garázdálkodhatnak. A különböző internetes felületek lehetővé tették, hogy a bűnözők világszerte kapcsolatokat létesíthessenek, a gyermekpornográfiával érintett anyagokat (képeket, videó-, és hangfelvételeket) birtokolhassanak, terjeszthessenek, és megoszthassanak.[148]

A világ-, és a számítástechnika globalizációjának köszönhetően -, az egyre nagyobb mértékű romlás iránti kereslet növekvő igényével párhuzamosan – mindezt úgy tehetik meg, hogy a megosztott tartalmaik a nagyközönség számára akár az országhatárakon belül, akár azokon kívül is költséghatékonyan elérhetővé váljanak. A szexipar – különböző ágazataival – hatalmas nyereséget termel. Becsléseink szerint az üzletágból befolyó profit nagysága éves szinten a 30-50 milliárd dollárt is eléri.[149] A pornográfia megszületésének hajnalán, az 1980-as években csak az Egyesült Államokban (Európát, és a többi kontinenst nem számolva) e szegmens értéke 8 millió dollárt ért el.[150] A századfordulón ez az árfolyam már a duplájára nőtt.[151] 1996-ban az interneten már több, mint 5000 kereskedelmi pornográf/erotikus webhelyszín működött, 1999-re ez a szám 30.000-re emelkedett, ami a legsikeresebb webhelyek számára az évek alatt 150-200 millió dollárt termelt.[152] Az internetes pornográf forgalom 43 százaléka ezekhez az explicit webhelyekhez köthető, a 15-25 éves korosztály elsődleges pornográf forrásként a leggyakrabban ezeket látogatja.[153] (És ezek csak felvételek, mi a helyzet az úgy nevezett „cam" oldalakkal? A „live", azaz élő internetes pornográf

[148] CROFTS Thomas, LEE Murray: „Sexting", Children and Child Pornography. In: Sydney Law Review, 2013., 35. évf. 85. sz. – p.: 85-106.

[149] HUGHES Donna: Men create the demand; Women are the supply. In: Safety at Work, 2000., 7. évf. – p.:10-14.

[150] COWAN Glen et. al: Dominance and inequality in X-rated videocassettes. In: Psychology of Women Quarterly, 1988., 12. évf. 3. sz. – p.:299-311.

[151] LANE Frederick: Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age. – New York: Routledge, 2000.

[152] MORIAS Richard et. al: Porn goes public. – New York: Forbes, 1999.

[153] HÄGGSTRÖM-NORDIN Elizabeth et. al: Associations between pornography consumption and sexual practices among adolescents in Sweden. In: International Journal of STD and AIDS, 2005., 16. évf. – p.: 102-107.

oldalak látogatottsága, és profitja még magasabb: lásd például a livejasmin.com weboldalt, amely G. Györgyöt, a becsült 174 milliárd forintos vagyonával 2014-2015. évek között Magyarország leggazdagabb emberévé tette.)[154] A forgalmazás terén 1999-re már több, mint 10.000 játékfilm állt rendelkezésre, amely a video-kölcsönzés és értékesítés üzleti tevékenységének mintegy 14 százalékát, valamint a piacon szereplő fizetős videohirdetés több mint felét kitette. Az adathordozók fejlődésének köszönhetően a DVD megjelenések évente körülbelül újabb 4 millió dollárral növelték a büdzsét, 2009-re pedig a mobiltelefon által megosztott felnőtt tartalom éves szinten 2,1 millió dollárt hozott.[155],[156] A számok, és a profit pedig napról napra emelkedik. Mára a felmérések azt mutatják, hogy másodpercenként 28.258 felhasználó néz pornográf anyagokat az interneten, ami a szolgáltatóknak ugyan ennyi másodpercenként 3075,64 dollár bevételt jelent. Az internetet használó minden második felhasználó a keresőprogramokban „felnőtt" tartalmú anyagokra keres rá, a keresőmotoros lekérdezések 25 százaléka pedig pornográfiával kapcsolatos. Ez csak a pornográfia kategóriájában napi 68 milliós keresési találatot eredményez. A találatok letöltésének 35 százaléka pornográf anyag. Ezek a statisztikai számadatok nem is kapnának túlzott jelentőséget, amennyiben a keresések napi szinten átlagosan ne 116.000 gyermekpornográfiával kapcsolatos keresési találatról adnának számot.[157]

A gyermekpornográfiával kapcsolatos bűncselekmények elkövetőinek többsége a gyűjteményének fenntartására, növelésére, és megosztására számítógépes technológiát alkalmaz. A digitális fényképezőgépek, és videókamerák, a mobiltelefonok egytől egyig megkönnyítették az életüket azoknak a bántalmazóknak, akik bűnözői magatartásukat a magánjellegű szórakoztatás, vagy a kereskedelmi haszon érdekében szeretnék tanúsítani.[158] Az internethez kapcsolt kamerás mobiltelefonok könnyen felhasználhatók a pornográf anyagok határokon átívelő küldésére, és fogadására. Nagyon sok ilyen, vagy ehhez kapcsolódó weboldal, ami gyermekek pornográfiájával kapcsolatos anyagokat oszt meg, és a

[154] SZAKONYI Péter: A 100 leggazdagabb magyar 2015. – Budapest: Online Kft, 2015.

[155] EGAN Timothy: Technology sent Wall Street into market for pornography. - New York: Routledge, 2000.

[156] HOLDEN William: Mobile to adult: Personal services. – United Kingdom: Juniper Research, 2000.

[157] FAGAN Patrick: Internet pornography by the numbers; a significant threat to society. – Broomfield: Webroot Cyber Security, 2009.

[158] ALLEN Ernie: Child Pornography: Model Legislation & Global Review. – United States: International Centre for Missing & Exploited Children, 2013.

világ különböző tájaira szortíroz Kelet-Európából származik, és szervezett bűnözői csoportokhoz köthető.[159] A gyermekek személyesen gyártott szexuális töltetű, illegális képei, hang-, és videóanyagai különösen értékesek az internet világában, és míg a bűnözők részére a kereskedelem milliós profitot termel, addig a kibertérben fellelhető, újratermelődő gyermekpornográf anyagok, a gyermekek életében helyrehozhatatlan, és örökké tartó lelki-, és testi bántalmakat keletkeztetnek. A gyermekpornográfia bűncselekményével kapcsolatos tudományos problémát az alábbiakban látom: a kibertérben, és a valóságban elkövetett gyermekpornográfia globális méreteket öltött, ezért az ellene irányuló fellépésnek (kormányzati-, bűnüldözői-, magánszektori-, szociális környezeti együttműködésnek) is világméretűnek kell lennie. A gyermekek szexuális kizsákmányolásának különböző formáitól egyetlen ország sem mentes, azonban a probléma mértékét és súlyosságát a különböző államok különböző módon, és legfőképpen egyenlőtlenül kezelik. Léteznek olyan országok, amelyek a kérdéssel egyáltalán nem-, vagy csak részben foglalkoznak, ám vannak olyanok is, akik a gyermekek szexuális kizsákmányolása elleni harc éllovasai. Minden államnak kötelessége, hogy kormányaik, bűnüldöző szerveik, valamint a civil társadalmuk összehangolt intézkedéseket tegyen annak érdekében, hogy a világ gyermekeinek védelmét biztosítsa. A gyermekpornográfia széles körű értelmezése magában foglalja a gyermekek szexuális bántalmazását, és kizsákmányolását, amely a gyermekprostitúcióhoz, a gyermekek szexuális célú kereskedelméhez is kapcsolódik. A gyermekek egészségi állapota, általános jóléte, szellemi/erkölcsi fejlődése kerül veszélybe, ezért a szexuális kizsákmányolás nem maradhat büntetlenül. A kérdés kezelésében a normatív, intézményi, és politikai eszközök sokat segítenek.

Mindamellett, hogy a tanulmány Magyarország gyermekvédelmével kapcsolatos modelljogára vonatkozó jogalkotási-, és alkalmazási folyamatait kritikával nem illeti, megpróbál a probléma aktuális állapotáról tudósítani, és javaslatokat tenni. A gyermekekkel kapcsolatos pornográf-, és a szexuális kizsákmányolással érintett bűncselekmények európai viszonylatának tekintetében Magyarország bűnüldöző szerveinek tevékenysége fokozásra-, az államok közötti kollaboráció, és párbeszéd javításra szorul. Hiányzik egy olyan eredményes, komplex makro-, és mikro szinten kidolgozott bűnüldöző stratégia, amely a látenciába burkolódzó jelenség feltérképezésére, a bűncselekmények megelőzésére, és az elkövetők

[159] PETIT Miguel Juan: Rights of the Child. – United Nations: Economic and Social Council, 2004.

elfogására a nemzetközi joganyag hazai harmonizációjával összhangban intézkedik. Magyarország sem teljes mértékben alkalmazkodik a nemzetközi joghoz, így annak harmonizációja felülvizsgálatra szorul. Álláspontom szerint e bűncselekmények elleni fellépés nélkülözhetetlen elemei az internet-, és távközlési szolgáltatók (, mint a kritikus infrastruktúra általános fogalma alá eső informatikai rendszerek, létesítmények, hálózatok) összességének formális-, és informális tevékenységei, amelyek Magyarország Nemzeti Kiberbiztonsági Stratégiájában kiemelt pozíciót tölthetnének be, biztosítva ezzel a veszélyeztetettség, és fenyegetettség, a globális kihívás mértékét.[160],[161],[162]

1.2 Célok

A társadalomban élők a közszolgálat és az általa nyújtott szolgáltatások színvonala iránt egyre magasabb követelményeket támasztanak, amelyeket az egyre szűkösebb költségvetési forrásokból, a hagyományos, korábban eredményes munkamódszerekkel, szervezeti kultúrával és alkalmazott hozzáállással már egyre nehezebben lehet megvalósítani. A felgyorsult világnak köszönhetően a közszolgálatnak is állandó változásban kell lennie, ha a globalizáció pozitív hatásait követni, az ebből adódó kihívásokat pedig leküzdeni szeretné. A gazdasági-, politikai körülmények, és társadalmi igények a közszolgálati, és rendvédelmi szerveket tevékenységük minőségének fejlesztésére késztetik. Ahhoz, hogy a közszolgálat ezeknek a körülményeknek megfelelni tudjon nemcsak naprakész, hanem alkalmazott tudásra, rendszerezett és értékelt ismeretanyagokra, módszerekre és megoldásokra van szüksége. Ezt a tudást egyrészt a nemzetközi színtéren rendelkezésre álló ismeretek és tapasztalatok, hazai adoptációján-, másrészt pedig a hazai-, a közszolgálati szervek tevékenységét megalapozó és azt fejleszteni képes tudásbázis kiépítésén keresztül abszolválhatja.

A pályázati munka a fentiek figyelembevételével három célt (általános, stratégiai, funkcionális) különböztet meg. A tanulmány elkészítésének általános célja, hogy a 2012. és 2016.

---

[160] KOVÁCS László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. – Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[161] A Kormány 1139/2013. (III. 21.) Korm. határozata - Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. (http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf) (hatályba lépett: 2013. március 22-én) (letöltés ideje: 2017. augusztus 05.)

[162] A tanulmány témaköre így illeszkedik a pályázatot kiíró kritikus információs infrastruktúra témajavaslatainak 2. pontban foglalt tárgyköréhez.

közötti időszak elemzésén keresztül egy olyan kutatómunkán alapuló információs adatbázist hozzon létre, amely a gyermekek szexuális kizsákmányolásán alapuló gyermekpornográfia bűncselekmény elleni küzdelem hazai rendvédelmi erőfeszítéseiről reális képet mutat, a kidolgozott javaslatok megvalósíthatóságának – relevanciájának, fenntarthatóságának, megalapozottságának, életképességének - tekintetében pedig a fellebbviteli szerv döntési mechanizmusát segíthesse. A dolgozat középtávú, koncentráló stratégiai célja egy olyan komplex mikro-, és makro szinten alkalmazható intézményesített rendszer kidolgozása, amely a gyermekek szexuális kizsákmányolásán alapuló gyermekpornográfia bűncselekményének tekintetében a rendőri intézkedéseket a bűnelkövetőkkel szemben eredményesebbé-, a rendőrség e kihívásokkal szembeni küzdelmét (az áldozatvédelem területén is) hatékonyabbá teheti. A funkcionális célt a kutatás-fejlesztés-innováció hármasán alapuló, az emberi-, és tárgyi erőforrásokat maximalizáló, logisztikai technológia színvonal emelése jelentette. A szexuális célú kizsákmányolással kapcsolatos bűncselekmények felderítésének tekintetében, az eddigi viszonylag lassú technológiai színvonal-változást a kutatási eredmények fejlesztésre késztethetik, amely a nemzetközi színtéren kamatoztató, horizontális, a jogi-, természeti akadályokat leküzdő, korszerű bűnüldözés lehetőségét teremtheti meg.

1.3 Hipotézisek

A tanulmány elkészítésekor az alábbi elméleti hipotézisekből indultam ki:

1. Feltételezem, hogy a vizsgált időszakban, a vizsgált kategóriákban az összes elrendelt büntetőeljáráshoz viszonyítva a Büntető Törvénykönyv nemi élet szabadsága, és a nemi erkölcs elleni bűncselekmények fejezetében elrendelt büntetőeljárások alacsony százalékos számértéket képviselnek, azonban a fentiek ellenére a gyermekpornográfiával érintett bűncselekmények e fejezetben kimagaslóan (szignifikáns) magas százalékos arányról adnak tanúbizonyosságot. A gyermekek szexuális kizsákmányolásán alapuló gyermekpornográfia bűncselekmény tekintetében a nyomozások fele zárul csupán eredményesen (különös tekintettel a vádemelési javaslatokra), az a nemzetközi arányszámokhoz viszonyítva is csekély százalékú. A magyar rendvédelmi erők arányszámaiban kevés bűncselekményt derítenek fel, a nemzetközi felderítés és együttműködés a nyomozások felderítését befolyásolja. A fentiek eredményezhetik, hogy a magyar rendvédelmi erők a nemzetközi kötelezettségvállalásban, a gyermekpornográfia elleni küzdelemben az elsők között nem szerepelhetnek.
2. Feltételezem, hogy Magyarországon a legtöbb büntetőeljárást, és a legtöbb sértettet a gazdaságilag elmaradott, és társadalmi mélyszegénységgel sújtott régióiban regisztrálják, a sértettek száma, és a büntetőeljárások elrendelése évről évre emelkedő tendenciát mutat. Feltételezem, hogy Budapesten sokkal kevesebb elrendelés történik, mint e régiókban. Feltételezem, hogy a nemzetközi fiú-lány sértetti százalékos arányszám a nemzeti arányszámokkal korrelál. Feltételezem, hogy Magyarországon (is) a gyermekpornográfia által legveszélyeztetettebb korosztály a gyermekkorú korosztály, azon belül is a kislányok a

legfenyegetettebbek. Feltételezem, hogy a háttérben megbúvó okok, célok és indítékok feltérképezhetők, mérsékelhetők, és egy jól felépített áldozatvédelmi stratégiával megszüntethetők. Feltételezem továbbá, hogy a hipotézisben foglaltak vizsgálata az inkriminált időszak magyar eredményes büntetőeljárásai tekintetében a korrelációs együtthatók lineáris szorosságával mérhetők.

3. Feltételezem továbbá, hogy a rendvédelmi szervek tekintetében egy olyan intézményesített rendszeren alapuló, és a gyermekek szexuális kizsákmányolásával kapcsolatos gyermekpornográfia bűncselekmények felderítését elősegítő stratégiai koncepció dolgozható ki, amely Magyarországot a nemzetközi viszonylat élvonalába sorolja. Feltételezem, hogy a megfelelő minőségű bűnüldözői munka, valamint a sértettek számára elérhető áldozatvédelmi tevékenység maximalizálása az eredményeket nagymértékben pozitív irányban befolyásolja, a látencia mértékét látványosan csökkenti.

1.4 Tudományos módszertan

A tanulmány az iOCTA, és az INHOPE, valamint a magyar rendvédelem 2012-2016. időszakból származó értékelésén alapuló gyermekek szexuális kizsákmányolásával kapcsolatos gyermekpornográfia bűncselekmények eljárásaival foglalkozik. A téma szenzitív volta, valamint az azt körülvevő erős látencia övezte jelenség kutatására célszerűnek tartottam több olyan eltérő, de mégis összetett kutatási módszert alkalmazni, ami reményeim szerint a rendőri intézkedések végrehajtásának mind elméleti-, mind pedig gyakorlati oldalának fejlesztéséhez iránymutatásul szolgál, és új tudományos eredmények létrejöttéhez segíthet hozzá.

Az első fejezetekben történelmi alapkutatást végeztem, amelynek során primer-, és szekunder forráselemzést hajtottam végre. Az adatgyűjtő tevékenység a pornográfiával, a gyermekek szexuális kizsákmányolásával, különös tekintettel a gyermekpornográfiával kapcsolatos levéltári kutatást, az írt, fennmaradt rendeletek, intézkedések, parancsok, jelentések, rendőri jegyzőkönyvek, publikált tanulmányok feldolgozását jelentette. Tekintettel arra, hogy a témában kevés magyar nyelvű szakirodalom állt rendelkezése, ezért (köszönetet mondva az általam látogatott és sok segítséget nyújtó könyvtáraknak) azokat angol-, és német nyelvű monográfiákkal egészíthettem ki. Az iOCTA, és INHOPE jelentések, valamint a nemzetközi anyagok (különösen az uniós jegyzőkönyvek) angol-, és német nyelven voltak csak elérhetők, ezáltal a nemzetközi színtér vizsgálatára is lehetőség adódott.

Az első fejezeteket követően az alapkutatást olyan alkalmazott kutatás váltotta fel, amely a témában megismert eredmények hasznosítási lehetőségeinek felhasználását elősegíti, a gyakorlati megvalósítás során felmerült problémák megoldásához pedig iránymutató jelleggel segítséget nyújt. Az alkalmazott kutatás döntő többségben a témával kapcsolatos

országhatáron belüli-, és azon átnyúló gyermekpornográfia elleni rendőri feladatok teljesítésének gyakorlatával függött össze. Ellentétben az alapkutatással, az alkalmazott kutatás a funkcionáló, középtávú stratégiai célommal parallel képes a bekövetkezett változásokra gyorsabban reagálni, folyamatos alkalmazása a közvetlen gyakorlati szükségleteket kielégíteni, és többnyire rövid időn belül alkalmazható eredményeket produkálni. (Az alkalmazott kutatás felhasználása a rend-, és honvédelmi eröknél jellegüknél fogva előnyös.)[163] Kiemelt jelentősége abban rejlik, hogy a felgyorsult világnak köszönhetően az elkövetői hálózatok a bűncselekmények elkövetéséhez napról-napra egyre fejlettebb technológiákat használnak, amelyek ellen a rendőrségnek fele ennyi idő alatt, még fejlettebb humán-, és tárgyi erőforrások bevetésére van szüksége ahhoz, hogy a bűncselekményeket megelőzhessék, és megakadályozhassák, megteremtve ezzel a bűnözőkkel szembeni lépéselőnyt. Az erre a célra szakosodott bűnözők, így önmagában a szervezett bűnözés dinamizmusa, rugalmassága a politikával és szervezeteivel szemben egyelőre egyértelmű előnyt biztosít.[164] (Az alábbi logikai összefüggést, miszerint az elkövetők elleni harc akkor lehet csak sikeres, ha a bűnüldöző hatóságok ugyanahhoz a leleményességhez, innovációhoz, szervezeti rugalmassághoz, és együttműködéshez, amelyek a bűnszervezeteket jellemzik asszimilálódnak már 1995-ben Naylor feltárta.)[165]

A tanulmány kutatási metódusának elméleti szakasza absztraktálható, logikai erő-felhasználást követelt meg. Az analízis és szintézis dialektikus felhasználása segítségemre volt abban, hogy a vizsgált témakört gondolati részekre bonthassam (szétválasztva lényeges tulajdonságaikat, strukturális elemeiket, és egyes kapcsolataikat), majd minden egyes részt – felépítés, és funkcionalitás alapján - az egészhez való viszonyulása alapján feltérképezhessem. Ezt egészítette ki az összehasonlítás módszertana, amely a vizsgálat tárgyáról számos ítéletet feltételezett, ezek egymással szorosan összefüggtek, az ismereteket pedig a keletkezett rendszeren belül az azonosság, a hasonlóság, a különbség, és az össze nem vethetőség szempontja választotta szét.

---

[163] GŐCZE István: A tudományos kutatás módszerei. In: Hadtudományi Szemle, 2011., 4. évf. 3. sz. – p.:157-166.

[164] FINCKENAUER James, VORONIN Yuri: The Threat of Russian Organized Crime. – Rockville: National Institute of Justice, Issues in International Crime, 2001.

[165] NAYLOR Thomas: From cold war to crime war. In: Transnational Organized Crime,1995., 1. évf. 4. sz. – p.:37-56.

A rendelkezésre álló statisztikai számadatokat pedig olyan kvantitatív eljárás keretén belül vizsgáltam, amely különböző függvények beágyazásával képes a minimum, maximum, átlag, módusz, és szórás számítások eredményeinek kimutatására. Az alapstatisztikai számítások alapján kapott eredményeket pedig olyan összehasonlító kvantitatív eljárás fogta össze, amely a gyakoriságok közötti korrelációs koefficiens értékét a Cohan féle általános skálán illusztrálni tudta.

Mivel a választott téma nagyon összetett jelenség, és komplex megértéséhez minden egyes elem részletes vizsgálata szükségeltetik, ezért tartom kiemelten fontosnak, hogy minden kutató a saját részével az egész megértéséhez hozzájáruljon.[166] Minden jelenség – így a gyermekek szexuális kizsákmányolása, a gyermekpornográfia is - egy olyan kirakósként értelmezhető, aminek a darabjai egymástól elkülönülten helyezkednek el, és csak akkor adják ki a kép teljes egészét, ha azokat összeillesztjük. Örömmel töltene el, ha olyan új tudományos eredmények jöhetnének létre, amelyek ennek a kirakósnak egy újabb darabját szolgáltathatnák.

1.5 A tanulmány felépítése

A tanulmány négy fejezetből áll. Az első fejezet a tudományos problémát, a kutatási célokat, a hipotéziseket, a módszertant, valamint a dolgozat szerkezeti felépítést tartalmazza. A második fejezet a pornográfia, és a szexuális kizsákmányolással érintett gyermekpornográfia bűncselekmények jelenségét dolgozza fel, különös tekintettel a fogalmára, rétegződésére, és a az idősík terminológiájára. A harmadik fejezet nemzetközi kitekintést tartalmaz, ahol az INHOPE, és a iOCTA szervezetek és értékeléseik elemzése valósult meg. A negyedik fejezet a saját kutatást tartalmazza, az eredményeket, és azok megvitatását, majd a javaslatokat ölelik fel.

[166] KOVÁCS István: Gésa kultúra, és japán prostitúció. In: Hadtudományi Szemle, 2017., 10. évf. 2. sz. – p.:447-464.

2. Pornográfia

2.1 A pornográfia fogalma

A szexualitás minden ember számára életének meghatározó jelensége, vezérelje azt akár a fajfenntartás biológiai ösztöne, vagy csupán a szexuális vágy élvezeti kielégítése. Sok szempontból lehetne ezt firtatni, de akár tetszik, akár nem, számadatok ide, vagy oda, mindannyian szexuális lények vagyunk, a biológiai szükségleteink kielégítése mindannyiunk Maslow piramisának szükségszerű eleme.[167] Sok ember számára a biológiai szükséglet-kielégítés, a szexuális kapcsolatok, az integrális szexuális tevékenység prominens jelentőségű, történjen az akár négy fal között édeskettesben, vagy azon kívül, akár több, aktív, vagy passzív résztvevővel. El kell fogadnunk, hogy egyes férfiak, és nők esetében a pornográfia fogyasztása, vagy előállítása szexuális életük részét képezi, vagy azt fokozza. Az embernek szüksége van arra, hogy felfedezze önmagát, megkapja a választ arra, hogy kicsoda, és mire képes.[168] A pornográfia termelése, fogyasztása, a részvétel tapasztalata, a kísérletezés mind-mind hozzájárulhat ahhoz, hogy az egyéniségünk, különösen az (egészséges) szexualitásunk fejlődhessen. Érdemes viszont elgondolkodnunk azon, hogy ez a kísérletezés milyen határok között minősül egészségesnek, és mi az a választóvonal, ami akár még önmagunk személyiségének, szexuális kultúrájának a fejlesztését is korlátozhatja. Meg kell tudnunk, hogy mit nevezünk egyáltalán pornográfiának, hogyan definiálhatjuk, és valójában hogy hat a személyiségünkre, miért kezeli akár a jog-, akár az erkölcs olykor-olykor prohibíció tárgyaként. Mielőtt a pornográfia definiálására rátérnék, Smith [1971] szavaival élve, érdemes megfontolnunk azt, hogy a pornográfia fogalommeghatározáskor mennyire voltunk előítéletesek. Ugyanis egy olyan jelenség, amely egyébként is sztereotípiára épül, nem felelhet meg a definícióalkotás alapkövetelményeinek, mert ebből kifolyólag az egységes meghatározás egyrészt a fontos körülményeket nem tartalmazná, másrészt pedig nem zárná ki az összes olyan körülményt, amely a fogalommeghatározás szempontjából nem releváns.[169] Az alábbiakat egy egyszerű példán keresztül kívánom illusztrálni: az ős-, és ókorban a tűz

[167] MASLOW Abraham: Motivation and Personality. – New York: Harper, 1954.

[168] FREDERICK Danny: Pornography and Freedom. In: Kritike, 2011., 5. évf. 2. sz. – p.: 84-95.

[169] SMITH Dwight: Some Things that may be more important to understand about Organized Crime than Cosa Nostra. In: University of Florida Lax Review, 1971., 24. sz. – p.: 1-30.

jelenségét természetfeletti magyarázatok, mint például Isten haragja, vagy teremtett csoda aposztrofálta. Ma már tudjuk, hogy a tűz keletkezése, ha nem is egy csoda természeti megnyilvánulása, de egy kémiai folyamat - a gyors oxidáció - része. Tűz a kandallóban, kályhában, vagy akár a tűzhelyen olyan ellenőrzött, és profitáló szolgáltatás, amit az emberek kellemesnek, és hasznosnak éreznek. De, ha ez a tűz, ellenőrizetlen keretek között a házban, vagy a természetben elterjed, akkor környezetünkben félelmetes pusztulást képes okozni. Így van ez a pornográfiával is. Először az szükséges, hogy a jelenséget megértsük, meg kell tudnunk, hogy mivel állunk szemben, hiszen, ha nem akarjuk megérteni, nem törődünk vele, sikeresen szocializálni sem tudjuk.[170] Romboló hatású, vagy egészséges? Választ kell találnunk arra a kérdésre, hogy önmagában a pornográfia kifejezés szóhasználata nem megfelelő, vagy azt csupán a hibás ítélőképesség terelte olyan negatív irányba, hogy az az emberekben megbotránkoztatást keltett, bizonyos jogterületeken pedig a jogalkotó reglementációs-, és egyenes prohibíciós intézkedések bevezetését látta szükségesnek.[171]

A szexuális aktusok emberközeli ábrázolása nem újdonság. Számos az ókori Görögországból és Rómából, valamint más ázsiai, afrikai és európai kultúrákból származó erotikus művészetet ábrázoló anyagokat régészek fedeztek fel.[172],[173] Például az időszámításunk utáni 2-3. századbeli Indiából származó Kámaszútra a világ minden táján ismert könyv, amely a különböző szexuális aktusokat, és gyakorlatokat vázolja fel, de ugyanakkor tudomásunk van olyan művészeti, irodalmi alkotásokról is, amelyek a viktoriánus Anglia termékei.[174],[175] Bár a tanulmányban megpróbálok minden idősíkot figyelembe venni, és a definíciót a legmesszemenőbbekig részletezni, a fogalommeghatározást mégis egy az 1960-as évekből fennmaradt nemzetközi eljárás elhíresült „anekdotájával" kezdem. Hogy

---

[170] CALDERONE Mary: Pornography as a public Health Problem. In: American Journal of Public Health, 1972., 62. évf. 3. sz. – p.: 374-376.

[171] Például lásd a korhatár-besorolás szabályozását, vagy a büntetőnorma a szexuális visszaélés forgalmazásának, készítésének, sokszorosításának tilalmát.

[172] SIGEL Lisa: Governing pleasures: Pornography and social change in England, 1815–1914. – Piscataway: Rutgers University Press, 2002.

[173] FERGUSON Christopher, HARTLEY Richard: The pleasure is momentary the expense damnable? The influence of pornography on rape and sexual assault. In: HASSELT van Vincent (szerk.): Aggression and Violent Behaviour, 2009., 14. évf. 5. szám – p.: 323-329.

[174] GLADFELDER Hal: Literature and Pornography 1660–1800. – United Kingdom: Oxford Handbooks, 2013.

[175] VATSZJAJANA Mallanaga: Kámaszútra. – Budapest: Librotrade Kft, 2002.

milyen nehéz is a pornográfia definiálása azt Potter Stewart bíró is jól tudta, amikor 1964-ben a „Jacobellis vs. Ohio” ügyben az ítélet indoklását felolvasta. Minden jogi „csűrcsavar” nélkül a pornográfiáról csak annyit mondott: „Tudom, ha látom.”[176] Hogy mi egy picit többet tudjunk a fogalomról, és ne csak akkor, mikor látjuk, megpróbálkozom a napvilágot látott definíciók elemzésére, majd saját fogalom meghatározására.

Mindenekelőtt annak tisztázása szükséges, hogy a pornográfia művészet, vagy önálló szakterület. Köze van-e annak az erotikához, ugyan az a fogalom-e, csak más aspektusban, esetleg teljesen különbözik attól. Nehéz feladatnak bizonyul a téma teljes körű megértése, és nem is csodálkozunk, mikor a tudományterületek képviselői a definiálás nehézségeivel találják szembe magukat. A különböző diszciplinák művelői között egyedül abban van egyetértés, hogy a fogalomnak nincs egységes, és mindenki által elfogadott definíciója.[177],[178],[179] A Magyar Katolikus Lexikon értelmezésében a pornográfia a görög eredetű „porneia”, azaz paráznaság, és a szintén görög eredetű „grafia”, mint leírás szavakból tevődik össze. Az erotika ugyan ezen lexikon vonatkozásában a görög eredetű „Erósz” istenség nevéből származik, jelentése „kívánni”.[180] Amikor az emberi történelem számos tárgyára, így különösen az itáliai freskókra, vagy a spanyol szobrokra, esetleg az NDK-s filmekre, és az angol irodalomra gondolunk, az emberi szóhasználat, és gondolatmenet

---

[176] Jacobellis vs. Ohio, 378 U.S. 184, 197 (1964): az Egyesült Államok Legfelsőbb Bíróságának döntése, amelyet 1964-ben hoztak arról, hogy Ohio állam - az első módosítással összhangban - tiltja-e a Louis Malle The Lovers (Les Amants) filmjének vetítését. Bár számos szakértő, jogtudós, és jogalkalmazó vett részt a tárgyalásokon, mégis azt Potter bíró szavai tették híressé, amikor a „kemény pornográfia” definiálásával próbálkozott. Az eredeti (bővített) mondat, szövegkörnyezetében így hangzott: "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that." Magyar fordításban: Nem ma lesz a napja annak, hogy tovább próbálom meghatározni azokat a fajtájú anyagokat, amelyek e rövid meghatározásba beletartoznak, és talán soha nem sikerül majd azt értelmesen megtenni, de tudom, amikor látom, és ebben a filmben az érintett mozgókép nem az.”

[177] CAMERON Samul: Economics of pornography. In: BOWMAKER Simon (szerk.): Economics Uncut: A Complete Guide to Life, Death, and Misadventure. Cheltenham: Edward Elgar Publishing, 2005.

[178] REA Michael: What is pornography? In: Noûs, 2001., 35. év., 1. sz. – p.: 118-145.

[179] SLADE Joseph: Pornography and Sexual Repression: A Reference Guide, Westport: Greenwood Press, 2001.

[180] DIÓS István, VICZIÁN János: Magyar Katolikus Lexikon I. – Budapest: Szent István Társulat, 2004.

valamiért azt mindig a pornográfiával köti össze.[181],[182],[183] És, ha már e dolgokat pornográfiaként írják le, általában azokra az erotikus szóhasználatot kerülik. Ez logikailag arra enged következtetni, hogy a két fogalom nem kontinuum, hanem koncepció tekintetében különbözik egymástól. A síkok közötti mozgás nehézsége abban rejlik, hogy az erkölcsi, vagy művészi érzelmek bármilyen elismerése, és fogadtatása szükségszerűen a társadalmi értékekhez, és értékrendhez kötődik. Ezért helyes az a megállapítás, hogy a pornográf anyag kulturális, vagy szubkulturális megítélése inkább kulturális, vagy szubkulturális értékeket, és normákat azonosít, mint pornográfiat vagy erotikát.[184],[185] A társadalom értékítélete, kultúrája, és szubkultúrája (különös tekintettel a moralista, feminista, és liberális irányzatokra) a fogalom alakulására igen jelentős hatást gyakorolt.[186]

2.1.1 A moralista értékrend

A moralista álláspont szerint a szexuális kapcsolat két felnőtt házas ember privát szférájának része, amely elsődlegesen a gyermekáldás célját szolgálja. A pornográfia (írásban, audiovizuálisan) arra készteti a nézőt, vagy az olvasót, hogy olyan szexuális kapcsolatokat folytasson, amely a hagyományos szabványokat megsértik.[187] [Eck (2001) az írásos, és audiovizuális pornográfia négy lényeges területét határozta meg: művészet, mint az irodalomban, a vizuális előadóművészetek, vagy az elektronikus művészetek, a szándékos pornográfia/erotika (mindkettő elektronikus, fényképészeti vagy irodalom alapú), az orvosi

[181] Itt kifejezetten azon művek értendők, amelyeknek szexuális töltöttsége van.

[182] KENDRICK Walter: The Secret Museum: Pornography in Modern Culture, Berkeley: University of California Press, 1987.

[183] ATTWOOD Feona: Reading porn: The paradigm shift in pornography research. In: Sexualities, 2002., 5. évf. 1. sz. – p.:91-105

[184] KIPNIS Laura: Bound and Gagged: Pornography and the Politics of Fantasy in America, Durham: Duke University Press, 1999.

[185] LUMBY Chatarine: Bad Girls: The Media, Sex and Feminism in the '90s. Australia: Allen and Unwin, 1997.

[186] Gondoljunk abba bele, hogy a lorno (light porno) műfaja, amely a férfi nemiszerv vaginális-, és anális közösülését „tiltja” a feminista irányzat szerint ugyan olyan morális, és negatív értékítélet alá esik, mint például egy szado-mazo elemekkel gazdagított pornofilm. De ugyan ilyen példa egy 1900-as években forgatott „pornofilm” is, amely a mai értékrend szerint még egy erotikus tartalommal rendelkező művészfilmnek se felel meg.

[187] KRONHAUSEN Eberhard, KRONHAUSEN Philips: The Psychology of Pornography. In: ARBARBANEL Aliza (szerk.): The Encyclopedia of Sexual Behavior. – New York: Hawthorn, 1967.

szövegek, és a pornográfia, mint marketingtevékenység. A területek közötti határok gyakran elmosódnak, az egyén számára nehézséget okoz, hogy azokat osztályozza. A társadalmi szocializációs folyamatok az osztályozás tevékenységére nagy befolyással bírnak.][188] A pornográfiát ezért a moralista ideológia képviselői sértőnek, és obszcénnek tartják, amely a társadalom tagjaira negatív hatást gyakorol. Rea [2001] szerint a pornográfia egy olyan kommunikációs anyag, amely ugyan a felhasználó szexuális vágyát felkelti, azt a felhasználó élvezi, viszont nem két ember intimitásának tárgyaként kezeli. Az alkotó az árucikket racionálisan úgy gyártja, hogy az a közönség szexuális örömét, vagy kielégítését szolgálja.[189] Az intimitás a fogalom egyik lényeges eleme. Az intimitás teremti meg két ember között a hagyományokon alapuló szexuális kapcsolatot, amennyiben a pornográfiát - akár egyedül, akár másokkal együtt - nézünk, annak a varázsa eltűnik. Rolph [1961] a jelenséget a „magányos elbájolás" képességének nevezte.[190] Ez a meghatározás összhangban van Soble [1985], Narveson [1993] és Olen, Barry és Van Camp [2005] által közvetítettekkel.[191],[192],[193] Más szerzők a fogalom meghatározásakor a morális értékrend erőteljesebb felvonultatásával szereznek érvényt maguknak: a pornográfia kizárólag anyagi profitszerzésre motivál, hiányoznak belőle a művészi értékek, az csak a szexuális objektivációról szól, egyenest degradáló.[194],[195],[196] A szexuális aktusok nyilvános megjelenítésével a pornográfia az embereket arra ösztönzi, hogy a privát szféra határain kívül is éljenek házaséletet, a fogyasztók szexuális vágyát olyan módon, és mértékben keltse fel, amely társadalmi keretek

---

[188] ECK Beth: Nudity and framing: Classifying art, pornography, information, and ambiguity. In: Sociological Forum, 2001., 16. évf. 4. sz. – p.: 603-632

[189] REA Michael: What is pornography? In: Noûs, 2001., 35. év., 1. sz. – p.: 118-145.

[190] ROLPH Harris: Does Pornography Matter? – London: Routledge and Kegan Paul, 1961.

[191] SOBLE ALAN: Pornography, defamation, and the endorsement of degradation. In: Social Theory and Practice, 1985., 11. évf. –p.: 61-87

[192] NARVESON Jan: Moral Matters. – Ontario: Broadview Press, 1993.

[193] OLEN Jeffrey et al.: Applying Ethics: A Text with Readings. – Belmont: Wadsworth Publishing Company, 2005.

[194] HUER Jon: Art, Beauty, and Pornography: A Journey Through American Culture. - Buffalo: Prometheus Books, 1987.

[195] BERGER Fred: Pornography, sex, and censorship. In: Social Theory and Practice, 1977., 4. évf. – p.: 183-209

[196] MCELROY Wendy: A Woman's Right to Pornography. – New York: St. Martin's Press, New York, 1995.

között elfogadhatatlan. A pornográfia pozitív üzenetet közvetít a házasságtörésről, a homoszexualitásról, sérti a nemi élet privát szférájához fűződő jogot, aláássa a moralista értékrendet, különösen a hagyományos családi struktúrát. Bizonyos kutatások beszámoltak arról, hogy az alapvető társadalmi értékek generális csökkenése kapcsolatban áll a pornográfia felhasználásával.[197],[198] A moralista értékrend szerint a pornográfiával kapcsolatos kockázatok öt kategóriába sorolhatók: a pornográfia hajlamos a morális értékrend elpusztítására, és az emberek megrontására. A pornográfia a hagyományos értékrenden alapuló szexuális kapcsolat résztvevőiből rabszolgákat alakít. Káros a fogyasztókra, leginkább a gyermekekre. A pornográfia közvetett módon bűncselekmények elkövetésére is felhív. Sérti a polgári, és szabadságjogokat.[199] Összegzésképpen megállapítható, hogy a moralista perspektíva a pornográfia magánszemélyekre, és a társadalmi struktúrákra gyakorolt negatív hatásokra összpontosít. Míg a negatív hatásokat felsorakoztatja, addig annak pozitív eredményeiről nem rendelkezik. Egyoldalúsága is ebben rejlik, amely a fogalomalkotás alapját – negatív, pejoratív értékítéletének köszönhetően – nem adhatja.

2.1.2 A liberális értékrend

A liberális perspektíva szerint a társadalmat alkotó egyéneket nem korlátozza senki, és szabadon dönthetnek arról, hogy a kultúrájukban mi a megfelelő, és elvárható viselkedés, a morális értékrendet racionális választások sorozata határozza meg. A liberalista felfogás olyan politikai teoretikusok gondolataira épül, mint Locke [1632-1704] és Mill [1806-1873], akik szerint az egyéneknek alapvető joguk van ahhoz, hogy véleményeiket, eszméiket szabadon kifejthessék, gyakorolhassák. Az állam csak akkor avatkozhat be, és korlátozhatja az alapvető jogok gyakorlását, ha a személyek cselekedetei, más emberek alapvető jogait sértik, vagy veszélyeztetik. Az emberi értékeknek, az egyének jogainak, és magánéletének, valamint a nemi életnek a társadalom fenntartásában, és stabilitásában, valamint a status quo-ban jelentkező szerepével összhangban az állam csak akkor-, és csak olyan minőségben hozhat

[197] ZILMANN Dolf, BRYANT Jennings: Effects of prolonged consumption of pornography on family values. In: Journal of Family Issues, 9. évf. – p.: 518-544.

[198] ZILMANN Dolf, BRYANT Jennings: Pornography, sexual callousness, and the trivialization of rape. In: Journal of Communication, 32. évf. – p.: 10-21.

[199] FREDERICK Danny: Pornography and Freedom. In: Kritike, 2011., 5. évf. 2. sz. – p.: 84-95.

korlátozó intézkedéseket, ha az más alapvető jogokat sért vagy veszélyeztet. Szexuális kapcsolat létesítése a nők, és férfiak alapvető joga – még, ha azt pornográf anyag is ihlette -, ezért annak gátlása a korlátozás expresszionálásának felelne meg. A felnőtt embereknek teljes szabadságot kell kapniuk ahhoz, hogy a pornográfiával kapcsolatos örömüket, például szexuális fantáziájukat, szexuális ösztönzőiket a más beleegyező felnőttekkel való interakcióban használhassák.[200],[201],[202] A pornográfia végtére is egy fantáziavilág, amellyel a fogyasztók tisztában vannak. Vannak olyan emberek (bár számuk lényegesen alacsony), akik azért néznek pornot, vagy azért olvasnak erotikus könyveket, mert tudásra szomjaznak, ám a legtöbben azért teszik, mert ennek a fantázia-kalandnak a részesei akarnak lenni. Ebben a világban nincs információhiány, nincsenek aggodalmak, és a partnerek szabadon kommunikálhatnak a szexről. Wilson [1978] arról számolt be, hogy felméréseik azt igazolták, hogy a pornográfia sok férfi, és nő számára a szexuális gátlásaikat csökkentette, a személyek a partnereik tekintetében hajlandóak voltak új dolgokat kipróbálni, általánosságban a szexuális kapcsolatokat javították.[203] Azon államok tekintetében, akik pornográfiát alkotnak, egyben művészetet is alkotnak: a pornográfia nem más, mint az egyén pszichéjének a szexuális szükségletekkel való szembesülése.[204] Az egyetlen érzés, ami a pornográfia során megszűnik az a szenvedés, a szexuális feszültség pedig felszabadul.[205] A pornográfia az egyénnek segítséget nyújthat a szexuális konfliktusok enyhítésében, rendezésében, esetleges terápiás hatásai is lehetnek. Az egészséges pornográfiával kapcsolatban egy kutatás megállapította azt is, hogy a fiú csecsemők körülbelül 30 százaléka már egyéves korában vagy az előtt, és a férfiak gyakorlatilag 100 százaléka már 18 éves kora előtt átéli az orgazmust.[206] Valójában tehát a közegészségügyben minden szakember elismeri, hogy az

[200] MILL John Stuart: On Liberty. – London: Longman, Roberts and Green, 1869.

[201] LOCKE John: The second Treatise of civil Government. – England: Industrial Systems Research, 2009.

[202] MALAMUTH Neil: Pornography. In: KURTZ Lester (szerk.): Encyclopedia of Violence, Peace, & Conflict. – Amsterdam: Elsevier Inc., 2008.

[203] WILSON Cody: Can pornography contribute to the Prevention of Sexual Problems? In: QUALLS Brandon et al. (szerk.): The Precention of Sexual Disorders: Issues and Approaches. – New York: Plenum, 1978.

[204] MICHELSON Peter: The Aesthetics of Pornography. – New York: Herder and Herder, 1971.

[205] KRONHAUSEN Eberhard, KRONHAUSEN Philips: The Psychology of Pornography. In: ARBARBANEL Aliza (szerk.): The Encyclopedia of Sexual Behavior. – New York: Hawthorn, 1967.

[206] GAGNON John: Sexuality and Sexual Learning in the Child. In: GAGNON John (szerk.): Sexual Deviance. – New York: Harper and Row, 1967.

erotika az egyén pszichodinamikus fejlődésének elkerülhetetlen összetevője, a születéstől, egészen a halálig. Az egészséges szexualitás erotikus örömöt keres, a gyengédség, és a szeretet összefüggéseiben.[207] Ennek megfelelően a pornográfia nem lehet egy drámai eszköz a nők propagandista, és társadalmi tabukat tesztelő harcában, amely a nőkkel szemben alkalmazott agresszió, és erőszak eszméjét hirdeti.[208] Forráskritikát alkalmazva megállapítottam, hogy a liberális eszme mindamellett, hogy az állammal szemben a szabadság-, és emberi jogok gyakorlása iránt magas követelményeket támaszt, ugyan olyan mértékű korlátozó intézkedések bevezetését is szükségesnek látja. Mind a kötelmi-, mind pedig a jogosultság gyakorlásának oldalán arányos-, és szükségszerű elemek jelennek meg. A liberális perspektíva úgy foglalható össze, amely a pornográfiát, annak fogyasztását, előállítását, és forgalmazását alapvető emberi jognak tekinti, amely az emberi test biológiai szükségleteinek kielégítését szolgálja, számos előnyös hatása ismert. Annak korlátozása csak úgy valósulhat meg, ha az más alapvető emberi-, és szabadságjogot sért.

2.1.3 A feminista értékrend

A feminizmus képviselői [közöttük is kiemelkedően Dworkin, és MacKinnon (1988)] különösen szókimondók voltak e témában, mind a moralista (konzervatív), mind pedig a liberális eszméket vallókat megkérdőjelezték, azokat éles hangnemben bírálták. Az ideológia központjában a szex, mint hatalom összefüggés áll. A szexuális kapcsolat az elsődleges eszköz, amellyel a férfi a nőre hatni képes. Mivel ez a hatalom egyenlőtlenül került elosztásra, képes arra, hogy a nők magatartását szabályozza, és kényszerítse őket olyan tettek megtételére, amelyet igazából a férfi igényeinek kielégítése vezérel. A férfi a nőket a szexualizáción keresztül eszközként használja. A pornográfia a nők elleni erőszak eszköze, amelynek fő célja a nemi hovatartozáson alapuló dominancia érvényesítése, és a nők fizikai/lelki károsítása. A pornográfia mindezt az agresszióval teremti meg.[209] A nő a

[207] CALDERONE Mary: Pornography as a public Health Problem. In: American Journal of Public Health, 1972., 62. évf. 3. sz. – p.: 374-376.

[208] MALAMUTH Neil, BILLINGS Victoria: Why Pornography? Models of Functions and Effects. In: Journal of Communication, 1984., 34. évf. 3. sz. – p.: 117-129.

[209] DWORKIN Alice, MACKINNON Andrea: Pornography and civil rights. – Minneapolis: Organizing Against Pornography, 1988.

pornográfia hím szubjektumának reflektora, és alkotója.[210] Brownmiller [1975] szavaival élve a pornográfia, olyan férfi találmány, mint a nemi erőszak: a nők személyét dehumanizálja, megalázó, és erőszakos, a szexuális érzelemtől, a morális gátlásig a nők szexuális kapcsolatának kiteljesedését korlátozza.[211] Álláspontom szerint – forráskritika alkalmazásával – a feminista megközelítés egyoldalúnak tűnik. A világban nemcsak heteroszexuális, hanem homoszexuális pornográf anyagok is fellelhetők. Amennyiben azt vesszük alapul, hogy a pornográfia erőszakot szül, és kényszerítésre utaló cselekvést tartalmaz, úgy akkor az – kiindulva a homoszexuális pornográfiából – nem csak a nők, hanem a férfiak ellen is ugyanúgy irányul.[212],[213] (Ez a megállapítás nemcsak a pornográfiával, hanem generálisan a nők ellen irányuló erőszakos cselekményekkel kapcsolatban is megállapítható. Lásd például a prostitúció jelenséget. Nemcsak heteroszexuális női-, hanem heteroszexuális férfi-, sőt homoszexuális nő-, és férfi prostitúció is létezik. De alapul vehetjük a női dominanciát hirdető „bdsm" filmeket is, amely a feminista szemléletnek éles ellentéte.)[214] Bár bizonyítható, hogy a pornográfia bizonyos területei lealacsonyító (dehumanizáló) tevékenységet közvetítenek, de azok egytől-egyig erőszakmentesek.[215] Sőt - a pornográfia alelemeként - az erotika, a felek konszenzusán alapuló egészséges szexet feltételez.[216] Wilson [1978] érvelése alapján a pornográfiának egyáltalán nincsenek negatív hatásai, azok a szexuális oktatás területén leginkább pozitív funkciókkal rendelkeznek.[217] (Megjegyezni kívánom, hogy Wilson az 1980-

[210] MALAMUTH Neil, BILLINGS Victoria: Why Pornography? Models of Functions and Effects. In: Journal of Communication, 1984., 34. évf. 3. sz. – p.: 117-129.

[211] BROWNMILLER Susan: Against our Will: Men, Woman and Rape. – New York: Simon & Schuster, 1975.

[212] DONNERSTEIN Edward, BERKOWITZ Leonard: Victim reactions in aggressive erotic films as a factor in violence against women. In:Journal of Personality and Social Psychology, 1981., 41. év. 4. sz. – p.: 710-724

[213] FISHER William, BARAK Azy: Sex education as a corrective: Immunizing against possible effects of pornography. In: ZILMANN Dolf, BRYANT Jennings (szerk.): Pornography: Recent Research, Interpretations, and Policy Considerations. – Hillsdale: Lawrence Erlbaum Associates, 1989.

[214] KOVÁCS István: A prostitúció jelensége és társadalmi kontrolljának vizsgálata empirikus módszerekkel PhD értekezés, Budapest, UNI-NKE, 2016.

[215] ZILMANN Dolf, BRYANT Jennings: Effects of massive exposure to pornography. In: MALAMUTH Neil, DONNERSTEIN Edward (szerk.): Pornography and Sexual Aggression. – Orlando: Academic Press, 1984.

[216] FISHER William, BARAK Azy: Pornography, erotica, and behavior: More questions than answers. In: International Journal of Law and Psychiatry, 14. évf. 1-2. sz. – p.: 65-83.

[217] WILSON Cody: Can pornography contribute to the Prevention of Sexual Problems? In: QUALLS Brandon et al. (szerk.): The Precention of Sexual Disorders: Issues and Approaches. – New York: Plenum, 1978.

as amerikai elnöki bizottság kutatási igazgatója volt.)[218] A feminista álláspont úgy foglalható össze, hogy a pornográfia a férfi dominancia intézményesítésének központi eleme, nem reformálható, nem szüntethető-, és nem tiltható meg. A fenyegetettség törvénye az erkölcsiségre vonatkozik, a férfiak szempontjából, a férfi uralkodás szempontjából. Egy olyan politika, ami kritika a férfi dominanciával szemben, a nők alárendelt álláspontján keresztül.[219]

Miután a három ideológia széleskörű elemzését végrehajtottam, olyan fogalom megalkotására törekedtem, amely a negatív diszkriminációt kerüli, azonban az álláspontok lényeges elemeinek megértése mellett konszenzusos megoldásra törekszik. Nézetemben a pornográfia az alábbi összetevőkkel bír: A pornográfia egy olyan leíró, vagy hallási, és látási

---

[218] A pornográfia meghatározására Amerikában az 1970-es, és 1980-as években két nemzeti bizottság alakult, amik a nyilvánosság számára megkísérelték pornográf expozíció és az agresszív viselkedés, valamint a bűnözés közötti kapcsolat tekintetében a leghatározottabb válaszokat megadni. Az 1970-es Obszcenitás és Pornográfia Bizottság megállapította, hogy a szexuális jellegű anyagokkal szembeni expozíció nem volt antiszociális, és káros hatású. Az 1980-as években Ronald Reagen [amerikai elnök, 1911-2004] a pornográfia káros/nem káros hatásairól egy másik kormányzati vizsgálatot rendelt el. A bizottságot Edwin Meese [1931-] főügyész vezette. Mielőtt a bizottság eredményeit nyilvánosságra hozták volna, az heves vitát váltott ki. A Meese Bizottság valószínűleg arra a következtetésre jutott, hogy a pornográfia és a nőkkel szemben alkalmazott szexuális erőszak között okozati összefüggés van. A jelentés szerint a pornofilmek megtekintése a tipikus szexuális viselkedést megváltoztatja, a nemi erőszakot trivializálja, a nők felé mutató férfi agressziót elősegíti. A jelentés azért nem volt teljesen objektív, mert a vizsgálat nagyrészt erőszakos pornográf anyagokra terjedt ki, általánosságban pedig az összes pornográf anyagra ilyen következtetés nem levonható. Bár a hírhedt sorozatgyilkos Ted Bundy is előadta vallomásában, hogy számos brutális gyilkosságát az erőszakos pornográfia ihlette, és a Meese Bizottság jelentése is ilyen összefüggést tárt fel, Palys (1986), és Linz (1987) kutatásai ezeket sorra cáfolták: a pornográfia a férfiak és nők közötti szexuális kapcsolat egalitárius viszonyát közvetítette, valamint a férfiak nőkre gyakorolt szexuális agressziója elhanyagolható (nem szignifikáns) volt. In: HERTZBERG Hunt: Ed Meese and his pornography commission. In: New Republic, 1986., 14. évf. – p.: 21-24.; PALYS Ted: Testing the common wisdom: The social content of video pornography. In: Canadian Psychology, 1986., 27. évf. – p.: 22−35; DONNERSTEIN Edward et al.: The findings and recommendations of the Attorney General's Commission on Pornography: Do the psychological “facts” fit the political fury? In: American Psychologist, 1987., 42. évf. p.: 946−953.; BALMER Steven: The Limits of Free Speech, Pornography and the Law. In: Aberdeen Student Law Review, 2010., 13. évf. 1. sz. – p.: 66-82

[219] MACKINNON Catharine: Not a moral issue. In: Yale Law & Policy Review, 1983., 2. évf. 2. sz. – p.: 321-345.

ingereket összekapcsoló produktum, amely egy vagy több ember szexuális kapcsolatát írásban, vagy képi-, és audió formátumban megjeleníti. A felek között fennálló szexuális viszony olykor a laikusok számára félreérthetően erőszakosnak tűnő jeleneteket is tartalmaz, az viszont a felek egybehangzó akaratnyilvánításán, és konszenzusán alapul. A pornográf anyagok előállításának célja a nemi vágy felkeltése, és a fogyasztók szexuális igényeinek kielégítése, amelyet a gyártó(k) kedvtelése, vagy profitszerzése motivál.

2.2 A gyermekpornográfia (jogi) fogalma

A pornográfián belül a gyermekpornográfia nem jelent mást, mint a gyermekek szexuális zaklatását, az azzal kapcsolatos visszaélések összességét.[220] Miután a köztudatban a gyermekpornográfia káros hatásainak tekintetében elsődlegesen a szexuális kizsákmányolás, valamint a szexuális visszaélés került azonosításra, ezért arra kell törekednünk, hogy ezeket az elemeket a definícióalkotás során integráljuk. Mindannyiunk közös érdeke, hogy a gyermekpornográfia meghatározása a lehető legpontosabb legyen, hogy a visszaélésekkel okozott károk, és elkövetők büntetlenül ne maradhassanak. Az már szinte megszokottnak nevezhető, hogy bármely a világon előforduló jelenség definiálására egységes álláspont még nem született. Ahogy a pornográfia fejezetben is bemutatásra került, sem a pornográfia, sem a gyermekpornográfia nem jelent kivételt e kitétel alól. A gyermekpornográfia meghatározására amennyi ország, annyi fogalommeghatározás, és szabályozás született. A teljesség igénye nélkül csokorba szedtem pár európai, afrikai, és amerikai országot, ahol nemhogy az elkövetői magatartás, hanem az életkor tekintetében sincs egyetértés, meggátolva ezzel a fogalommeghatározás osztatlanságát.

A legtöbb országban a gyermekpornográfiával kapcsolatos szabályozás a felnőtté még nem vált populációt helyezi oltalom alá. (Ez lehet 18-, de ugyanakkor például az Amerikai Egyesült Államokban 21 életév is.)[221] Teszi mindezt azért, mert a gyermekek beszámítási, és

[220] ALLEN Ernie: Child Pornography: Model Legislation & Global Review. – United States: International Centre for Missing & Exploited Children, 2013.

[221] Érdekességként kell már e kritériumnál is megjegyeznünk, hogy a szóhasználat a gyermekpornográfiát öleli fel, ám a fogalom a klasszikus gyermekkor, a fiatalkor, vagy a fiatalkorú felnőtt vonatkozásában különbséget nem tesz.)

cselekvőképességgel nem rendelkeznek, nem képesek arra, hogy erkölcsileg, jogilag önálló döntést hozhassanak. Ugyanakkor vannak olyan országok, ahol a jogi cselekvő-, és beszámítási képesség a szexuális aktivitáshoz kapcsolódó hozzájárulás életkorát nem befolyásolja. Portugáliában például a gyermekpornográfiával kapcsolatos bűncselekmény sértettje kizárólag 14 év alatti személy lehet. A 14 év feletti, és a szexuális aktivitásra már megérett fiatalkorú, ha hozzájárulását adja, gyermekpornográfia bűncselekmény sértettjévé nem válhat. Svájcban ez a beleegyezési idő a 16. életév betöltése, ugyanakkor a gyermekpornográfiával kapcsolatos jogszabályok minden 18 életév alatti gyermek védelmét megteremtik. A svájci jogalkotás első olvasatra kicsit ellentmondásosnak tűnhet, azonban ez csak látszat: Amennyiben a 16. életévét betöltött személy előzetes tájékoztatást követően, beleegyezésével pornográf anyag előállításában részt vesz, úgy e bűncselekmény sértettje nem lehet. Amennyiben viszont e szükségszerű kritériumok hiányoznak, úgy akár a 16-18 év közötti korosztály is a bűncselekmény sértettjévé válhat. A 16-18 év közötti gyermekek érvényes beleegyező nyilatkozata határozza meg, hogy a kapcsolódó tevékenységek jogellenessé válnak avagy sem. Álláspontom szerint a gyermekpornográfiával kapcsolatban alkotott jogszabályoknak minden nagykorúvá nem vált gyermeket meg kell védeniük, tekintet nélkül arra, hogy a szexuális aktivitáshoz kapcsolódó hozzájárulási „jogosultságukat" gyakorolhatják-e vagy sem. A gyermekek, és fiatalkorúak szexuális aktus létesítéséhez fűződő jognyilatkozatát nem lehet úgy tekinteni, hogy az megfelel a jogi beszámítási-, és cselekvőképesség kritériumainak. Nem létezhet olyan hatályos, normaszerű gyermekkorútól, vagy fiatalkorútól származó érvényes jognyilatkozat, ami lehetőséget teremt arra, hogy a gyermekek pornográfiában, és a hozzá kapcsolódó jogellenes cselekményekben (pl. prostitúció) résztvehessenek. De ugyan ez a helyzet az elkövetés tárgyával is. Míg Barbadoson az elkövetés tárgyának kizárólag a gyermekekről készült fényképfelvételek számítanak, addig Belgiumban bármely médiával kapcsolatos vizuális objektum e tekintet alá esik. Dél-Afrikában bármely kép, vagy leírás megvalósíthatja a bűncselekményt, amennyiben azon 18 év alatti személy szerepel. Az elkövetési magatartás is országonként változó: Svédországban a gyermekpornográf felvételek birtoklása jogellenes, ám, ha valaki azt „csak nézi, figyeli" nem büntethető. Svédországban például nem jogellenes interneten gyermekpornot nézni, csak akkor válik valaki bűnelkövetővé, amennyiben azt adathordozóra

elmenti.[222] Számtalan országot, példát lehetne még hozni arra, hogy a nem egységes jogrendszer a gyermekpornográfia fogalmát hogyan kezeli, azonban a tanulmánynak ez – a korlátozott oldalszám végett - nem tárgyköre.

A következőkben a tematika szerint ismerjük meg, hogy európai viszonylatban, az unióban, és különös tekintettel hazánkban a gyermekpornográfia hatályos szabályozása milyen magatartást rendel büntetni, a bűncselekményt ki követheti el, és a büntetőjogág mely személyeket helyezte oltalom alá.

2.3 A gyermekpornográfia a nemzetközi (uniós) jogalkotásban

A gyermekpornográfia elleni küzdelem az uniós jogalkotásban stratégiai jelentőségű. Amióta a Tanács 1997-ben az emberkereskedelem és a gyermekek szexuális kizsákmányolása elleni küzdelem terén együttes fellépést fogadott el, a kezdeményezések száma nemzeti és regionális szinten is megsokszorozódott.[223] A tanulmány csupán két – talán súlyozottan a legfontosabb - uniós dokumentum elemzését tudja végrehajtani, mert a pályázat terjedelmének nagysága korlátozott.

Az első a Tanács 2004/68/IB (2003. december 22.) számú kerethatározata.[224] A kerethatározatot a CNS 2001/0025 számú konzultációs eljárással fogadták el, 2004. január 20-án lépett hatályba, az elfogadó államok pedig 2006. január 20-ig voltak kötelesek azokat a hazai joganyagukba beemelni. A kerethatározat a gyermekek szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelem vonatkozásában a tagállamok büntetőügyekben folytatott rendőrségi és igazságügyi együttműködésére vonatkozó törvényi és rendeleti szabályozásait kívánta közelíteni, összehangolni. Az uniós norma egy olyan rendszert hozott létre, amelyben a gyermekpornográfiát bűncselekménnyé nyilvánította, meghatározta a minősítő (súlyosbító) körülményeket, megteremtette az elkövetők büntetőjogi üldöztetését, szankciókat szabott ki, és a sértetteket megfelelő támogatásban részesítette. A joganyag a

[222] PETIT Miguel Juan: Rights of the Child. – United Nations: Economic and Social Council, 2004.

[223] 97/154/JHA - Joint action to combat trafficking in human beings and sexual exploitation of children – (hatályba lépett: 1997. február 24-én) (http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33072) (letöltés ideje:2017.08.01.)

[224] 2004/68/JHA - Combating of the sexual exploitation of children and child pornography - (hatályba lépett: 2003. december 22-én) (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33138&from=HU) (letöltés ideje:2017.08.01.)

gyermekek szexuális kizsákmányolásával kapcsolatos bűncselekmény tiltott-, valamint a gyermekpornográfiával kapcsolatos, számítógépes rendszer felhasználásával vagy anélkül megvalósított büntetendő magatartásait az elsők között konkretizálta. (Tilos a gyermekek prostitúcióra kényszerítése, a gyermekprostitúció bármilyen módon történő kihasználása vagy elősegítése, vagy az abból származó haszonszerzés. Tilos a gyermekkel folytatott szexuális tevékenység, amely érdekében az elkövető erőszakhoz, kényszerítéshez vagy fenyegetéshez folyamodik, vagy a szexuális szolgáltatásért cserébe pénzt vagy bármilyen egyéb jutalmazást ajánl fel, vagy visszaél bizalmi helyzetével, tekintélyével vagy a gyermekre gyakorolt befolyásával. Tilos gyermekpornográfia előállítása, gyermekpornográfia forgalmazása, terjesztése vagy továbbítása, gyermekpornográfiát tartalmazó anyagok felajánlása vagy azok hozzáférhetővé tétele, gyermekpornográfia megszerzése vagy birtoklása.) A tagállamok részére meghatározta továbbá, hogy a jogharmonizáció során úgy kötelesek eljárni, hogy gyermekpornográfia bűncselekmény esetén mind a felbujtói-, mind pedig a kísérleti magatartást büntetendővé kell nyilvánítaniuk, valamint a cselekmények alapbüntethetőségi tétele 3 évnél-, minősítő körülmény esetén 5 évnél alacsonyabb szabadságvesztéssel járó büntetés nem lehet. A jogszabály a természetes személy felelősségén felül, a jogi személy büntető-, és polgári felelősségét is bevezeti. Tekintettel arra, hogy az uniós normát az aláíró államok a saját joganyagukba beemelni kötelesek, ezért a kerethatározat a hatásköri szabályokra is kritériumokat határozott meg. (Területiség elve: valamely állam igazságszolgáltatási jogkörrel rendelkezik, amennyiben a bűncselekményt a területén követték el. Aktív személyiség elve: valamely állam igazságszolgáltatási jogkörrel rendelkezik, amennyiben az elkövető az adott tagállam állampolgára. A bűncselekményt az adott tagállam területén székhellyel rendelkező jogi személy javára követték el.) A norma vonatkozásában gyermek bármely 18 életév alatti személy, gyermekpornográfia pedig, minden olyan pornográf anyag, amely vizuálisan jeleníti meg a következőket: kifejezetten szexuális magatartást tanúsító vagy abban közreműködő létező gyermeket, beleértve a gyermek nemi szerveinek vagy szeméremtájékának explicit bemutatását, vagy ilyen magatartást tanúsító vagy abban közreműködő gyermeknek tűnő létező személyt, vagy ilyen magatartást tanúsító vagy abban közreműködő nem létező gyermeket ábrázoló élethű képeket.

A kerethatározatot az Európai Parlament és Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló irányelve váltotta.[225] Az irányelv a bűnelkövetőkkel szemben alkalmazott szankcióktól az áldozatvédelmen át, egészen a prevencióig terjedő szempontrendszert összefoglalja. A jogszabály a gyermekek szexuális bántalmazásával, szexuális kizsákmányolásával, valamint a gyermekpornográfiával kapcsolatos bűncselekményeket az Európai Unió egész területén harmonizálja. A kerethatározathoz képest számos változtatást eszközölt, így például az internetes gyermekpornográfia és a szexturizmus elleni küzdelemmel kapcsolatos rendelkezéseket is tartalmaz. A norma négy bűncselekményi kategóriában mintegy húsz bűncselekményt határoz meg. A négy kategória a szexuális bántalmazást, a szexuális kizsákmányolást, a gyermekpornográfiát, és a gyermekekkel való, szexuális céllal történő internetes kapcsolatfelvételt öleli fel. A szexuális bántalmazás a beleegyezési korhatárt el nem ért gyermekkel folytatott szexuális tevékenység, vagy a gyermeknek valamely harmadik féllel folytatott szexuális tevékenységre kényszer alkalmazásával történő késztetését jelenti. A szexuális kizsákmányolás alatt a gyermek gyermekprostitúcióra kényszerítését vagy pornográf előadáson való részvételre való késztetését értjük. A gyermekpornográfia a jogszabály értelmében annak birtoklását, ahhoz való hozzáférést, terjesztését, szolgáltatását, vagy készítését jelenti. A gyermekkel való, szexuális céllal történő internetes kapcsolatfelvétel a szexuális kizsákmányolás elkövetése céljából történő találkozásra gyermeknek tett internetes ajánlatot, valamint a gyermek ugyanilyen úton való késztetését, az őt bemutató pornográf anyag szolgáltatására vonatkozó tényállásokat gyűjti össze. Bár hasonlóan, ahogy a korábbi fejezetben is ismertetésre került, a jogszabály a tagállamokra bízza, hogy a beleegyezésen alapuló szexuális tevékenységek tekintetében bizonyos gyakorlatok büntetendőnek tekintendők-e vagy sem. (Mindezt persze csak akkor, ha azok hasonló életkorú, hasonló lelki és testi érettségi szintű személyeket érintenek, és a szexualitás normális felfedezésének tekinthetőek.) Ugyanakkor e kitételtől függetlenül az irányelv a

[225] Directive 2011/93/EU - of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework-Decision 2004/68/JHA – (hatályba lépett: 2011. december 17-én) (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0064&from=HU) (letöltés ideje:2017.08.01.)

gyermekpornográfiával kapcsolatban többletfeladatokat is megszab: az internetes gyermekpornográfia vonatkozásában a tagállamoknak intézkedniük kell a területükön üzemeltetett, gyermekpornográf jellegű honlapok azonnali eltávolítása érdekében, emellett törekedniük kell arra, hogy a külföldön üzemeltetett honlapokat eltávolíttassák. Ezenkívül az internetfelhasználókkal kapcsolatos, bizonyos átláthatósági és tájékoztatási feltételek mellett lehetőségük van arra, hogy a területükön az ilyen honlapokhoz való hozzáférést letilthassák. A vádemeléssel kapcsolatos büntetőeljárások lefolytatása pedig nem lehet kizárólag az áldozat által tett bejelentés vagy feljelentés függvénye, a büntetőeljárásnak akkor is lefolytathatónak kell lennie, ha az adott személy a vallomását, vagy magánindítványát például visszavonta. Ezenkívül a legsúlyosabb bűncselekmények bizonyos típusai esetében kellő idővel az áldozat nagykorúvá válását követően is lehetőséget kell biztosítani a vádemelésre. Mindemellett az irányelv a korábbi kerethatározattal megegyezően a büntetési tétel minimumát is meghatározza, valamint a felbujtást, és a kísérletet is büntetni rendeli. A súlyosbító körülmények között megtaláljuk a különösen kiszolgáltatott gyermek fogalmát is, valamint csakugyan minősítő körülmény, ha a bűncselekményt a gyermek családtagja, vagy bizalmi vagy hatalmi helyzetével visszaélő személy követi el, sőt az is, ha az elkövetőt korábban már hasonló jellegű bűncselekményért elítélték. A joghatóság kérdéskörében az irányelv a kerethatározatot az alábbiakkal egészítette ki: a tagállamok joghatósággal rendelkeznek a területükön az állampolgáraik által elkövetett bűncselekmények esetén, joghatóságukat a külföldön elkövetett bűncselekményekre is kiterjeszthetik, ha az elkövető szokásos tartózkodási helye a területükön található, illetve ha a bűncselekményt a területükön letelepedett jogi személy javára követték el, sőt akkor is, ha az áldozat az ő állampolgáruk.

Bár a tanulmány korlátozott terjedelem között mozog, nem szabad elfeledkeznünk arról, hogy a két jogforrás mellett ugyan olyan kiemelt jelentőséggel bírnak az Egyesült Nemzetek Szövetségének, és az Európa Tanács jogforrásai is. (A Gyermekek Jogairól szóló New York-i Egyezmény, és annak Fakultatív Jegyzőkönyve, vagy az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye, és a Gyermekek Szexuális Kizsákmányolás és Szexuális Zaklatás elleni védelméről szóló Egyezménye is.)[226],[227],[228],[229]

[226] Convention on the Rights of the Child - Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20. November 1989. – (hatályba lépett: 1990. szeptember 02-án) (http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx) (letöltés ideje: 2017.08.01.)

A következőkben pedig ismerjük meg, hogy Magyarország az uniós jogalkotást a büntető joganyagába milyen módon helyezte át, az a nemzetközi kerethatározathoz, és irányelvhez asszimilálódik-e.

2.4 A gyermekpornográfia a nemzeti (hazai) jogalkotásban

Bár a hatályos Büntető Törvénykönyvünk XX. fejezete a gyermekek érdekét sértő, és család elleni bűncselekmények címet viseli, a gyermekpornográfia mégis a XIX. fejezetben a nemi élet szabadsága, és a nemi erkölcs elleni bűncselekmények között található.[230]

Gyermekpornográfia

204. § (1) Aki tizennyolcadik életévét be nem töltött személyről vagy személyekről pornográf felvételt

a) megszerez vagy tart, bűntett miatt három évig,

b) készít, kínál, átad vagy hozzáférhetővé tesz, egy évtől öt évig,

c) forgalomba hoz, azzal kereskedik, illetve ilyen felvételt a nagy nyilvánosság számára hozzáférhetővé tesz, két évtől nyolc évig

terjedő szabadságvesztéssel büntetendő.

(2) Két évtől nyolc évig terjedő szabadságvesztéssel büntetendő, aki az (1) bekezdés b) pontjában meghatározott bűncselekményt az elkövető nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, illetve a sértettel kapcsolatban fennálló egyéb hatalmi vagy befolyási viszonnyal visszaélve követi el.

---

[227] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography - Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25. May 2000. – (hatályba lépett: 2002. január 18-án) (http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx) (letöltés ideje: 2017.08.01.)

[228] Convention on Cybercrime – Council of Europe - (hatályba lépett: 2001. november 23-án) (http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (letöltés ideje: 2017.08.01.)

[229] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse - Council of Europe - (hatályba lépett: 2007. október 25-én) (https://rm.coe.int/168046e1e1) (letöltés ideje: 2017.08.01.)

[230] 2012. évi C. törvény – a Büntető Törvénykönyvről – (hatályba lépett: 2012. július 13-án) (https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV) (letöltés ideje: 2017.08.01.)

(3) Egy évtől öt évig terjedő szabadságvesztéssel büntetendő, aki az (1) bekezdés c) pontjában meghatározott bűncselekményhez anyagi eszközöket szolgáltat.

(4) Aki tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf műsorban

a) szereplésre felhív, három évig,

b) szerepeltet, egy évtől öt évig

terjedő szabadságvesztéssel büntetendő.

(5) Három évig terjedő szabadságvesztéssel büntetendő, aki

a) tizennyolcadik életévét be nem töltött személyt vagy személyeket pornográf felvételen való szereplésre felhív,

b) olyan pornográf műsoron vesz részt, amelyben tizennyolcadik életévét be nem töltött személy szerepel vagy ilyen személyek szerepelnek,

c) tizennyolcadik életévét be nem töltött személy vagy személyek pornográf műsorban való szerepeltetéséhez anyagi eszközöket szolgáltat.

(6) Aki tizennegyedik életévét be nem töltött személyről vagy személyekről pornográf felvétel készítéséhez, forgalomba hozatalához vagy az azzal való kereskedelemhez szükséges vagy azt könnyítő feltételeket biztosítja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

A törvény a hetedik bekezdésben a pornográf felvétel, valamint a pornográf műsor fogalmát határozza meg. A jogszabály szerint a pornográf felvétel olyan videó-, film- vagy fényképfelvétel, illetve más módon előállított képfelvétel, amely a nemiséget súlyosan szeméremsértő nyíltsággal, célzatosan a nemi vágy felkeltésére irányuló módon ábrázolja. A pornográf műsor fogalma alatt pedig a nemiséget súlyosan szeméremsértő nyíltsággal megjelenítő, célzatosan a nemi vágy felkeltésére irányuló cselekvés vagy előadást értjük.

A bűncselekmény jogi tárgya a kiskorúak egészséges szexuális fejlődésének védelméhez fűződő társadalmi érdek. Passzív alanya a kiskorú személy, ám a törvény joghatóságát a tizenhatodik életévét betöltött, és házasságkötéssel nagykorúvá vált személyekre is. Az elkövetés tárgya a pornográf felvétel, illetőleg a pornográf műsor.

Az elkövetési magatartások hat csoportba oszthatók. Az első csoportba azok a magatartások tartoznak, amelyek a passzív alanyról pornográf felvételt megszereznek, tartanak, készítenek, kínálnak, átadnak, (nagy nyilvánosság számára) hozzáférhetővé tesznek,

forgalomba hoznak, azzal kereskednek. A második csoportban az anyagi eszközök szolgáltatása található. A harmadik csoportban azok az elkövetési magatartások lelhetők fel, amelyek a passzív alanyt pornográf műsorban szereplésre felhívják, szerepeltetik. A negyedik csoport a szereplésre felhívás magatartását vonultatja fel, azonban a passzív alanyt nem pornográf műsorban, hanem pornográf felvételen kívánja szerepeltetni. Az ötödik csoportban a részvétel büntetendő, olyan pornográf műsoron, amin a passzív alany szerepel. A hatodik csoport az anyagi eszközök szolgáltatását jelenti, mint sui generis bűnsegédi magatartást.

A bűncselekményt bárki elkövetheti, azonban a bűnösség kizárólag szándékosság lehet. Mivel célzatos bűncselekmény, ezért a bűnösség tekintetében is csak dolus directus (egyenes szándék) állapíthat meg.

A magyar jogszabály a nemzetközi szabályozáshoz részben alkalmazkodott. Gondolok itt például arra, hogy a törvény a minősített esetek közé a nemzetközi elvárásokat is beépítette. Ilyen magatartás például, és egyben a cselekménye súlyosabban büntetendő annak, aki a bűncselekményt az elkövető nevelése, felügyelete, gondozása vagy gyógykezelése alatt álló személy sérelmére, illetve a sértettel kapcsolatban fennálló egyéb hatalmi vagy befolyási viszonnyal visszaélve követi el. A hazai és a nemzetközi norma között a bűncselekmények büntetési tételének vonatkozásában is összhang van. Megjegyzést kíván viszont a nemzetközi szerződés azon szövegrésze, amely a „kiskorúnak látszás" fogalmával operál. A hatályos Büntető Törvénykönyv a pornográf felvételen ábrázolt alany életkorához köti a cselekmény megvalósulását, amely a nemzetközi norma aktusát figyelmen kívül hagyja. A szóban forgó tényállás egyfajta szexuális perverzió ellen kíván büntetőjogi védelmet teremteni, amelynél nem az ábrázolt személy életkorának van döntő jelentősége, hanem gyermeki kinézetének. A büntetőjogi fellépés tehát nem csak akkor indokolt, ha az ábrázolt személy nem töltötte be a 18. életévét, hanem akkor is, ha az ábrázolt személy - aki esetleg már 18 év feletti - kinézetében fejletlen. E véleményt erősíti, hogy az ábrázolt alanyok életkorát az eljárás során legritkább esetben lehet felderíteni. Valójában az ábrázolt alanyok kinézete alapján kerül sor az elkövető felelősségre vonására. Ez a gyakorlat ellentétben áll a törvényességgel, mert a hatóságnak bizonyítani kellene a pornográf felvételen szereplő személy életkorát, és nem lenne elegendő az ábrázolt alanyok életkorának csak a becslése. Éppen ezért indokolttá válhat kiegészítő törvényhely és/vagy szöveg beemelése, ami ezt a joghézagot megszüntethetné.[231]

[231] BLASKÓ Béla, MIKLÓS Irén, PALLAGI Anikó, POLT Péter, SCHUBAUER László: Büntetőjog különös rész I. – Budapest-Debrecen: Rejtjel Kiadó, 2013.

A gyermekek sérelmére elkövetett visszaélések, és a gyermekpornográfia bűncselekmények elemzését követően a nemzetközi szervezetek témával kapcsolatos iOCTA, és INHOPE jelentéseit veszem górcső alá, egyúttal bemutatom, hogy világszerte ez milyen fenyegetettségét, és veszélyt hordoz magában.

3. Nemzetközi kitekintés

3.1 A gyermekpornográfia, mint nemzetközi veszélyforrás

E fejezetben a már meglevő kutatási eredményekkel próbálom felhívni a figyelmet arra, hogy a gyermekpornográfia milyen veszélyeket is rejt önmagában. Miért is veszélyes, ha a jogalkotó nem szab gátat annak, hogy a gyermekek önállóan, bizonyos kor eltelte után a gyermekpornográfiában való részvételhez beleegyezésüket adják? Költői kérdésre nemes egyszerűséggel az alábbi választ adhatjuk: ezáltal a bűnelkövetők a törvényi üldöztethetőség elől megmenekülhetnek.

A világon számos tanulmány született, amely a pornográfia gyermekkorúakra, és serdülőkre gyakorolt hatását vizsgálja. Mindegyikben közös, hogy a gyermekpornográfiával kapcsolatos kényszeres, addiktív bűnözői magatartás olyan globális trendnek tekinthető, amely egyetlen kultúra, vagy régió számára sem különíthető el. A gyermekpornográfia nem szűkíthető le egy adott régióra, az a világon mindenhol jelen van, érintve akár a 10-, a 18-, vagy a 21 éves korosztályt, akár Angliában, akár az Egyesült Államokban, vagy akár Tajvanon is.[232],[233],[234],[235],[236] Köszönhető ez mindannak, hogy az internet szinte minden fiatal életében kiemelt szerepet játszik. Egy világméretű - tizenhárom különböző ország

[232] YBARRA Mitchell et al: Exposure to Internet pornography among children and adolescents: A national survey. In: CyberPsychology and Behavior, 2005., 8. évf. – p.: 473–486.

[233] BRAUN_CUORVILLE Debra et al: Exposure to sexually explicit web sites and adolescent sexual attitudes and behaviors. In: Journal of Adolescent Health, 2009., 45. évf. – p.: 156–162.

[234] MALAMUTH Neil et al: Developmental pathways into social and sexual deviance. In: Journal of Family Violence, 2010., 25. évf. – p.:141–148.

[235] SUSSMAN Steven: Sexual addiction among teens: A review. In: Sexual Addiction & Compulsivity, 2007., 14. évf. – p.: 257–278.

[236] YEN Chang et al: Multi-dimensional discriminative factors for Internet addiction among adolescents regarding gender and age. In: Psychiatry Clinical Neurosciences, 2009., 63 évf. 3. sz. – p.: 357–364.

részvételével zajló - internetes felmérés azt mutatta, hogy a brit fiatalok 100-, az izraeli ifjúság 98-, a cseh serdülők 96-, és a kanadai gyerekek 95 százaléka rendszeresen használja az internetet. Az Egyesült Államokban a 12-17 éves korosztály 93 százaléka internet-felhasználó, ebből 63 százalék az internetre naponta átlagosan többször fellép, és 36 százalék a világhálón folyamatosan online státusszal megtalálható.[237]

A serdülők szexuális jellegű anyagokkal való találkozását és fogyasztását az internetes technológiák közelmúltbeli elterjedése jelentősen megváltoztatta. Ha egyszer az adatkapcsolat a személyi számítógép, a mobiltelefon, vagy más elektronikai eszköz felületén létrejön, ebben a rendkívül szexualizált környezetben a gyermekek felügyelet nélkül maradnak.[238] Figyelemre méltó az a tartalom, mennyiség, és terjedelem, ami a szexualitással kapcsolatban az interneten fellelhető. A technikailag közvetített pornográf tartalom példátlan sebességgel megannyi újdonságot, és változatosságot kínál. E körülmények alapján feltételezhetjük, hogy a serdülők interneten keresztül történő pornográfiához való hozzáférése semmilyen más eszközzel nem párosul.[239]

Egy lengyel kutatás szerint az internetet használó gyermekek 92 százaléka online szolgáltatásokon belül kommunikál. 75 százalékuk neten kívüli találkozóra kapott már ajánlatot, és 25 százalék volt, aki - elfogadva ezt a javaslattételt – a találkozón részt vett. A gyermekek 56 százaléka már folytatott nemkívánatos szexuális beszélgetést, a beszélgetések 14-, a képek küldése és/vagy fogadása 66-, és a találkozóra való felhívás 69 százalékát szexuális indíttatás ösztönözte.[240] A gyermekek koruknál fogva fel sem fogják, hogy a szexuális bűnelkövetők milyen erkölcsi-, és fizikai károkat okozhatnak/okoznak. Egy közelmúltban lezajlott kísérlet a fentieket teljes mértékben alátámasztja: Croft [2007] és társai az úgy nevezett „sexting" jelenség gyermekekre gyakorolt hatását vizsgálták, amely bizonyította, hogy a gyermekek ugyan a gyermekpornográfia veszélyeivel tisztában vannak, ám a legtöbb fiatal e veszélyre fittyet hányva, a szexuális képek, videók és különböző

[237] OWENS Eric et al.: The Impact of Internet Pornography on Adolescents: A Review of the Research. – United Kingdom: Routledge, 2012.

[238] COOPERSTMIH Jonathan: Does your mother know what you really do? The changing image and nature of computer-based pornography. In: History and Technology, 2006., 22. évf. 1. sz. – p.:1–25.

[239] WOLAK Janis et al.: Trends in youth reports of sexual solicitations, harrassment and unwanted exposure to pornography on the Internet. In: Journal of Adolescent Health, 2007., 40. évf. – p.: 116–126.

[240] OWENS Eric et al.: The Impact of Internet Pornography on Adolescents: A Review of the Research. – United Kingdom: Routledge, 2012

anyagok cserélését szórakoztatónak tartja.[241] Az Egyesült Államokban a serdülők-kultúrájában a „sexting" normalizált magatartásformává vált. A megkérdezett fiatalok közül 58 százalék, azaz a többség nem tartotta veszélyesnek, ha az interneten szexuális tartalmú anyagot oszt meg, annak legáltalánosabb indokát egymás szórakoztatásában jelölték meg. A kutatás azt mutatta, hogy a gyermekek a „sextinghez" kapcsolódó kockázatokkal tisztában vannak, mégis az napi életük részévé vált, a szexuális tartalmú anyagok cserélése folyamatos jellegű. Az a tény, hogy a szocializációs folyamatok eredményeképpen a jelenség mindennapossá vált, nem jelenti azonban azt, hogy ezt a viselkedést egyszerűen a felnőtteknek, a hatóságoknak, és a szociális szakembereknek el kell fogadniuk és ártalmatlannak kell tekinteniük, ugyanis a gyermekek nem rendelkeznek kellő érettséggel ahhoz, hogy a jelenség káros következményeit felismerjék. Az interneten kicserélt képek, ha nem is abban a pillanatban, de a gyermekek későbbi életük során becsületükre, hírnevükre negatív hatást gyakorolhat, amely akár zaklatásokhoz, visszaélésekhez is vezethet.[242] Mivel a gyermekek korlátozott beszámítási-, és cselekvőképességgel rendelkeznek, ezért a felnőttekre, a hatóságokra, és a szociális szakemberekre nagy felelősség hárul, hogy a gyermekek egészséges erkölcsi-, testi-, és lelki fejlődésüket megvédjék, és megteremthessék.

3.2 Nemzetközi szervezetek és jelentéseik

3.2.1 iOCTA

Ahogy azt láthattuk a gyermekpornográfia a határokon átnyúló nemzetközi veszélyforrássá nőtte ki magát, ezért az ellene való fellépés nem egy állam, hanem az államok közösségének a feladata. Ad absurdum e logikát tovább folytatva az Európiai Unió gyermekpornográfia elleni küzdelmének hatékonysága az államok által delegált szakpolitikai döntéshozóinak együttműködésétől nagymértékben függ. Az együttműködés pedig csak úgy valósulhat meg, ha van egy olyan közös uniós szervezet, amely a végrehajtásban résztvevő

[241] A „sexting" a szexuálisan szuggesztív, explicit képek, videók, és anyagok digitális rögzítését, majd annak mobiltelefonnal, vagy internetes felülettel a közösségi oldalakon - például Facebook, MySpace, Twitter, stb. – való megosztását, továbbítását, cserélését jelenti.

[242] CROFTS Thomas, LEE Murray: „Sexting", Children and Child Pornography. In: Sydney Law Review, 2013., 35. évf. 85. sz. – p.: 85-106.

ügynökségek, intézmények, és más releváns partnerek kölcsönös információcseréjén alapuló helyzetelemzését a döntéshozók számára előkészíti. Ennek egyik legfontosabb csúcsszerve, az EUROPOL 1995-ben alakult, amelynek elsődleges feladatai közt szerepelt, hogy a tagállamok bűnüldöző hatóságainak a nemzetközi bűncselekmények, és a terrorizmus elleni fellépésében segítséget nyújtson, valamint az államok közötti koordinációt megteremtse.[243] (A tanulmány az EUROPOL felépítését, szervezetét, és működését nem tárgyalja, annak részintézményével az iOCTA jelentéseivel foglalkozik.)

Több alapfeladat mellett ez volt az első olyan szerv, amely a döntéshozók részére a hírigényeket kielégítette, azaz a tagállamok közötti bűnügyi információk elemzését-értékelését elvégezte, megteremtve ezzel az Európai Unió (bűnüldözési) szakpolitikája kidolgozásának információs háttértámogatását. Ez a háttértámogatás a tagállamok rendőrségi, vám- és igazságügyi együttműködésének biztosításában, valamint a menekültüggyel, a bevándorlással és a külső határok ellenőrzésével kapcsolatos összehangolt politika kialakításában kiemelkedő szerephez jutott. A Maastrichti, Amszterdami és Nizzai Szerződések a bel- és igazságügy terén egy közös jogi keretrendszert hoztak létre, a tagállamok politikai területeit az Európai Unió többi politikai területével összehangolták, azonban az új veszélyek, és fenyegetések a világban olyan változást idéztek elő, ami a tagállamokat új intézkedések bevezetésére sarkallták.[244],[245],[246] A külvilágban materializálódó változásokra minden Európai Uniót érintő szervnek és/vagy szervezetnek az eredményesség megtartása mellett reagálnia kellett, ezért ez a természetes fejlődés, mesterséges fejlesztés az EUROPOL intézményét sem kímélte. A Rómában 2004. október 29-én aláírt Európai Alkotmány létrehozásáról szóló szerződés a szabadságon, a biztonságon és a jog

[243] DISLEY Emma, IRVING Barrie, HUGHES William, PATRUNI Bhanu: Evaluation of the implementation of the Europol Council Decision and of Europol's activities. – Santa Monica: Rand Corporation, 2012.

[244] Amszterdami Szerződés - Az Európai Unióról szóló szerződés, az Európai Közösségeket létrehozó szerződések és egyes kapcsolódó aktusok módosításáról -, 1997. október 02-án, (letöltés ideje: 2017. 07. 12.)

[245] Maastrichti Szerződés – Az Európai Unióról szóló szerződés -, 1992. február 07-én, (https://europa.eu/european-union/law/treaties_hu), (letöltés ideje: 2017. 07. 12.)

[246] Nizzai Szerződés – A Bizottság összetételének módosításáról, illetve a tanácsi szavazási rendszer átalakításáról -, 2001. február 26-án, (https://europa.eu/european-union/law/treaties_hu), (letöltés ideje: 2017. 07. 12.)

érvényesülésén alapuló közös térséget szilárdabb alapokra helyezte.[247] A 2005. évben hatályba lépő Hágai Program feladatul szabta meg, hogy az EUROPOL közreműködésével minden tárgyévben egy olyan tagállami információkon alapuló összefoglaló helyzetjelentés készüljön, amely a biztonságot fenyegető-, és veszélyeztető kockázatokat - különös tekintettel a szervezett bűnözés-, és terrorizmus vonatkozásában - azonosítsa, elemezze-értékelje, és azt a döntéshozók részére stratégia-alkotás céljából felterjessze.[248] E feladat végrehajtására alakult meg az úgy nevezett OCTA (Organized Crime Threat Assessment) jelentés-készítésének intézménye, amely a korábbi EUROPOL által gyártott témajelentéseket, először 2006-ban immáron a Hágai Programnak megfelelően az „Európai Unió Szervezett Bűnözés Fenyegetettségének Értékelése" címmel leváltotta.

Az OCTA jelentések egy olyan közös adatbázis változóit dolgozták fel, amelyekhez a számadatokat a tagállamoknak kiküldött kérdőívek megválaszolása szolgáltatta. Az úgy nevezett „Survey" statisztikai feldolgozó módszer célja annak megteremtése, hogy olyan információkat gyűjtsön, amelyek alapján egy adott jelenség leírhatóvá-, más jelenségekkel összehasonlíthatóvá váljék, a közöttük levő összefüggés feltárható legyen, eredményeit pedig általánosítani tudják. A kutatások módszere alapos szakmai előkészítő munkát, gondos adatfelvitelt, ellenőrzést, és pontos dokumentálást követel meg, különben az eredmények torzulhatnak, és azoknak a valósághű értelmezése veszélybe kerül.[249] Az OCTA jelentések mindösszesen hat szemesztert éltek meg, a hozzá fűzött reményeket nem váltották be, a Hágai Programban meghatározott célt megvalósítani nem tudták. A hivatalos felülvizsgálati jelentés megállapította, hogy sem az alapos szakmai előkészítő munka (kutatási metódus megválasztása), sem a gondos adatfelvitel (adatgyűjtési mechanizmus bonyolultsága), sem az ellenőrzés (tagállamok beküldött dokumentációinak hivatalos jóváhagyása), sem a pontos dokumentálás (tagállamok részértékelései) sem valósult meg, így az eredmények nem voltak

---

[247] Szerződés az Európai Alkotmány létrehozásáról – Rómában -, 2004. október 29-én, (https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_hu.pdf) (letöltés ideje: 2017. 07. 12.)

[248] Hágai Program – A szabadság, a biztonság, és a jog érvényesülésének erősítése az Európai Unióban – 2005. március 03-án (http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52005XG0303(01)), (letöltés ideje: 2017. 07. 12.)

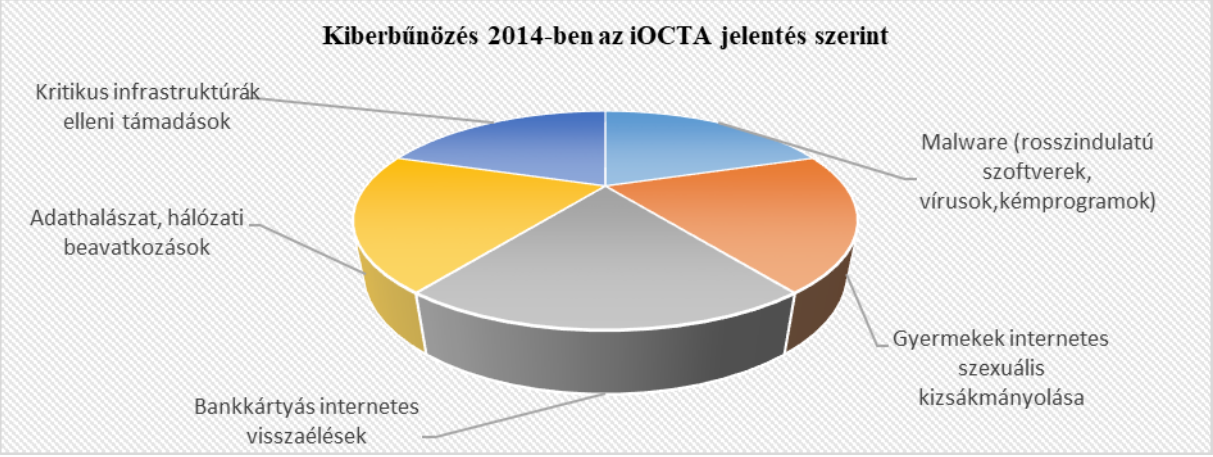
[249] LEEUW Edith, HOX Joop, DILLMAN Don: International Handbook of Survey Methodology. - United Kingdom: Routledge, 2008.

legalizálhatók. Egy torz, valósághűtlen adatbázis nem alkalmas arra, hogy elméleti szinten megalapozott, és a gyakorlatban alkalmazható stratégiát teremtsen. Az OCTA megszűnése viszont az Európai Unió egyik szervét és/vagy szervezetét sem mentesítette a Hága Program célkitűzésének-, és feladatvégrehajtásának kötelme alól. A szakágakért felelős politikusok olyan azonos jellegű, de új kutatási metóduson alapuló, és új tartalommal rendelkező jelentés elkészítését követelték, ami alapján a szervezett bűnözés ellen kivitelezhető, és a gyakorlatban alkalmazható stratégia-megalkotására van lehetőség. Ezen a ponton került képbe az operatív, bűnügyi hírszerzés fontossága. Nem meglepő, hisz a felgyorsult világnak – globalizáció, urbanizáció, stb. – köszönhetően egyre inkább felerősödik a hírszerzés, a felderítés, a rendszerszemléletű információ-adatgyűjtés, a komplex információkezelés (gyűjtés, rendszerezés, tárolás, feldolgozás, hasznosítás) és az elhárítás szerepe.[250] A hírszerző tevékenység során begyűjtött információk, azok elemzése-értékelése kellő alapot nyújtott az új „Európai Unió Súlyos, és Szervezett Bűnözés Fenyegetettségének Értékelése" címet viselő SOCTA (Serious and Organized Crime Threat Assessment), jelentések elkészítéséhez. A jelentések adatbázisát már nemcsak a tagországokhoz kiküldött kérdőívek (csak bűnüldözési területen több, mint 2300 kérdőív), hanem a tagállamok hírszerző tevékenységének eredményei, az uniós, és unión kívüli együttműködő partnerek, intézmények számadatai, az analitikus munkafájlok, és az EUROPOL által rendelkezésre bocsátott nyitott forrásokból származó információinak adathalmaza is kiegészítette. A jelentések elkészítéséhez szükséges, és felhasználható adatbázis terjedelme az OCTA adatbázisához képest, több, mint a kétszeresére nőtt. Az interakciós folyamat részeként a SOCTA módszertanát továbbfejlesztették, és a szervezetben dolgozó szakemberek által finomították. Az új módszernek köszönhetően a szervezett bűnözés dimenzionális összetevői – így különösen annak piacai, a bűnözői területek, az egyéni elkövetők, az elkövetett bűncselekmények, a környezeti változások – értékelhetők, és megérthetők. A SOCTA az Európai Unióra legveszélyesebb bűnügyi jelenségeket, a kérdőíves feldolgozás mellett vegyes módszerekkel, például minőségi, és mennyiségi analízissel egyértelműen képes meghatározni. A jelzett, és ajánlott prioritásokra a döntéshozók figyelmét felhívja, a jelentések az átláthatóságot, és a megbízhatóságot biztosítják. Tényként kezelendő, hogy a SOCTA értékelése az OCTA jelentésekhez viszonyítva mérföldköves változtatásokon ment keresztül, amely előnyére vált.

[250] KOVÁCS István: Is the prostitution a threat/danger to a country's (national)security? In: National Security Review, 2017., 5. évf. 1. sz. – p.:12-24.

Ugyanakkor nem elhanyagolható tény, hogy bizonyos tekintetben – például a szervezett bűnözői hálózatok tagoltsága, vagy a levont konklúziók túlzott általánosítása, stb. – a SOCTA is fejlesztésre szorul, amelyet a tagállamok erre a célra kijelölt egységei, és tisztviselői a mai napig fejlesztenek.

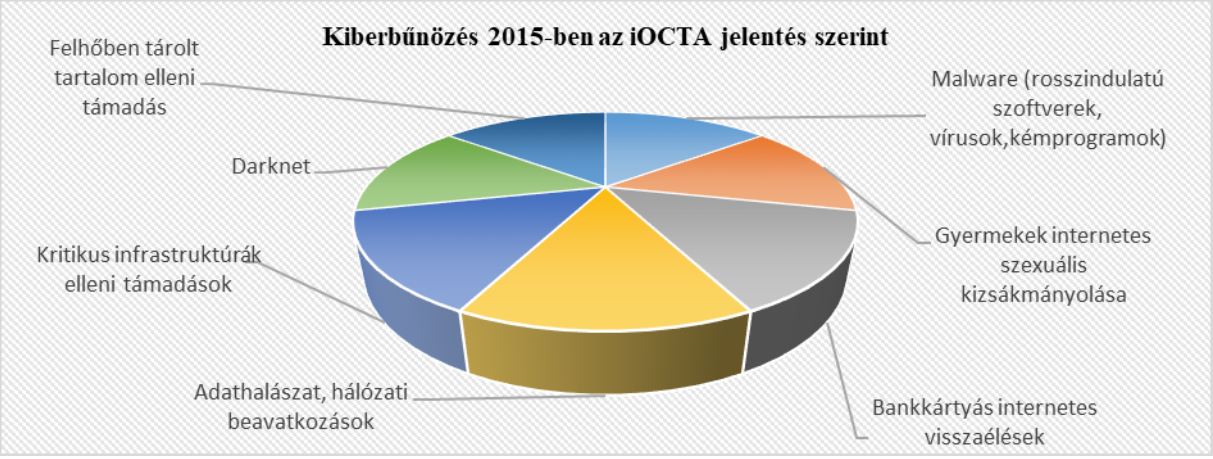
A fejlesztés eredményeképpen születhetett meg az internetes szervezett bűnözés értékelésére létrehozott adatbázis, az iOCTA, az „Európai Unió Internetes Szervezett Bűnözés Fenyegetettségének Értékelése" (Internet Organized Crime Threat Assessment) adatbázisa, és jelentései. Tekintettel arra, hogy a szervezett bűnözői hálózatok már nemcsak transznacionálisan a szárazföldön, levegőben, vízen, hanem a kibertérben is tevékenykednek, a kibertérhez kapcsolódó bűncselekmények elemzésére-értékelésére, valamint az az elleni fellépésre ezért égető jelleggel ugyan olyan szükség van. A bűnözői hálózatok növekvő, kifinomult támadásai, az attribúció, a szolgáltatásokkal való visszaélés, a nem megfelelő jogi szabályozás mind-mind hozzájárul ahhoz, hogy a kibertér veszélyessé váljon. A kihívásokkal szemben az iOCTA olyan ajánlásokat képes megfogalmazni, ami a számítógépes bűnözés elleni fellépést nagymértékben segítheti. A fentiek illusztrálására az EUROPOL szervezeténél fellelhető iOCTA jelentések (3 darab) éves vizsgálatát végeztem el, majd arról grafikont készítettem.



1. diagram: iOCTA jelentések a kiberbűnözés tükrében 2014; Forrás: A szerző (iOCTA jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

Az iOCTA első jelentése 2014. évből származik. A jelentés öt darab bűncselekmény elemzését-értékelését hajtotta végre, majd szolgáltatott ajánlásokat a döntéshozók számára. A kiberbűnözéssel kapcsolatosan öt kategóriát állított fel: olyan internetes bűncselekmények,

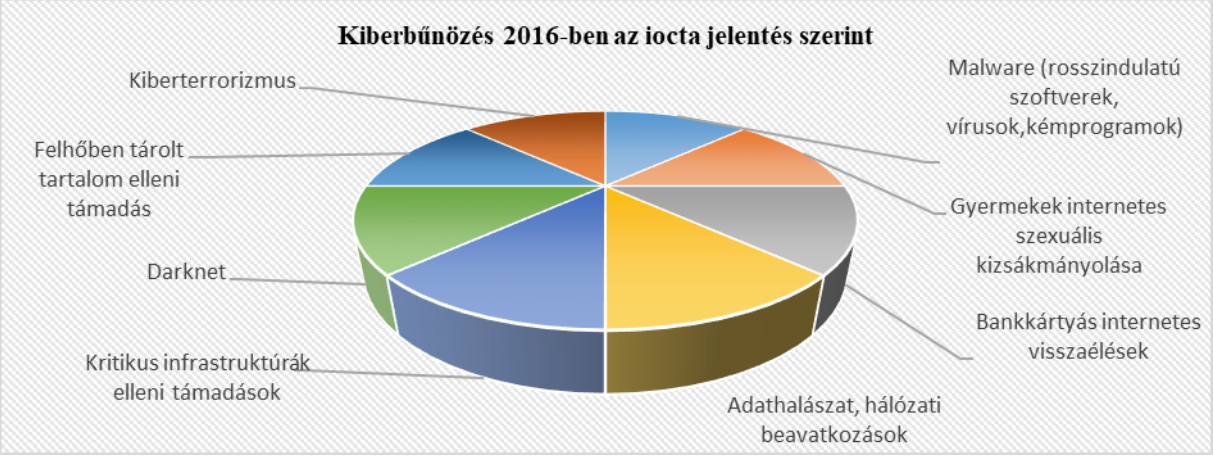
amelyek egy ország kritikus infrastruktúrái elleni támadásokat hajtanak végre; adathalászok, hálózati beavatkozások; bankkártyás online visszaélések; malware programok; valamint a gyermekek internetes szexuális kizsákmányolása. Az iOCTA jelentés vonatkozásában a kritikus infrastruktúrák elleni támadás azokat a bűncselekményeket öleli fel, amelyek például az ország fontosabb távközlési rendszerei ellen irányulnak. Az adathalászok általi hálózati beavatkozások fontos akár magán, akár állami érdekeket sérthet, az információk megszerzése visszaélésekhez vezethet. A bankkártyás internetes visszaélések a tranzakciókkal kapcsolatos valuták megszerzését jelentik. A malware olyan rosszindulatú szoftver, vagy vírus, amely a számítástechnikai rendszer működését összeomlasztja. A gyermekek internetes szexuális kizsákmányolása a gyermekpornográfiával azonosítható. Bár a jelentés a bűncselekmények között prioritást nem állít fel, az az elleni fellépés halasztást nem tűr. Ahogy a világ rohamosan fejlődik, úgy a bűncselekmények is ahhoz asszimilálódnak, a bűnüldöző szerveknek ugyan ilyen gyorsasággal kell azokra reagálniuk.



2. diagramm: iOCTA jelentések a kiberbűnözés tükrében 2015; Forrás: A szerző (iOCTA jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

Az iOCTA második jelentése 2015. évből származik. Az első jelentés felülvizsgálatát követően a kiberbűnözés terén a 2015-ös évben két újabb bűncselekmény-kategóriát sikerült azonosítani. Mindamellett, hogy az öt kategóriában változás nem történt, a bűnözői hálózatok a felhőkben tárolt tartalmak ellen is támadást indítottak, azok eltulajdonítására törekedtek, valamint az internetet elárasztották az úgy nevezett darknet oldalak is. A technikai fejlődésnek köszönhetően adatainkat már nem különböző háttértárakon tároljuk, hanem azokat felhőkbe töltjük, hogy bárhonnan elérhetővé váljanak. A bűnözők ezeket próbálják meg eltulajdonítani,

és azokkal a lehető legszélesebb körben visszaélni. A darknet alatt olyan honlapokat értünk, amelyek az az anonimitást biztosító úgy nevezett TOR hálózatokon keresztül elérhetők, a különböző keresőmotorok azokat nem látják, és fedett linkeken keresztül illegális oldalakra, illegális tevékenységekhez juthatunk el. A darknet a gyermekpornográfiával kapcsolatos internetes oldalak használatát elősegíti, támogatva ezzel a gyermekek internet alapú szexuális kizsákmányolását.



3. diagramm: iOCTA jelentések a kiberbűnözés tükrében 2016; Forrás: A szerző (iOCTA jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

Az iOCTA soron következő jelentése a 2016-os évből származik. 2014., és 2015. évekhez hasonlóan a bűncselekményi kategóriák nagy változáson nem mentek keresztül. A gyermekek internetes szexuális kizsákmányolása, a darknet rendszerek támogatásával szinte mindennapos. Nap, mint nap újabb és újabb oldalak jelennek meg, amelyek a világhálót a gyermekpornográfiával beterítik. 2016. év újdonsága, a kiberterrorizmus fogalmának megjelenése. Olyan zsarolóvírusok, amelyek nagyrésze közintézmények számítástechnikai rendszereit támadják meg, és leginkább anyagi ellenszolgáltatást követelnek. Évről évre a régi veszélyek mellett újabb és újabb fenyegetésekkel vagyunk kénytelenek szembesülni. Mindannyiunk közös érdeke, hogy ezeket a veszélyforrásokat megszüntessük.

A következő fejezetben egy olyan nemzetközi szervezet munkáját mutatom be, amelyik a gyermekpornográfia elleni küzdelem élharcosa, a hálózat tevékenységének ideje alatt több ezer darkneten keresztül elérhető gyermekpornográf oldalt sikerült azonosítaniuk, majd elkövetőiket az igazságszolgáltatás elé állítaniuk.

3.2.2 INHOPE

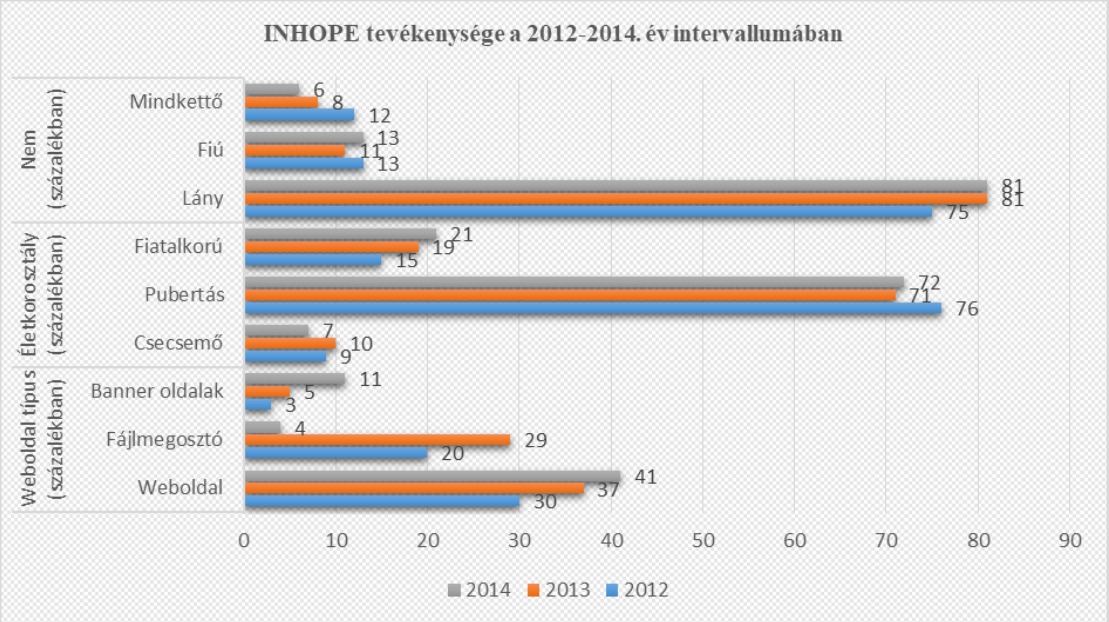
Az internethasználat a lakosság mindennapi életére közvetlen hatással van, a kommunikáció módját, az üzleti tevékenységet, valamint az életmódot is megváltoztatja, egyre több gyermek és serdülő használ online technológiát az otthonában vagy az iskolában. Mivel vannak olyanok, akik ezt a technológiát illegális tevékenységekre, különösen a gyermekek szexuális visszaélésével kapcsolatos anyagok terjesztésére, birtoklására, és megosztására használják, ezért az állami szerveknek nagy felelősségük van abban, hogy - a felnőtteket, a szülőket, a tanárokat, és mindenkit, aki ebben érintett - annak veszélyeiről is tájékoztassák. Az Európai Unió különböző szervei nagymértékben hozzájárultak ahhoz, hogy az internetet biztonságosabb közeggé varázsolják, de ez nem jelenti azt, hogy a veszély teljes mértékben megszűntetésre került, és további intézkedésre ne lenne szükség.

Az Internetes Forródrótok Nemzetközi Szövetségét (az INHOPE-ot, azaz az „International Association of Internet Hotlines-t") 1999-ben alapították, abból a célból, hogy egy olyan globális hálózatot hozzon létre, és koordináljon, amely az internetet-használatát biztonságosabbá teszi, az illegális tartalmakra pedig kellő időben, és kellő hatással reagál. Mindennek megvalósítását az Európai Bizottság a „biztonságosabb internet" programjának keretében nyújtott támogatásból valósíthatták meg.[251] A szervezet az internetes pedofil tartalmak eltávolításának az élharcosa, elkötelezett a gyermekek internetes szexuális visszaéléseinek, bántalmazásainak leküzdésére indított prevenció mellett. Feladata, hogy olyan felületet hozzon létre, és kezeljen, ahol bárkinek lehetősége van arra, hogy amennyiben az interneten olyan a gyermekek szexuális visszaéléseivel kapcsolatos anyagot talál, amely megítélése szerint illegális, és törvénysértő, akkor bejelentését névtelenül megtehesse. Az ügynökség az ügyet kivizsgálja, majd amennyiben annak jogellenessége megállapítást nyer, a megfelelő rendészeti szervnek azt átadja. A bejelentések nyomán gyakran rendőri akciók indulnak, az áldozatokat sikerül azonosítani, helyzetükből kiszabadítani, és gyakorta sikerül a tetteseket kézre keríteni. Mindemellett csökkenti a jogellenes tartalmakat és megoldást keres az online káros viselkedésformák problémájára. Ahol lehetőség nyílik az online jogellenes

[251] A program célja a gyermekek online környezeten belüli védelmének fokozása. A program, amely a legújabb kommunikációs szolgáltatásokat (például a társasági hálózatokat) is felöleli, nem csak a jogellenes tartalmak ellen veszi fel a harcot, de az olyan káros viselkedésformák ellen is, mint a zaklatás vagy a bizalmaskodás is fellép.

tartalmak és káros viselkedésformák bejelentésére - különös tekintettel a gyermekek szexuális bántalmazásához kapcsolódó anyagokra és a bizalmaskodásra - lépéseket tesz annak érdekében, hogy a nyilvánosság számára az úgynevezett nemzeti kapcsolattartási pontok elérhetővé váljanak. Elősegíti a biztonságosabb online környezet kialakítását: ösztönzi a tagállamok önszabályozási kezdeményezéseit, illetve a gyermekek és fiatalok részvételét a biztonságosabb online környezet létrehozásában - az ifjúsági testületek révén - fokozza. A lakosság tudatosságát biztosítja. A kapcsolattartási pontok létrejöttét támogatja, ahol a szülők és a gyermekek az internet biztonságos használatára vonatkozó tanácsadásban részesülhetnek. Olyan tudásalapot hoz létre, ami az új technológiák gyermekek általi használatáról, ezek által a gyermekekre kifejtett hatásokról, valamint a kapcsolódó kockázatokról tudósítanak. Mindezt felhasználja annak érdekében, hogy a biztonságosabb internet programon belül jelenleg folyó intézkedések hatékonyságát javítsa. 2010-ben az INHOPE Egyesület, és Alapítvány jótékonysági szervezetek segítségével olyan innováción alapuló fejlesztési tevékenységet indított meg, amely arra irányult, hogy az olyan feltörekvő országokban, ahol a finanszírozás és a jogi szabályozás hiányzik, a gyermekek szexuális kizsákmányolása ellen forródrótokat hozhassanak létre. Eredményeképpen a fejlesztéshez egyre több uniós tagország csatlakozik.

A következő grafikonon az INHOPE eddig ismertetett, és statisztikai mérőszámokkal alátámasztott tevékenységét mutatom be.



3. diagramm: INHOPE tevékenysége a 2012-2014. év intervallumában; Forrás: A szerző (INHOPEjelentéseinek számadataiból összeállított) kutatásának ábrázolása.

Az INHOPE aktív tevékenységének köszönhetően 2012. évben 37404-, 2013. évben 54962-, és végül 2014. évben 89758 darab tiltott/illegális gyermekpornográfiával érintett linket sikerült az internetről eltávolíttatni. Ez az adott évek szerinti lebontásban a weboldalak 30-, 37-, és 41-, a fájlmegosztó hálózatok 20-, 29-, 4-, és a banner oldalak 3-, 5-, és 11 százalékát jelentette. Az életkorosztály tekintetében a vizsgált időszakokban a megosztott tartalmak a csecsemők 9-, 10-, 7-, a pubertáskorúak 76-, 71-, 72-, és a fiatalkorúak 15-, 19-, és 21 százalékát érintette. A nem szerinti megoszlás tükrében a megosztott tartalmak a kislányok vonatkozásában 75-, 81-81-, a kisfiúk vonatkozásában 13-, 11-, 13-, és olyan anyagok esetén, amelynél mindkettő jelen volt 12-, 8-, és 6 százalékban voltak érintettek.

Összegzésképpen megállapítást nyert, hogy az Európai Unió nagy hangsúlyt fektet arra, hogy a gyermekek egészséges testi-, lelki-, és szellemi fejlődését biztosítsa. Kijelenthetjük, hogy a gyermekpornográfiával-, és a gyermekek internetes szexuális visszaéléseivel kapcsolatos intézkedések különböző szervek, és/vagy szervezeti egységeken keresztül megtételre kerülnek. Az így létrehozott iOCTA, INHOPE rendszerek olyan számadatokkal szolgáltak, amelyek a gyermekpornográfia, így különös tekintettel a gyermekek szexuális célú kizsákmányolásával érintett internetes bűncselekményekről valós képet adhattak. Bár a számstatisztika csak az eddig felderített sértettek, és bűncselekmények vonatkozásában mérhető, a látenciában maradt adatok ezt a képet negatív/pozitív irányban még befolyásolhatják/befolyásolhatnák. Az így kapott eredmények viszont azt tükrözik, hogy a gyermekek szexuális célú internetes kizsákmányolása, a gyermekpornográfia bűncselekmények száma európai viszonylatban rendkívül magas, potenciális veszélyt a pubertás gyermekekre, azon belül pedig leginkább a kislányokra jelentenek, de rohamosan emelkedik a csecsemők-, és fiatalkorú sértettek száma is. Az európai unió tagországaiból számos állampolgár érintett, akik a sértetti kört erősítik. Az arányszámok között néhol csökkenés-, néhol emelkedés mutatható ki, amely összességében egy stagnáló értéket produkál. Tekintettel arra, hogy az európai viszonylatban a számadatokat megismerhettük, a következő fejezetrészben, és annak alfejezeteiben a magyar statisztikákkal, és a kutatási összehasonlítás eredményeivel ismerkedhetünk meg.

4. Kutatás

4.1 A kutatás tárgya

A kutatás tárgya a gyermekpornográfia bűncselekmények időszakos statisztikai vizsgálata, azaz azok statisztikai reprezentációinak feltárása. Nem egyszerűen egy leíró statisztikai elemzésről van szó, hanem nemzetközi-, és hazai számadatok hivatalos összevetéséről, időszerű elemző-értékelő vizsgálatáról. Mint, ahogy a korábbi fejezetben bemutatásra került, a gyermekek internetes szexuális kizsákmányolása egy olyan nemzetközi veszélyforrás, amely ellen nem egy, hanem a Föld összes országa fellépni köteles. Különböző bűncselekményekkel milliárdos nagyságrendű euró és/vagy dollár profitot termelnek, amely az országok gazdaságát, és becsléseink szerint több-milliós nagyságrendű ember életét teszi tönkre. A gyermekek internetes szexuális kizsákmányolása, azon belül is kiemelt veszélyként a gyermekpornográfia több ezer áldozatot szednek, amely ellen az uniós-, és nemzeti stratégiák bevethetők, az eredményorientáltság célja mellett pedig tovább fejleszthetők. A kutatás tárgykörét három részre bontottam fel: első helyen a nemzetközi-, második helyen a hazai statisztikai adatok reprezentációt-, majd legvégül azok eredményeit hasonlítottam össze. Mindazért, hogy a statisztikán alapuló uniós-, és nemzeti stratégiák jogi-, és szabályozási alkalmasságát-, alkalmazhatóságát empirikus alapon is meg lehessen vizsgálni, olyan módszert választottam, amely a hozzá fűzött igényeket maximálisan kielégíti.

Álláspontom szerint a statisztikai reprezentációktól (és mérési technikáktól) függően a vizsgált jelenség bizonyos attitűdjei, fontos tulajdonságai jelentőséggel felruházott úgy nevezett identitás-markerré léphetnek elő, így más jegyeket primer attribútumként háttérbe szoríthatnak, azok szekunder jellegzetességgé alakulnak. (Példának okáért: amennyiben a statisztikai összehasonlító vizsgálat eredményeképpen a fájlmegosztó rendszerek az illegális honlapokhoz képest kimagasló eredménnyel bírnak, úgy a többi elkövetési helyhez képest (például internetes link és/vagy banner) (feltéve, ha a módszerek között a Cohan féle skálán a korrelációs koefficiens érték is kimagasló) háttérbe szorulhatnak, és a fókusz a legmagasabb statisztikai eredménnyel szolgáló módszerre koncentrálódik. A mérések különböző technikái hozzájárulhatnak ahhoz, hogy a vizsgált jelenség bizonyos kategóriáit megszilárdítsák, bizonyos kategóriákat pedig (elenyésző számukra tekintettel) akár el is tüntessenek. Véleményem szerint, amennyiben a gyermekpornográfia bűncselekmények összetettségét,

okát, céljait, körülményeit, mibenlétét, funkcionális jellegzetességeit, dinamikáját meg szeretnénk ismerni, akkor minden részinformációra szükségünk lehet, amelyet a tudomány területén, a különböző empirikus módszerrel végzett kutatások biztosíthatnak. A tanulmány megírása során örömmel töltött el, hogy olyan statisztikai adatokkal dolgozhattam, amelyek hivatalos, nyílt, és hiteles forrásból származtak. A közhiteles forrás számstatisztikái nem hazudnak, így a realitás talaján maradva az eredmények, és az összehasonlítás végkifejlete is reális, megbízható, pontos, és objektív maradhat:

- közhiteles, hisz az adatok olyan nyilvántartásokból származtak, amelyek az adatkörre vonatkozó információk tekintetében, a felvétel-, módosítás-, és törlés funkciók használatában kizárólag jogszabály, és az erre feljogosított szerv kezelésében végezhetők; valamint az adatok generálása jogszabályban rögzített eljárási rend szabályai szerint, a kategorizált okiratok alapján történik, garantálva ezáltal az adathalmaz pontosságát, teljességét, és megbízhatóságát;
- reális, hisz kézzelfogható, valóságos, tényleges, gyakorlati adatokat tartalmaztak, és a fókuszjelenség valóságát tükrözték, amely kizárólag a vizsgálat tárgyán belüli számstatisztikán alapult;
- megbízható, mert az adatforrásra minden körülmény között számítani lehetett, kétségtelenül hiteles, tartósan igaznak bizonyult, céljának megfelelően viselkedett.
- objektív, hisz a vizsgálatot-, és azok eredményeit tárgyi körülmények határozták meg, a személyek hatókörén kívül állónak tekintett körülményektől függöttek; azt személyi szempontok, érzelmek, vélemények nem befolyásolták, pártatlanok, részrehajlás, és elfogultság nélküliek voltak.

A fentiekre azért fordítottam kiemelt hangsúlyt, mert amennyiben sikerül olyan nemzeti-, és esetleg uniós stratégia-fejlesztő, innovációs eljárást, ajánlást kidolgozni, amely a gyermekek internet alapú szexuális kizsákmányolását, visszaéléseit, és a gyermekpornográfia bűncselekmények vonatkozásában az eredményorientáltságot fejlesztheti, akkor mind a döntéshozók, mind a végrehajtók nap, mint nap ehhez a kerethez fognak viszonyulni, ezt fogják alkalmazni, ezért azok torz képet nem tükrözhetnek. A statisztikai számokat az emberek magatartása sokféleképpen alakíthatja, ezért is izgalmas, hogy nemcsak a magyar nemzeti-, hanem a többi tagállam, így az uniós nemzetközi aspektusról is képet kaphatunk, majd az egyik legfontosabb alapkérdésre -, miszerint vajon a magyar nemzeti-, és az uniós statisztikák egymással megegyeznek, egymástól különböznek, az egyezés-, és különbözőség mértéke közötti korreláció mértéke mekkora – választ kaphatunk.

4.2 A kutatás módszerei

Szerencsésnek érzem magam a tekintetben, hogy tudományos pályafutásom alatt számos kvalitatív, és kvantitatív módszert kipróbálhattam, és alkalmazhattam, amely bizonyos tudományágak (társadalomtudomány, rendészettudomány, hadtudomány) területén az általam választott, és tanulmányozott témákban új tudományos eredmények létrejöttét eredményezhette. Személy szerint a kvalitatív kutatási módszereket jobban kedvelem, a személyes konzultációk, megfigyelések, tapasztalatok, interjúk, kísérletek a szívemhez közelebb állnak, személycentrikusak, és énközpontúak. Mégis most a pályázati munka elkészítésekor e preferált hagyománnyal szakítottam, és a kvalitatív kutatási módszereket kvantitatív kutatási módszerekre-, fekete-fehér alapú statisztikai számításokra cseréltem. Bár Feyerabrend [2002] szerint, ez is csak boszorkányság, és még senki sem bizonyította, hogy a tudomány (különösen a statisztika) racionálisan járna el, mégis bátorkodtam kicsit a számok bűvöletében varázsolni.[252] Ahogy a híres Churchilli idézet is tartja: „Csak abban a statisztikában hiszek, amit én magam hamisítok”.[253] Komolyra fordítva a szót, vélhetőleg nem választottam volna ezt a kutatási metódust, ha nem olyan adatbázisokból dolgozok, amelyek a közhiteles, reális, megbízható, és objektív kritériumokkal szemben támasztott követelményeknek nem feleltek volna meg, és a számításaim, azok eredménye ezeknek a feltételeknek ellentmondanának. Hiszen nem elég, hogy egy jelenség vizsgálatakor megfelelő módszert választunk, a kapott eredményeket megfelelően kell tudnunk értelmeznünk is.

A statisztikát elsőkörben a matematikához, és más tudományágak határterületeihez kapcsolhatjuk. Annak tudományágak közötti elhelyezése, és besorolása viszont nem egységes. Vannak, akik szerint nem is tudomány, mert törvényszerűségeket a statisztika nem tud megfigyelni, ezért inkább nem tudománynak, hanem tudományos módszernek tekinthető. Más értelmezésben viszont ez azért sem helytálló, mert a módszertan kidolgozása, a kérdőívek megszerkesztése, a fogalomalkotás, és az adatkezelési folyamat is e tevékenységbe tartozik, így nem csak módszerként használható. A harmadik álláspont szerint a statisztika a gyakorlatban alkalmazott módszerek, és azok eredményeinek összefoglalását jelenti, így a társadalomtudományok közé sorolandó. (Ez azért vitatható, mert más tudományterületeket, például a természettudományokat kirekeszti.) A negyedik csoportba azok tartoznak, akik a

[252] FEYERABREND Paul: A módszer ellen. – Budapest: Atlantisz Kiadó, 2002.

[253] GILBERT Martin: Churchill: A life. – United States: Holt Paperbacks, 1992.

statisztikát saját fogalmakkal bíró, egységes módszertudományként kezelik.[254,255,256,257] AZ OTKA (Országos Tudományos Kutatási Alapprogram) a statisztikát a társadalomtudományokon belül a gazdaság- és jogtudományok közé helyezi. A kutatás módszerének felhasználása az objektív valóság feltárását, számszerű jellemzését tűzte ki célul, egy olyan megismerési folyamat részeként, amelynek alanya a vizsgálat tárgyához aktívan viszonyul, és a nyert ismereteket a valóságnak nem passzív képeiként, tükörszerű másolataiként, hanem az alkotói tevékenység eredményeiként értelmezi. Örömmel töltene el, ha új ismereteket tudnék sajátoméva tenni, új elméleteket tudnék kidolgozni, és a korábban jól bevált módszereket tovább fejleszthetném, az eredményeket tökéletesíthetném. Mindezekhez a statisztika segítségével kvantitatív eljárás keretén belül különböző függvények beágyazásával minimumot, maximumot, átlagot, móduszt, és szórást számítottam. Az alapstatisztikai számítások alapján kapott eredményeket pedig olyan összehasonlító kvantitatív eljárás fogta össze, amely a gyakoriságok közötti korrelációs koefficiens értékét a Cohan féle általános skálán illusztrálni tudta. A fentiekkel összhangban a statisztikai számításokat egyenként szeretném bemutatni.

I. Függvények:

a) Minimum függvény

Az adatok minimum függvénnyel történő vizsgálata különös matematikai számolást nem igényel. A vizsgált adatbázis során a legalacsonyabb-, legkisebb értékkel rendelkező elem kiválasztása szükséges, amely az adathalmaz minimum értéke lesz.

b) Maximum függvény

Az adatok maximum függvénnyel történő vizsgálata matematikai számolást szintén nem igényel. Tekintettel, hogy a maximum a minimum ellentéte, ezért a vizsgált adatbázisban a

[254] KORPÁS Attiláné: Általános statisztika. – Budapest: NTK, 1996.

[255] PETRES Tibor, TÓTH László: Statisztika. – Budapest: KSH, 2006.

[256] PUKLI Péter, VÉGVÁRI Jenő: A statisztika: tudomány és szakma. In. Statisztikai Szemle, 2004., 82. évf. 1. sz. – p.:5-30.

[257] KATONA Tamás, LENGYEL Imre, PETRES Tibor, CSENDES Tibor: Statisztikai ismerettár. – Szeged: JATEPress, 1999.

legmagasabb-, legnagyobb értékekkel rendelkező elemet kell kiválasztanunk ahhoz, hogy az adathalmaz maximum értékét megkaphassuk.

$$R = x_{\max} - x_{\min}$$

c) Átlag függvény

A számított középértékek, azaz átlagok az ismérvértékekből számíthatók ki. Számomra a számtani átlag bír jelentőséggel, de harmonikus-, mértani-, és négyzetes- átlagszámításra is van lehetőségünk. A számtani átlag számítása azért releváns, mert az ismérvértékeknek jelen esetben tárgyi értelme van A számtani átlagszámítás során így azt a számot kapjuk meg, amelyet az egyes átlagolandó értékek helyére írva, azok összegében változás nem következik be. Az egyszerű sokaság ismérvértékei számának a matematikai számítása a számtani (arimetikai) átlag a összegének, és az elemei hányadosai.[258] A függvény következő:

$$\overline{x} = \frac{x_1 + x_2 + x_3 + \ldots + x_N}{N}$$

d) Módusz függvény

Ha egyszerűen szeretnénk megfogalmazni, akkor móduszon nem értünk mást, mint az adatbázisban előforduló leggyakoribb adatot. Ezek a helyzeti középértékek az ismérvértékek közötti elhelyezkedésükkel adhatók meg. Az ismérvértékek e körül sűrűsödnek, tömörülnek. Diszkrét változó esetén a módusz a leggyakrabban előforduló ismérvérték, míg folytonos változó esetén a gyakorisági görbe maximumhelye. Egy adathalmaz eloszlása egy-, de többmóduszú is lehet, attól függően, hogy hány módusz van. Ha mindegyik ismérvérték csak egyszer fordul elő, akkor az eloszlásnak módusza nincs. A függvény matematikai számítása a következő:

[258] Megjegyezni kívánom, hogy az átlagfüggvény választásánál a négyzetes minimum tulajdonság nagyban motivált. Ez azt jelentette, hogy minden ismérvérték számtani átlaggal való helyettesítésekor elkövetett előjeles hibák kiegyenlítik egymást, vagyis az egyes ismérvértékek számtani átlagtól való eltéréseinek összege 0. Illetve minden ismérvérték számtani átlaggal való helyettesítésekor elkövetett hibák négyzetösszege minimális lesz; és fordítva: a számtani átlag az a konstans, amely esetén a négyzetes hiba minimális. Az átlagfüggvény szintén biztosítja a torzításmentes képet.

e) Szórás függvény

Az ismertetett függvények, így különösen a középértékek az adatbázist egyetlenegy számmal is képesek jellemezni, de olykor ez igen kevés információnak tűnik. Ezért van szükség arra, hogy az ismérvértékek szóródását is kiszámítsuk. Szóródáson nem értünk mást, mint az egyes ismérvértékeknek egymástól, illetve valamely nevezetes középértéktől való eltérését. A szóródás terjedelme a legnagyobb és a legkisebb ismérvérték közötti különbség. A függvény matematikai számítása a következő:

$$Mo = mo + \frac{k_1}{k_1 + k_2} \cdot h$$

A szórás a szóródás mérőeszköze. A szórás az ismérvértékek számtani átlagtól vett különbségeinek négyzetes átlaga. A szórás nem súlyozott, és súlyozott képlete a következő:

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \ldots + (x_N - \bar{x})^2}{N}}$$

$$\sigma = \sqrt{\frac{x_1^2 + x_2^2 + \ldots + x_N^2}{N} - \bar{x}^2}$$

$$\sigma = \sqrt{\bar{x}_q^2 - \bar{x}^2}$$

$$\sigma = \sqrt{\frac{f_1 \cdot (x_1 - \bar{x})^2 + f_2 \cdot (x_2 - \bar{x})^2 + \ldots + f_N \cdot (x_N - \bar{x})^2}{N}}$$

$$\sigma = \sqrt{\frac{f_1 \cdot x_1^2 + f_2 \cdot x_2^2 + \ldots + f_N \cdot x_N^2}{N} - \bar{x}^2}$$

$$\sigma = \sqrt{\bar{x}_q^2 - \bar{x}^2}$$

II. Cohan féle korrelációs koefficiens érték

A gyermekek internet alapú szexuális kizsákmányolásának, visszaéléseinek, és a gyermekpornográfia bűncselekmények statisztikai mutatóinak vonatkozásában a hatásnagyság mérésének rendkívül fontos szerepe van.[259] A hatásnagyság mérésével hipotéziseimet tesztelhettem, valamint segített abban is, hogy az összehasonlításon alapuló eredmény szignifikáns értékét kimutathassam. Ahhoz, hogy a hatásnagyságot mérhessem, korrelációs

[259] A statisztikában a hatásnagyság a vizsgált jelenség erősségét szimbolizáló kvantitatív mutató, azaz két változó közötti korreláció, regressziós együttható, átlagos különbség, vagy akár annak a kockázata, hogy valami bekövetkezik, vagy sem. Minél nagyobb a vizsgált jelenség statisztikai mutatóinak abszolút értéke, a hatásnagyság annál erősebb.

számításokra volt szükségem. (A matematikai statisztikában a korreláció két tetszőleges érték közötti lineáris kapcsolat nagyságát, és irányát, azok egymáshoz való viszonyát jelzi.)[260] A dolgozatban így lehetőségem volt arra, hogy több változót több változóval összevessek. Megnézhettem, hogy a gyermekek internet alapú szexuális kizsákmányolása, visszaélései, és a gyermekpornográfia bűncselekmények nagysága európai (uniós)-, és hazai viszonylatban hogyan alakul, de elvégezhettem a hazai-, nemzeti évek során összegyűjtött, elemzett-, és értékelt számadatokat összehasonlító vizsgálatát is. Alapvető kérdésem volt tehát, hogy az európai-, és a magyar-, azaz nemzeti adatok között áll-e fent kapcsolat (logikusan igen, hisz a magyar statisztika az európai uniós statisztika részét képezi), amennyiben a kapcsolat fennáll, és a válasz igenlő, úgy a két változó között egyenes-, fordított arányú- vagy hiányzó kapcsolat (pozitív, negatív vagy nem létező korreláció) áll fenn, azok mértéke pedig mekkora értéket képvisel. Szükséges tisztázni, hogy, ha nincs lineáris korreláció, akkor a korrelációs koefficiens értéke: 0, tökéletes pozitív, ill. negatív lineáris korreláció fennállása esetén a korrelációs koefficiens értéke +1,00, ill. -1,00. Ennek értéke független a mértékegységtől, amelyekben a két változó meghatározásra került. A korreláció nem jelent feltétlen ok-okozati kapcsolatot, mert ez lehet annak a következménye, hogy az x tengelyre felvett változó befolyásolja az y tengelyre felvettet, az y tengelyre felvett változó befolyásolja az x tengelyre felvettet, így egyik eset sem áll fenn, hanem egy harmadik tényező mindkettőt egy irányba (pozitív korreláció) vagy különböző irányokba (negatív korreláció) mozdítja el.[261],[262] A korreláció számítása az alábbi matematikai képlettel volt lehetséges:

$$r = \frac{n \cdot \sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{\left(n \cdot \sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2 \right) \left(n \cdot \sum_{i=1}^{n} y_i^2 - (\sum_{i=1}^{n} y_i)^2 \right)}} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2 \sum_{i=1}^{n} (y_i - \bar{y})^2}}$$

[260] VARGHA András: Matematikai statisztika pszichológiai nyelvészeti és biológiai alkalmazásokkal. Budapest: Pólya Kiadó, 2000.

[261] ZÁVOTI József: Matematikai statisztikai elemzések 5., Kapcsolatvizsgálat: asszociáció, vegyes kapcsolat, korrelációszámítás. Varianciaanalízis (egyszeres osztályozás). – Nyugat-Magyarország Egyetem, TAMOP 4.2.5 pályázata, 2010.

[262] KOVÁCS István: Gésa kultúra, és japán prostitúció. In: Hadtudományi Szemle, 2017., 10. évf. 2. sz. – p.:447-COHEN Jacob: Statistical Power Analysis for the Behavioral Sciences. – New Jersey: Lawrence Erlbaum Associates, 1988.

A képlettel végzett számítások tekintetében a Cohan féle skála a korreláció mértékét mutatta meg, attól függően, hogy az kicsi (r=0,10), közepes (r=0,30), vagy nagy (r>0,50) értéket képviselt.[263] A következő fejezetben a kutatási mintát, azaz azt a nemzetközi-, és hazai forrásadatbázist mutatom be, amelyek a statisztikai adatokkal való számítások alapját megteremtették.

4.3 A kutatási minta

Egy kvalitatív kutatás mindig közvetlenül a személlyel foglalkozik, a kutató a kísérleti alanyhoz hasonul, az elmondottakat, a megélt élményeket magáénak érezheti. Interjúkészítéssel például átélheti mindazt, amit az interjú alanya megoszt, kísérletnél pedig például a vizsgált környezet részese, és/vagy része lehet. Számomra ezek az élmények a kutatás során hiányoztak. Egy kvantitatív kutatásnak mindig közvetett alanyai vannak, a kutatás ettől válik személytelenné. Azok a statisztikai számok, amelyekkel jelen tanulmány elkészítésekor is dolgozom egy-egy embert, egy-egy sorsot szimbolizálnak. Sajnos a matematika világában ezek a sorsok nem mások, mint számok. Számok, amik statisztikát képeznek. Statisztikát, amiből konklúzionálhatnak. De ezek az emberek, akik nap, mint nap szenvednek, és a megélt élményeik még álmukban is kísértik őket nem érdemlik meg azt, hogy egyszerű számokká, statisztikává avanzsáljuk őket. A fentiek figyelembevételével ezért, ha a kutatási mintát – tőlem független okok miatt - nem is, de legalább a javaslatokat megpróbáltam emberközpontúvá, és emberbaráttá tenni.

A kutatási minta olyan statisztikai adatbázisok számadataira épült, mint az iOCTA-, és INHOPE jelentések, valamint a magyar rendőrség nyilvános, és az állampolgárok által is elérhető, a közvélemény számára is megismerhető statisztikai forrásai.[264],[265],[266],[267],[268] A

---

[263] COHEN Jacob: Statistical Power Analysis for the Behavioral Sciences. – New Jersey: Lawrence Erlbaum Associates, 1988.

[264] The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2014. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014), (Letöltés ideje: 2017. augusztus 20.)

[265] The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2015. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015), (Letöltés ideje: 2017. augusztus 20.)

iOCTA-, és INHOPE jelentések statisztikai adatai a korábbi fejezetekben feldolgozásra kerültek, az összehasonlítás alapját többek között ezek az adatok képzik majd. Az elemzett adatok az oldalak, bannerek, fájlmegosztók számát, a sértettek nem-, és korbeli megoszlását is tartalmazták. A magyar statisztikák a 2012-2016. időszakra vonatkozóan egyrészt az összes regisztrált büntetőeljárást, bűnelkövetőt, sértettet, azok település-, és életkor szerinti eloszlását-, másrészt pedig ugyan ilyen metodológia szerint a gyermekek internet alapú szexuális kizsákmányolásának, visszaéléseinek, és a gyermekpornográfia bűncselekményeknek az eljárásait, sértettjeit, elkövetőit tartalmazták. A táblázatok számadatainak igényes feldolgozása lehetővé tette, hogy mind nemzetközi- (uniós), mind a hazai (nemzeti) statisztikai adatbázisokat elemezhessem-értékelhessem, azokat megfelelő módon, és minőségben összehasonlíthassam, és a kapott eredmények alapján a hazai stratégia fejlesztésének javaslatára kísérletet tegyek, és az uniós bűnüldözési célok elérésének maximalizálásához a magyar rendvédelem hozzájárulhasson.

---

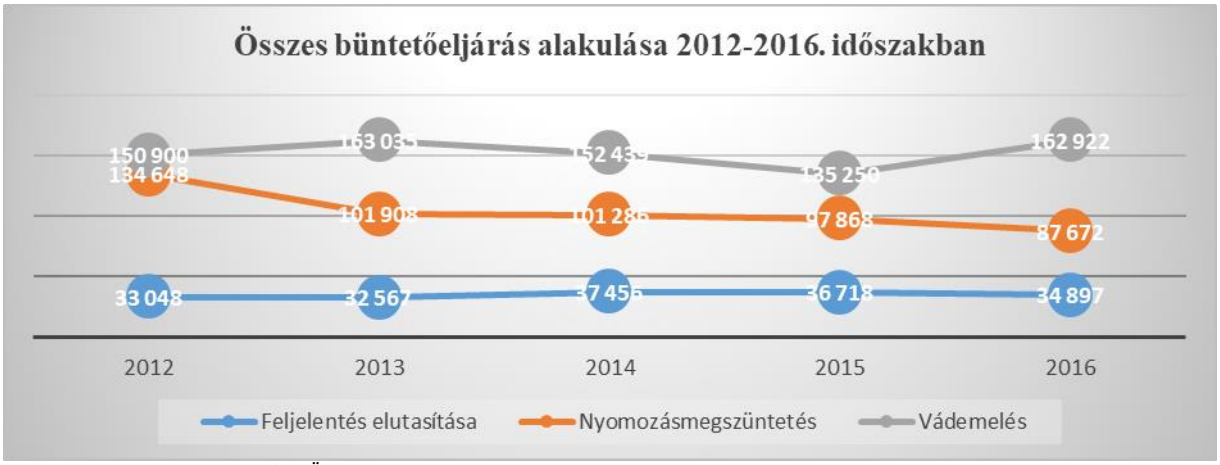
[266] The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2016. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016), (Letöltés ideje: 2017. augusztus 20.)

[267] The International Association of Internet Hotlines (INHOPE) report 2012-2014. (http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx), (Letöltés ideje: 2017. augusztus 20.)

[268] Magyar rendőrség – bűnügyi statisztikák (http://www.police.hu/hu/a-rendorsegrol/statisztikak/bunugyi-statisztikak), (Letöltés ideje: 2017. július 18.)

4.4 Kutatási adatfeldolgozás

4.4.1 Összes büntetőeljárás

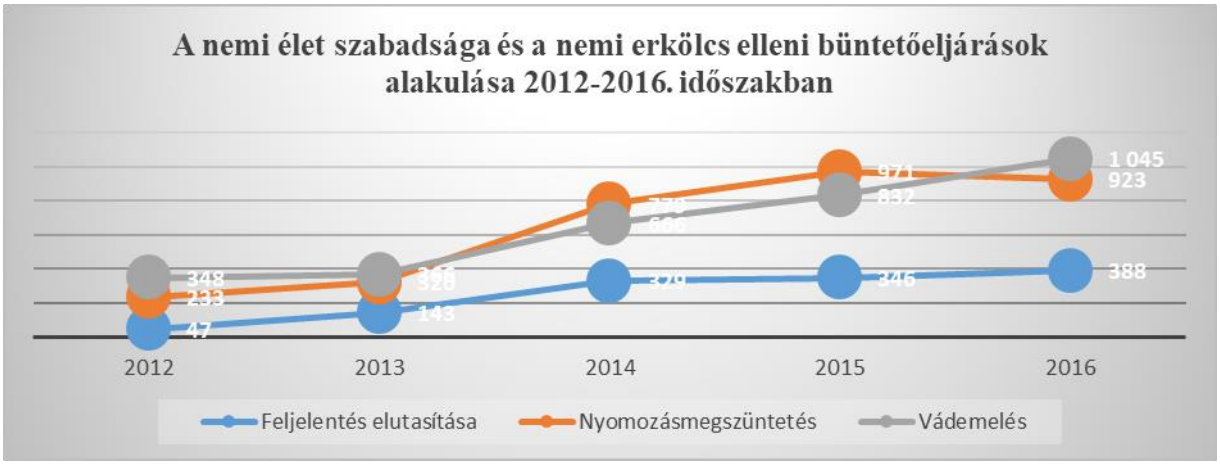


4. diagram: Magyar rendőrség statisztika; Összes büntetőeljárás alakulása 2012-2016. időszakban; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása.

Az összes büntetőeljárás tekintetében kizárólag a feljelentés elutasítása, a nyomozások megszüntetése, valamint a vádemelési javaslattal megküldött büntetőeljárások kerültek vizsgálatra. Összességében e számadatok szerint az adatbank 2012-2016. intervallumban 1 462 614 ügyet regisztrált. A feljelentések elutasítására 2012-ben 33048-, 2013-ban 32567-, 2014-ben 37456-, 2015-ben 36718-, 2016-ban pedig 34897 esetben került sor. A nyomozás megszüntetését 2012-ben 134648-, 2013-ban 101908-, 2014-ben 101286-, 2015-ben 97868-, 2016-ban pedig 87672 esetben regisztrálták. A vádemelési javaslattal megküldött ügyeket 2012-ben 150900-, 2013-ban 163035-, 2014-ben 152439-, 2015-ben 135250-, 2016-ban pedig 162922 esetben vették lajstromszámba. Az összes büntetőeljárás 2012. év 2013. évhez képest 7-, 2013. év 2014. évhez képest 3-, 2014. év 2015. évhez képest 8 százalékkal csökkent, míg 2015. év 2016. évhez képest 6 százalékkal nőtt. A minimum, és maximum skála feljelentés elutasítása során 32567 és 37456-, nyomozás megszüntetése során 87672, és 134678-, vádemelési javaslat során pedig 135250, és 163035 értékek között mozgott. A legtöbb vádemelés 2016-ban, legkevesebb 2015-ben volt. A legtöbb nyomozás megszüntetés 2012-ben, a legkevesebb 2016-ban volt. Feljelentés elutasítására legtöbbször 2014-ben, legkevesebbszer 2013-ban került sor. Az átlagszámítás szerint 4 éves intervallumban a

feljelentés elutasításának átlaga 34937-, a nyomozás megszüntetésének átlaga 104676-, a vádemelési javaslattal megküldött ügyek átlaga pedig 152909 darabszámú volt. Módusz-számításra lehetőség nem volt, hisz ugyan azt az érték kétszer nem szerepelt. A szórás értéke feljelentés elutasítása esetén 2162,41-, nyomozás megszüntetés esetén 17698,58-, vádemelési javaslat esetén pedig 11389,61 volt.

4.4.2 A nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások

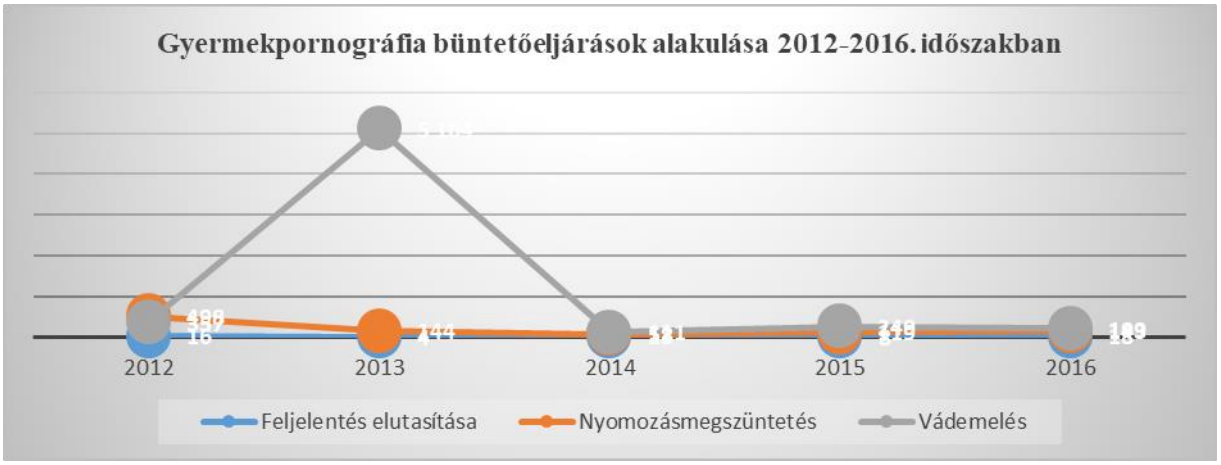


5. diagram: Magyar rendőrség statisztika; A nemi élet szabadsága és a nemi erkölcs elleni büntetőeljárások alakulása 2012-2016. időszakban; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása.

A nemi élet szabadsága, és a nemi erkölcs elleni bűncselekmény tekintetében is a nyomozások megszüntetése, a vádemelési javaslatok száma, valamint a feljelentések elutasítása került vizsgálatra. (Fontos kritérium, hogy a gyermekpornográfia külön kategóriát képvisel, ezért annak számadatai a csoportban feltüntetésre nem kerültek.) E három kategóriában 2012. és 2016. évek között összesen 7736 eljárás került lezárásra. A feljelentések elutasítására 2012-ben 47-, 2013-ban 143-, 2014-ben 329-, 2015-ben 346-, 2016-ban pedig 388 esetben került sor. A nyomozás megszüntetését 2012-ben 233-, 2013-ban 320-, 2014-ben 779-, 2015-ben 971-, 2016-ban pedig 923 esetben regisztrálták. A vádemelési javaslattal megküldött ügyeket 2012-ben 348-, 2013-ban 366-, 2014-ben 666-, 2015-ben 832-, 2016-ban pedig 1045 esetben vették lajstromszámba. 2012. év 2013. évhez képest 25-, 2013. év 2014. évhez képest 54-, 2014. év 2015. évhez képest 18-, és 2015. év 2016. évhez képest 9 százalékos emelkedést mutatott. A feljelentés elutasítása minimum és maximum értéke 47 és 388-, a nyomozás megszüntetésének minimum és maximum értéke 233 és 971-, a vádemelési

javaslattal lezárt ügyek minimum és maximum értéke 348 és 1045 értékek között mozgott. Feljelentés elutasítása tekintetében a legkisebb értéket 2012-ben, a legnagyobb értéket pedig 2016-ban mértem. Nyomozás megszüntetése esetében a legalacsonyabb érték szintén 2012-ben, a legmagasabb érték pedig 2015-ben realizálódott. A vádemeléssel érintett ügyek tekintetében a leggyengébb évnek szintén a 2012-es, legerősebb évnek pedig a 2016-os év sikerült. Módusz számításra egy esetben sem volt lehetőség, mert az évek különböző értékeket képviseltek, megegyező adat nem merült fel. A szórás értéke feljelentés elutasítása során 147,61-, nyomozás megszüntetése esetében 345,28-, vádemelési javaslattal lezárt ügyekben pedig 300,52 volt. Átlagosan a 2012-2016. közötti időszakban feljelentés elutasítására 250,6-, nyomozás megszüntetésére 645,2-, és vádemelési javaslattal megküldött ügyekre 651,4 esetben került sor.

4.4.3 Gyermekpornográfia büntetőeljárások



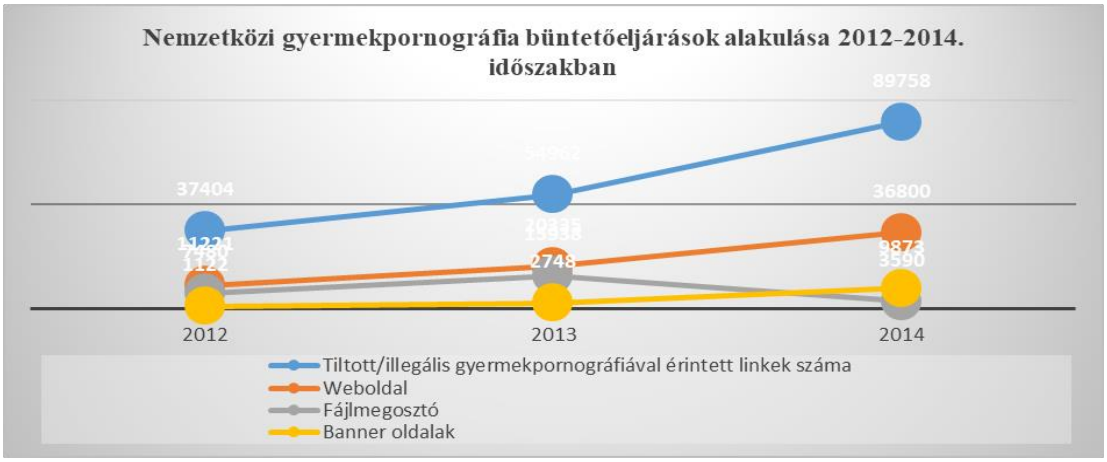
6. diagram: Magyar rendőrség statisztika; Gyermekpornográfia büntetőeljárások alakulása 2012-2016. időszakban; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása

A gyermekpornográfia bűncselekmény tekintetében is a nyomozások megszüntetése, a vádemelési javaslatok száma, valamint a feljelentések elutasítása került vizsgálatra. E három kategóriában 2012. és 2016. évek között összesen 7041 eljárás került lezárásra. A feljelentések elutasítására 2012-ben 16-, 2013-ban 4-, 2014-ben 13-, 2015-ben 8-, 2016-ban pedig 18 esetben került sor. A nyomozás megszüntetését 2012-ben 498-, 2013-ban 144-, 2014-ben 58-, 2015-ben 119-, 2016-ban pedig 143 esetben regisztrálták. A vádemelési javaslattal megküldött ügyeket 2012-ben 357-, 2013-ban 5104-, 2014-ben 11-, 2015-ben 249-, 2016-ban pedig 199 esetben vették lajstromszámba. 2012. év 2013. évhez képest 84

százalékos növekedést, 2013. év 2014. évhez képest 72 százalékos csökkenést, 2014. év 2015. évhez képest 52 százalékos növekedést, és 2015. év 2016. évhez képest 1 százalékos csökkenést mutatott. A feljelentés elutasítása minimum és maximum értéke 4 és 18, a nyomozás megszüntetésének minimum és maximum értéke 58 és 498-, a vádemelési javaslattal lezárt ügyek minimum és maximum értéke 111 és 5104 értékek között mozgott. Feljelentés elutasítása tekintetében a legkisebb értéket 2013-ban, a legnagyobb értéket pedig 2016-ban mértem. Nyomozás megszüntetése esetében a legalacsonyabb érték 2014-ben, a legmagasabb érték pedig 2012-ben realizálódott. A vádemeléssel érintett ügyek tekintetében a leggyengébb évnek szintén a 2013-as, legerősebb évnek pedig a 2014-es év sikerült. Módusz számításra egy esetben sem volt lehetőség, mert az évek különböző értékeket képviseltek, megegyező adat nem merült fel. A szórás értéke feljelentés elutasítása során 5,76-, nyomozás megszüntetése esetében 174,37-, vádemelési javaslattal lezárt ügyekben pedig 2181,97 volt. Átlagosan a 2012-2016. közötti időszakban feljelentés elutasítására 11,8-, nyomozás megszüntetésére 192,4-, és vádemelési javaslattal megküldött ügyekre 1204 esetben került sor.

4.4.4 Nemzetközi gyermekpornográfia büntetőeljárások

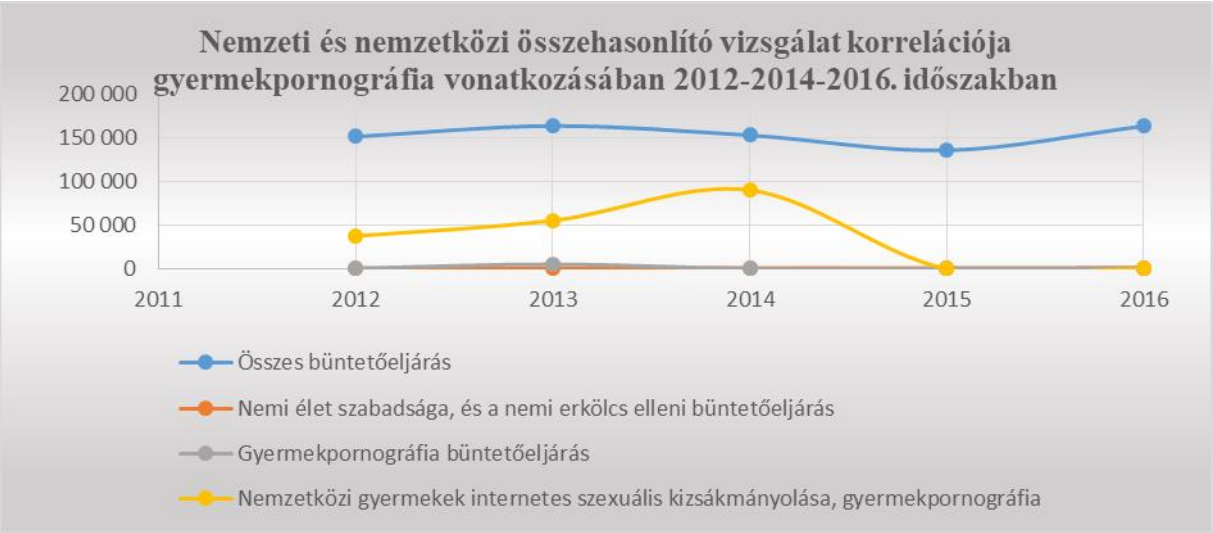
A gyermekek internetes szexuális kizsákmányolásával kapcsolatosan, a gyermekpornográfia uniós és/vagy nem uniós országok lefolytatott büntetőeljárásainak viszonylatában az INHOPE jelentéseket vettem alapul. Ha elfogadjuk azt, hogy az INHOPE tevékenysége a rendőri eljárások alapját képezik – bejelentés, INHOPE vizsgálat, majd rendőrségi eljárás, eredmény pedig annak függvényében a honlapok eltávolítása, az elkövetők felelősségre vonása -, akkor a 2012-2014. időszakból adatok állnak rendelkezésre. ezek az adatok a későbbi fejezetekben részletezett összehasonlítás adatbázisát adhatják.



7. diagram: INHOPE; Nemzetközi gyermekpornográfia büntetőeljárások alakulása 2012-2014. időszakban; Forrás: A szerző (INHOPE jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

A vizsgált időszak számadatait tekintve az INHOPE tevékenységének köszönhetően összesen 182124 darab gyermekek szexuális kizsákmányolásával kapcsolatos, gyermekpornográfiával érintett internetes link került eltávolításra. Ha a fenti logikai rendszert követjük, akkor ez logikailag ugyan ennyi büntetőeljárást, elkövetőt, és megannyi sértettet prognosztizál. A számadatok legalacsonyabb értékét 2012-ben, a legmagasabbat 2014. években mértem. 2012-ben 37404-, 2013-ban 54962-, majd 2014-ben 89758 darab olyan internetes gyermekek szexuális kizsákmányolásával kapcsolatos gyermekpornográfiával érintett link került eltávolításra, amely súlyos visszaélésekre adott lehetőséget. Ezekből 2012-ben 11221 darab weboldal, 7480 darab fájlmegosztó, és 1122 darab banner került betiltásra. 2013-ban ezek az adatok a weboldalak számában 20335 darabra-, a fájlmegosztók tekintetében 15938 darabra-, és a bannerek viszonylatában 2748 darabra emelkedtek. Az utolsó év vizsgálata megmutatta, hogy újabb növekedés érhető el: a betiltott weboldalak 36800 darabra-, a bannerek 9873 darabra emelkedtek, emellett 3590 fájlmegosztó is eltávolításra került. Minden év az előző évekhez képest emelkedő tendenciát mutatott. 2012. év 2013. évhez képest 47-, 2013. év 2014. évhez képest 63 százalékos emelkedést tudhat magáénak. A három év alatt átlagosan 60708 illegális, és tiltott link került beszüntetésre, a szórás mértéke 26645,78 volt. Módusz számításra nemzetközi viszonylatban sem volt lehetőség, mert ugyan olyan értéket egyik évben sem sikerült regisztrálni.

4.4.5 Az összes-, a nemi élet szabadsága, és a nemi erkölcs elleni-, a gyermekpornográfiával érintett büntetőeljárások hazai (nemzeti)-, és nemzetközi (uniós) összehasonlítása, azok eredményei



8. diagram: INHOPE; Magyar rendőrség statisztika; Nemzeti és nemzetközi összehasonlító vizsgálat gyermekpornográfia 2012-2014. időszakban; Forrás: A szerző (INHOPE jelentéseinek és a rendőrség számadataiból összeállított) kutatásának ábrázolása.

Az összehasonlítás során azok a számadatok kerültek vizsgálat alá, amelyek a nyomozások eredményességét tükrözték, így a korrelációs számításokat a vádemelési javaslattal zárt ügyek tekintetében végeztem el. Az összes büntetőeljárás vádemeléssel történt befejezése 764546-, a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások 3257-, a gyermekpornográfia büntetőeljárásai 6020-, és a nemzetközi gyermekek internetes szexuális kizsákmányolása, a gyermekpornográfia 182124 darab eljárást jelentett (és az is csak 3 év intervallumára értendő). Az összes vádemelési javaslattal lezárt büntetőeljáráshoz viszonyítva a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások 1,2-, a gyermekpornográfia 0,7 százalékát teszi ki a váderedményességnek. Ha a fenti nemzetközi színtérre vonatkozó számítási hipotézist elfogadjuk, akkor ahhoz mérten a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások 5-, a nemzeti gyermekpornográfia bűncselekmények vádeljárásainak 3,3 százalékát teszik ki. Ez relatív viszonyítási arányszám tekintetében alacsony értéket képvisel. A gyermekpornográfia büntetőeljárásai 2012-ben 2-, 2013-ban 70 százalékkal magasabb vádemelési arányt produkáltak, mint az összes nemi élet szabadsága, és nemi erkölcs elleni büntetőeljárások vádjavaslatai. Ugyan ez a 2014., 2015., 2016-os évről nem mondható el, ahol a fordított arány 16, 29, és 19 százalékos mutatóval rendelkezett. A Cohan

féle skálán a korrelációs koefficiens értéke az összes büntetőeljárás, és a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások tekintetében -0,11. A nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások, és a gyermekpornográfia tekintetében -0,54. Az összes büntetőeljárás, valamint a gyermekpornográfia tekintetében 0,48, a nemzetközi gyermekek internetes szexuális kizsákmányolása, gyermekpornográfia, valamint a nemzeti gyermekpornográfia tekintetében 0,25. Két tökéletesen negatív, és tökéletesen pozitív korrelációs értéket kaptunk. A Cohan féle skálán két érték szembetűnő, amelynél a korreláció majdnem közepes, és majdnem nagy. Az összes büntetőeljárás, valamint a gyermekpornográfia tekintetében a korrelációs együttható majdnem nagy, a nemzetközi gyermekek internetes szexuális kizsákmányolása, gyermekpornográfia, valamint a nemzeti gyermekpornográfia tekintetében majdnem közepes.

Az alfejezet összegzéseképpen megállapítást nyert, hogy Magyarország büntetőeljárásainak feljelentés elutasításával, nyomozás megszüntetésével, és a vádemelési javaslattal lezárt eredményei tekintetében a nemi élet, és szabadság elleni büntetőeljárások az összes büntetőeljárás 1 százalékát jelentik. Országos viszonylatban ezek a számok nem jelentik azt, hogy hazánk igen fertőzött, vagy veszélyeztetett volna, azonban minél részletesebb a vizsgálat, annál inkább látszik annak ambivalenciája. A nemi élet szabadság fejezetén belül a gyermekpornográfiával érintett büntetőeljárások száma viszont már 47 százalékot ölelt fel. Ez azt jelenti, hogy a három kategóriában a nyomozó hatóság által a Büntető Törvénykönyv e fejezetébe ütköző bűncselekmények tekintetében 47 százalékos aránnyal gyermekpornográfia bűncselekmény elkövetése miatt rendelt el nyomozást. E bűncselekményi kategóriában közel (kerekítve) minden második elrendelt nyomozás a gyermekpornográfia bűncselekmény elkövetésével volt érintett. Ez az arányszám az 1 százalékhoz képest máris szignifikáns eltérést eredményez, jelentősen magas értéket képviselt. Ha a kérdést e aspektusból vizsgáljuk, elmondhatjuk, hogy gyermekpornográfia tekintetében a 4 évi intervallumon belül a 47 százalékos arányszám igen nagy fertőzöttségre, és veszélyeztetettségre vall. A váderedményesség tekintetében még kaotikusabb arányszámokat kapunk: az összes vádemelési javaslattal lezárt büntetőeljáráshoz viszonyítva a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások 1,2-, a gyermekpornográfia bűncselekmény pedig az érték 0,7 százalékát tette ki. Ha ezeket az arányszámokat szintén aprópénzre váltjuk, akkor annak az eredményét is megkaphatjuk, miként viszonyul egymáshoz a Büntető Törvénykönyv e fejezete, valamint a gyermekpornográfia

bűncselekmény miatt elrendelt nyomozások vádemelési arányszámai. A nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások, és a gyermekpornográfia hazai büntetőeljárásainak vádemelési javaslattal lezárt ügyeinek összehasonlításából megállapítható, hogy a gyermekpornográfia büntetőeljárásainak vádemeléssel lezárt ügyeinek száma a 2012. évben 2-, 2013. évben pedig 70 százalékkal magasabb volt, azonban 2014. évtől kezdődően a vádemelések száma először 16-, majd 29-, végül 19 százalékkal csökkent, és maradt el a többi bűncselekményhez képest. Bár az első év mindösszesen 2 százalékost növekedést ért el, és épphogy nem csúszott el negatív irányba, megjegyzendő, hogy 2013. évben a nyomozó hatóság igen nagyszabású vádemelési javaslattal zárult büntetőeljárást fejezett be. A következő években viszont kétséget kizáróan megállapítható, hogy a vádemelési javaslattal érintett ügyek száma nagymértékben csökkent, esetekben még az ¼ százalékos lélektani határt sem érte el. A hazai összes büntetőeljárás számadataihoz viszonyítva elenyésző a gyermekprostitúcióval, és a nemi élet szabadságával kapcsolatos bűncselekmények száma, mindannak ellenére, hogy azok évről-évre növekednek. Mindkét összehasonlítás lineáris korrelációját számítani lehetett, amely nemzetközi vonalon majdnem közepes, hazai vonalon pedig majdnem nagy korrelációs együtthatót eredményezett. A nemzetközi adatokhoz viszonyítva a magyar gyermekpornográfiával érintett báncselekmények közepesen erős tábort-, hazai viszonylatban pedig majdnem nagy tábort alkotnak. A korrelációs számítás az arányaiban vizsgált százalékos mutatókat szintén megerősítette. A nyomozó hatóság által lefolytatott nemi élet szabadsága fejezetébe illeszkedő büntetőeljárások tekintetében megállapítást nyert, hogy a gyermekpornográfiával érintett vádemelési javaslattal lezárt ügyek jóval kevesebb darabszámúak, mint a nyomozás megszüntetése, valamint a feljelentés elutasítása kóddal befejezett eljárások. A váderedményesség a megszüntetések, feljelentések elutasítása csoporthoz képest 2013. év kivételével mindig alulmaradt. A vádemeléssel lezárt ügyek alacsony száma eredményezheti azt, hogy a magyar rendvédelmi erők a gyermekpornográfia elleni harc nemzetközi élvonalába nem kerülhetnek be. Támasztja ezt alá az az adat is, hogy a gyermekpornográfiával érintett bűncselekmények tekintetében a 7041 darab ügyből csupán 1110 esetben került sor a nyomozó hatóság kezdeményezésére nyomozás elrendelésére, abból is 100 esetben nemzetközi szerv kezdeményezte a felelősségre vonást. Azaz a rendvédelmi szervek az esetek 15 százalékát tudták csak felderíteni, és nyomozást kezdeményezni, amelyből 10 százalék külföldi, nemzetközi szerv

indítványozására került lefolytatásra. Ez a magyar rendvédelmi erőket a kötelezettségvállalásban negatívan befolyásolja.

4.4.6 Gyermekpornográfia bűncselekmény Magyarországon régiók szerint

9. diagram: Magyar rendőrség statisztika; Gyermekpornográfia bűncselekmény régiók szerint 2012-2016. időszakban; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása

.

2012-2016-ig terjedő időszakban a gyermekpornográfia bűncselekmény számának vizsgálatára (megyei szintű) település, azaz régiószint szerint került sor. (A statisztika nem érintette a külföldi-, a Magyarország területére nem bontható-, és a nem beszerezhető adatok körét. Továbbá megjegyezni kívánom, hogy a büntetőeljárások, valamint a régiós bűncselekmények száma közötti eltérést az okozhatja, hogy előző évekből fennmaradt büntetőeljárások döntését nem tárgyévben hozták meg, vagy az érdemi döntés az követően született.) A négy év viszonylatában összesen 6629 darab regisztrált gyermekpornográfia bűncselekmény jutott a nyomozó hatóság tudomására, ez 19 megyét, és a fővárost foglalta magában. A minimum érték Zala megyében született, ahol mindösszesen 10 darab elrendelés történt. Ezzel ellentétben Nógrád megyében több, mint 4906 darab eljárást regisztráltak. A szórás mértéke 1080,24 volt. Átlagosan 331 darab gyermekpornográfiás bűncselekmény jutott 2012-2016. évek között a nyomozó hatóság tudomására, amely a 19 megyében, valamint a fővárosban nyomozás alapját képezte. A módusz számítás eredményes volt a tekintetben, hogy két megye is ugyan azzal a bűnügyi mutatóval rendelkezett. Baranya-, és Fejér megye egyaránt 42-42 eljárást regisztrált. A megye szintű lebontásban Baranya-, Csongrád-, Fejér-, Győr-Moson-Sopron-, Komárom-Esztergom-, Jász-Nagykun-Szolnok-, Tolna-, Vas-, és Zala

megye négy év távlatában 50 darab elrendelés alatt teljesített, a maradék megye ezt az értéket jóval meghaladta. Kiemelt helyen Budapest, Bács-Kiskun, Békés-, Hajdú-Bihar-, Heves-, Nógrád-, Somogy megye szerepelt, amelyek 150 darabszámú bűncselekményszám felett regisztrált.

4.4.7 Gyermekpornográfia bűncselekmény Magyarországos régiók szerint, különös tekintettel a pornográf felvétel elkövetés tárgyára

10. diagram: Magyar rendőrség statisztika; Gyermekpornográfia bűncselekmény régiók szerint 2012-2016. időszakban különös tekintettel a pornográf felvételekre; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása

Az alábbi grafikonon hasonlóképpen az előzőkhez 2012-2016-ig terjedő időszakban a gyermekpornográfia bűncselekmény számának vizsgálatára (megyei szintű) település, azaz régiószint szerint került sor, kiegészítve azzal, hogy az elkövetés tárgyát kizárólag a pornográf felvételekre terjesztettem ki. (A statisztika nem érintette a külföldi-, a Magyarország területére nem bontható-, és a nem beszerezhető adatok körét.) A négy év viszonylatában összesen 6216 darab regisztrált gyermekpornográfia bűncselekmény jutott a nyomozó hatóság tudomására, amelynek tárgya pornográf felvétel volt. A minimum érték Zala-, Vas-, és Győr-Moson-Sopron megyében született, ahol mindösszesen 7 darab elrendelés történt. Ezzel ellentétben Nógrád megyében több, mint 4895 darab olyan eljárást regisztráltak, amelynek elkövetési tárgya a pornográf felvétel volt. A szórás mértéke 1082,56 volt. Átlagosan 310 darab gyermekpornográfiás bűncselekmény jutott 2012-2016. évek között a nyomozó hatóság tudomására, amely a 19 megyében, valamint a fővárosban nyomozás alapját képezte, és az elkövetők azokat pornográf felvétel formájában rögzítettek, használtak fel, továbbítottak. A

módusz számítás eredményes volt a tekintetben, hogy a minimum értékeket képviselő megyék egyaránt 7 eljárást indítottak. Baranya-, és Fejér megye egyaránt 42-42 eljárást regisztrált. A megye szintű lebontásban Baranya-, Csongrád-, Fejér-, Győr-Moson-Sopron-, Komárom-Esztergom-, Pest, Jász-Nagykun-Szolnok-, Szabolcs-Szatmár-Bereg-, Tolna-, Vas-, Veszprém-, és Zala megye négy év távlatában 50 darab elrendelés alatt teljesített, a maradék megye ezt az értéket jóval meghaladta. Kiemelt helyen Budapest, Bács-Kiskun, Békés-, Heves-, Nógrád-, Somogy megye szerepelt, amelyek 100 darabszámú bűncselekményszám felett regisztrált.

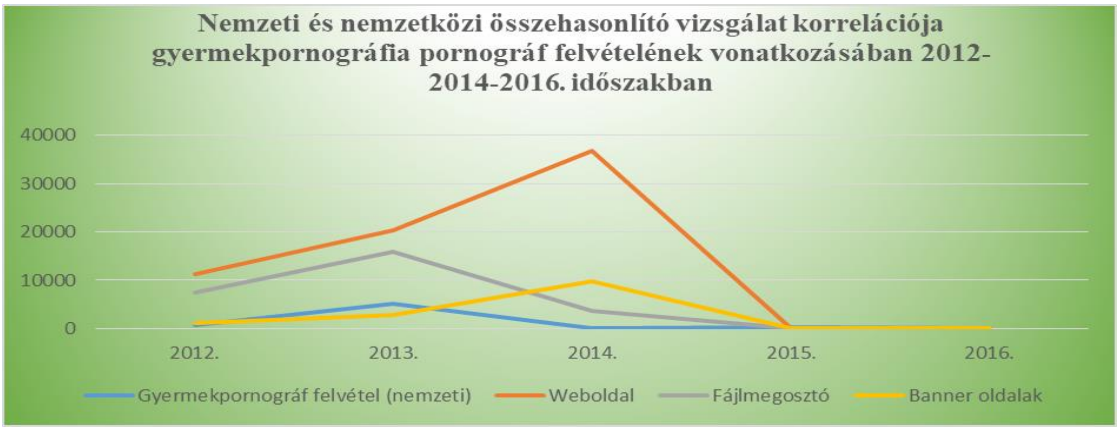
4.4.8 Nemzetközi gyermekpornográfia az elkövetés tárgyának vonatkozásában

11. diagram: INHOPE; Nemzetközi gyermekpornográfia büntetőeljárások alakulása 2012-2014. időszakban különös tekintettel a pornográf felvételekre ; Forrás: A szerző (INHOPE jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

A fenti diagramm a gyermekpornográfiával kapcsolatos nemzetközi statisztikák alapján azt mutatja meg, hogy a lefolytatott eljárások során az elkövetés tárgya mennyi esetben, és milyen minőségben volt gyermekpornográf felvétel. Az INHOPE által lefolytatott eljárások 182124 darab az interneten fellelhető tiltott pornográf linknek az eltávolítását eredményezték. Ennek a vizsgált időszakba 2012-ben 30 százaléka weboldal, 20 százaléka fájlmegosztó, és 3 százaléka banner volt. Számadatok tekintetében ez 11221, 7480, és 1122 darab pornográf felvételt jelent. 2013. évben ugyan ezen adatok vonatkozásában 37-, 29-, és 5 százalékról, azaz 20335, 15938, és 2748 darab felvételről volt tudomásunk. Az utolsó vizsgált

évben, amelyről számadattal rendelkezünk az arányszámok 41-, 4-, és 11 százalékra változtak, amely 36800, 3590, és 9873 darab elkövetési tárgyat jelentett. Összesen gyermekpornográf felvétellel kapcsolatosan 68356 darab weboldal, 27008 darab fájlmegosztó, és 13743 darab banner volt fertőzött. A minimum értékek weboldalak vonatkozásában 2012-ben 11221 darab, a fájlmegosztók tekintetében 2014-ben 3590 darab, és a bannerekkel összefüggésben szintén 2012-ben 1122 darab között mozgott. A maximum értékek weboldalak vonatkozásában 2014-ben 36800 darab a fájlmegosztók tekintetében 2013-ban 15938 darab, és a bannerekkel összefüggésben szintén 2014-ben 9873 darab között mozgott. Átlagosan 22785 weboldal, 9002 fájlmegosztó, és 4581 banner volt veszélyeztetett, és fertőzött. Módusz számításra lehetőség nem volt, tekintettel arra, hogy ugyan olyan értéket egyik év sem képviselt. A szórás mértéke weboldalakkal összefüggésben 12964,35, fájlmegosztók kapcsán 6313,25, és bannerek vonatkozásában 4654,55 volt.

4.4.9 A gyermekpornográfiával érintett elkövetési tárgyak hazai (nemzeti)-, és nemzetközi (uniós) összehasonlítása, azok eredményei



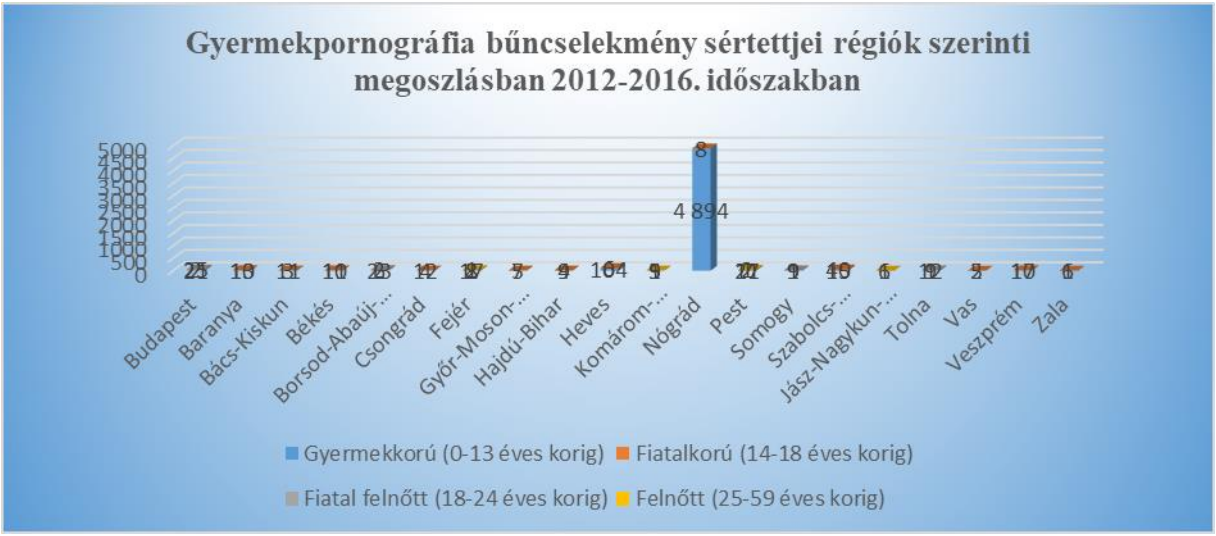
12. diagram: INHOPE; Magyar rendőrség statisztika; Nemzeti és nemzetközi összehasonlító vizsgálat korrelációja gyermekpornográfia pornográf felvételének vonatkozásában 2012-2014-2016. időszakban; Forrás: A szerző (INHOPE jelentéseinek és a rendőrség számadataiból összeállított) kutatásának ábrázolása.

A nemzeti és nemzetközi összehasonlítás grafikonjából az alábbiak olvashatók ki: a magyar gyermekpornográf bűncselekményekkel kapcsolatba hozható felvételek összesen 6215 darab elkövetési tárgyat jelentettek. Ez a nemzetközi weboldalakhoz viszonyítva 9-, a fájlmegosztó rendszerekhez viszonyítva 23-, a bannerekhez viszonyítva 45 százalékot tett ki. Ha elfogadjuk a nemzetközi rendszerrel kapcsolatos hipotéziseimet, akkor ez azt jelenti, hogy

a magyar felvételek arányszámai a nemzetközi bannerek majdnem felének megfelelő-, a fájlmegosztó hálózatok majdnem ¼-nek megfelelő-, és a weboldalak majdnem 1/10-nek megfelelő arányszámait teszik ki. Minél több tehát a magyar illegális felvételek száma, annál több a gyermekek internetes szexuális kizsákmányolása a nemzetközi vonalon is. A növekedés között – tekintettel a világhálóra – egyenes arányosság logikai összefüggése állapítható meg. Ezeket leginkább a Cohan féle skálán lehet illusztrálni. A Cohan féle skálán a korrelációs koefficiens értéke a weboldalakkal összefüggésben 0,22-, a fájlmegosztó rendszerek vonatkozásában 0,91-, a bannerek viszonylatában -0.03. Ez azt jelenti, hogy két pozitív, és egy negatív eredményt kaptunk. A -0,03, valamint a 0,22 értékek tekintetében majdnem tökéletes korrelációt, a 0,91 érték vonatkozásában pedig pozitív korrelációs értéket kaptunk. Az utóbbi vonatkozásában a Cohan skálán a korreláció mértéke nagy, a maradék kettő esetén majdnem közepes, és majdnem kicsi.

Az alfejezettel összefüggésben az alábbi részmegállapítások tehetők: a magyar gyermekprostitúcióval érintett gyermekpornográfia felvételek száma nemzetközi viszonylatban is tetemes mennyiséget ölel fel. Akár a bannerekhez, akár a weboldalakhoz viszonyítjuk, a számok a fertőzöttség, és veszélyeztetettség tükrében a nemzetközi viszonylat 10, de közel az 50 százalékát is kiteszik. A helyzet súlyossága a magyar rendvédelmi erők fokozottabb fellépését igénylik. A magyar viszonylatot elemezve megállapítható, hogy a legtöbb eljárást Nógrád megyében regisztrálták, a pornográf felvételek legtöbbje is e régióból származik. A legkevesebb nyomozás elrendelés Zala megyét érintette, míg a legkevesebb pornográf felvétel szintén Zala-, valamint Vas-, és Győr-Moson-Sopron megyéből származott. Megyei szintű lebontásban fertőzöttség tekintetében a főváros, valamint Bács-Kiskun-, Békés-, Hajdú-Bihar-, Heves-, Nógrád-, és Somogy megye volt a legérintettebb. E megyékben az elrendelt nyomozások száma a 150 darabot, a pornográf felvételekkel érintett eljárások a 100 darabot is meghaladták. A megyék között megtaláljuk az ország gazdaságilag elmaradottabb, és szegénységgel sújtott régióit is. A főváros veszélyeztetettsége szintén magas. Megállapítható továbbá, hogy a 2013. év 2014. évhez viszonyított arányszámokon kívül, a pornográf felvételek, és az elrendelt nyomozások szintén emelkedő tendenciát mutatnak.

4.4.10 Gyermekpornográfia bűncselekmény sértettjei Magyarországon régiók szerint

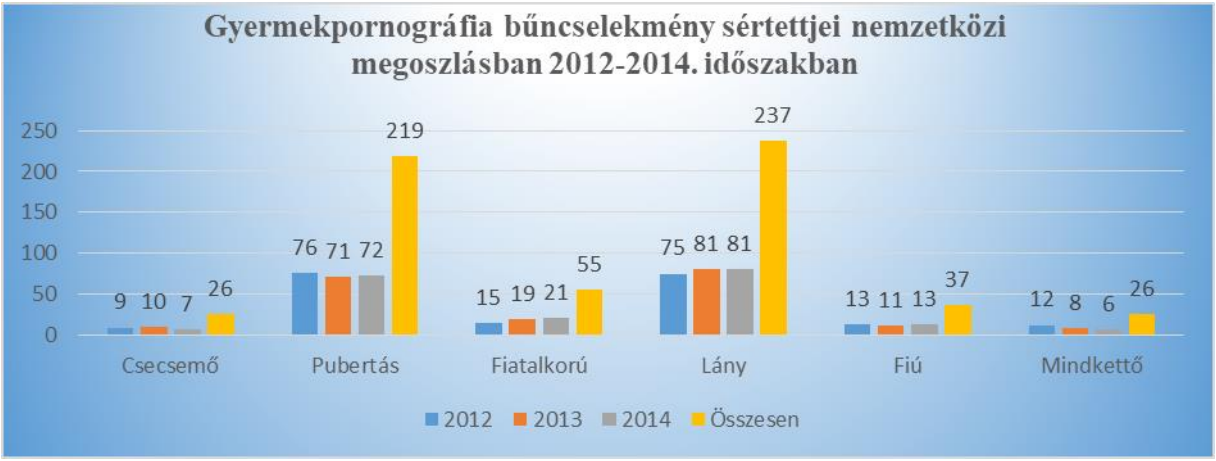


13. diagram: Magyar rendőrség statisztika; Gyermekpornográfia bűncselekmény sértettjei régiók szerinti megoszlásban 2012-2016. időszakban különös tekintettel a pornográf felvételekre; Forrás: A szerző (Magyar rendőrség számadataiból összeállított) kutatásának ábrázolása

2012-2016-ig terjedő időszakban a gyermekpornográfia bűncselekmény sértettjei számának vizsgálatára (megyei szintű) település, azaz régiószint szerint került sor. (A statisztika nem érintette a külföldi-, a Magyarország területére nem bontható-, és a nem beszerezhető adatok körét.) A bűncselekmény a vizsgált intervallumban összesen 5418 áldozatot szedett, amelyből 5361 lány, és 57 fiú nemű sértett került regisztrálásra. Az összes sértett 1 százaléka volt kisfiú, a maradék 99 százalék a kislányokat érintette. A szexuális visszaélésekkel érintett gyermekpornográfia bűncselekmény szörnyűségeit gyermekkorú (0-13 éves korig) kategóriában 5168-, a fiatalkorú (14-18 éves korig) kategóriában 236-, a fiatal felnőtt (18-24 éves korig) kategóriában 9-, és a felnőtt (25-59 éves korig) kategóriában 5 sértett élte át. Ahogy a magyar törvényi szabályozás fejezetben ismertetésre került, a norma lehetőséget teremt arra, hogy az elkövető hatósági üldöztetését hatályos magánindítvány esetén a felnőttkorú sértett is kérhesse, amennyiben sérelmére a bűncselekményt gyermekkorában követték el. A sértettek száma 2012-ben 58-ról 4947-re növekedett, majd 2014-ben 55-re csökkent. Az elkövetkezendő években így 2015-ben 218-ra nőtt, majd 143-ra csökkent. A minimum, azaz a legalacsonyabb sértettszámot Jász-Nagykun-Szolnok megyében regisztráltak, amelyhez a módusz számítás is, azonos értékkel, Vas-, és Zala megyékkel csatlakozott. A legtöbb sértettet Nógrád megyében regisztrálták, a bűncselekmény áldozatául

4902 személy esett. Átlagosan négy év intervallumban 270 sértettet regisztrálnak, a szórás értéke pedig 1090,3.

4.4.11 Nemzetközi gyermekpornográfia bűncselekmény sértettjei

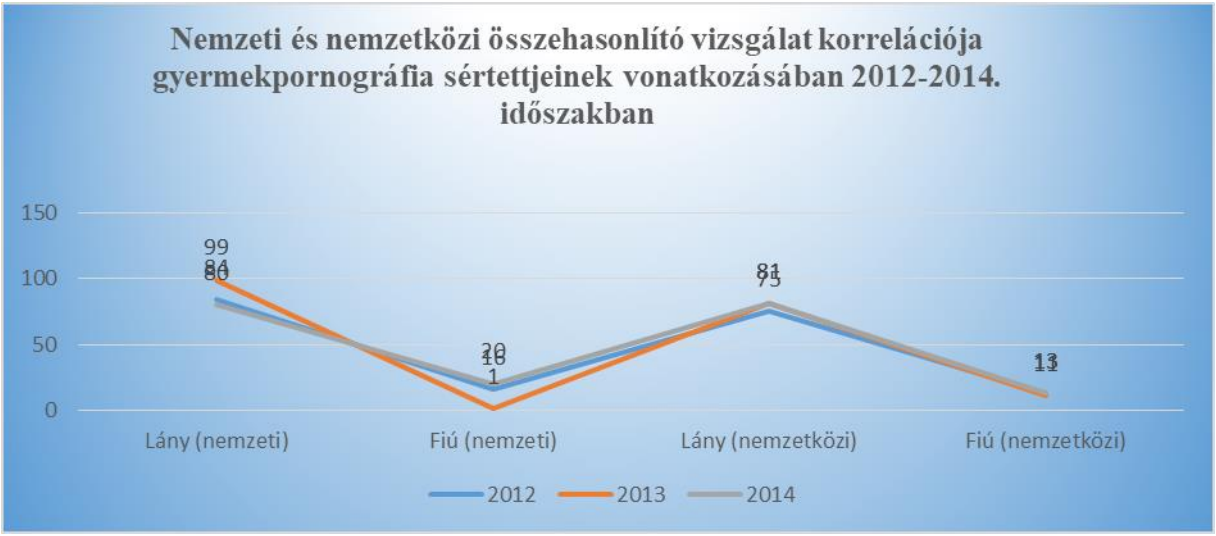


14. diagram: INHOPE; Nemzetközi gyermekpornográfia sértettjei 2012-2014. időszakban; Forrás: A szerző (INHOPE jelentéseinek számadataiból összeállított) kutatásának ábrázolása.

Az INHOPE statisztikai számadatokat a sértettekről nem közölt. Azt azonban a statisztikai jelentésekből kiolvasható volt, hogy a sértettek milyen korúak, valamint milyen neműek voltak. (Ezek az arányszámok az inkriminált időszakban az eltávolításra kerülő oldalak számához viszonyultak.) 2012-ben a csecsemők 9-, a pubertás korosztály 76-, és a fiatalkorú korosztály 15 százaléka volt érintett. Ebből 13 százalék volt fiú, és 75 százalék lány. Olyan anyag, amelyen mindkét nem szerepelt 12 százalékban volt tettenérhető. 2013-ban ezek a kategóriák 10-, 71-, és 19 százalékra emelkedtek. A lányok 81-, a fiúk 11 százaléka volt érintett. Mindkettő vonatkozásában 8 százalékot rétek el a mutatók. 2014. évben a csecsemő korosztály 7-, a pubertás korosztály 72-, és a fiatalkorú korosztály 21 százalékban esett áldozatul. A lányok 81-, a fiúk 13-, és mindketten 6 százalékos arányt adtak ki. Ha a három év intervallumát vesszük alapul, akkor a 300 százalékhoz viszonyítva a csecsemő korosztály összesen 26-, a pubertás korosztály összesen 219-, a fiatalkorú korosztály 55 százalékot jelent. Ugyan ezzel a százalékos aránnyal számolva a lányok 237-, a fiúk 37-, és mindketten 26 százalékot tettek ki. A minimum értékek gyermekkorban 7, pubertásban 71, fiatalkorban 15, lányoknál 75, fiúknál 11, és mindkettő esetében 6 százalékot jelentett. Ezzel ellentétben a maximum értékek ugyan ezen kategóriákban 10, 76,21,81,13,12 százalékos értékeket képviseltek. Átlagosan a csecsemőkorúaknál a 8,6-, a pubertásoknál a 73-, fiatalkorúaknál a 18,3-, lányoknál a 79-, fiúknál a 12,3-, és mindkettőnél szintén 8,6

százalék a sértetti kör alkotója. A szórás értékei 1,5-,2,6-, 3-, 3,4-, 1,1-, 3 százalékosak voltak. A módusz számításra két esetben volt lehetőség, a lány nem, valamint a fiú nem vonatkozásában, ahol a 81-, és a 13 százalék ismétlődött.

4.4.12 A gyermekpornográfiával érintett sértettek hazai (nemzeti)-, és nemzetközi (uniós) összehasonlítása, azok eredményei



15. diagram: INHOPE; Magyar rendőrség statisztika; Nemzeti és nemzetközi összehasonlító vizsgálat korrelációja gyermekpornográfia sértettjeinek vonatkozásában 2012-2014. időszakban; Forrás: A szerző (INHOPE jelentéseinek és a rendőrség számadataiból összeállított) kutatásának ábrázolása.

Tekintettel arra, hogy nemzetközi viszonylatban a sértettek életkori kategóriái, valamint a magyar életkori kategóriák nem fedték egymást, ezért annak összehasonlítására lehetőség nem volt. Korábbi fejezetekben ismertettem, hogy a nagykorúság például egyes államokban a 18., más államokban pedig akár a 21. betöltött életévet is jelentheti. E megállapítás figyelembevételével kizárólag az évekre lebontott fiú, és lány, azaz nemek szerinti százalékos arányszámokat lehetett összehasonlítani. 2012-ben a nemzeti lány és fiú aránypár 84-16, a nemzetközi aránypár 75-13 százalék volt. (A fennmaradó értéket azok az anyagok képezték, amelyeken mindkét nem egyszerre szerepelt.) 2013-ban a nemzeti lány és fiú aránypár 99-1, a nemzetközi aránypár 81-11 százalék volt. 2014. évben a nemzeti lány és fiú aránypár 80-20, a nemzetközi aránypár 81-13 százalék volt. Az, hogy a nemzeti arányszám a nemzetközi arányszámhoz hogyan hasonul a Cohan féle korrelációs együttható lineáris szorosságával mérhető volt. A Cohan féle skálán a korrelációs koefficiens értéke

minden évben 1 volt. Ez azt jelenti, hogy minden évben a fiú, és lány nemek vonatkozásában tökéletesen pozitív, és a korreláció mértéke nagy volt. Vagyis a nemzeti arányszámok a nemzetközi arányszámokkal megegyeztek.

Az alfejezet zárásaként összegezhető, hogy Magyarországon, akárcsak a nemzetközi vonalon a gyermekpornográfia bűncselekmény elkövetésének legveszélyeztetettebb korosztálya a gyermekkorú, a szexuális életre még fel nem készült – ám már lehet annak beleegyezési jogával bíró – lányai, fiai. A nem szerinti megoszlás arról tanúskodott, hogy a lányok a gyermekpornográfia veszélyének sokkal inkább kiszolgáltatottabb résztvevői, mint a fiúk. Sokkal magasabb százalékos arány rendelkezik a lányok veszélyeztetettségéről, mint a fiúk esetében. Mindezek viszont, akár a fiúk, akár a lányok vonatkozásában - egyenes arányban - a nemzetközi statisztikákhoz asszimilálódtak. A korrelációs együttható tökéletesen pozitív értéke, valamint a korrelációs mérték nagysága ezt alátámasztotta. A gyermekpornográfia bűncselekménnyel érintett legkevesebb sértettet Magyarország viszonylatában Jász-Nagykun-Szolnok, Vas-, és Zala megyében-, a legtöbb sértettet pedig Nógrád megyében regisztrálták. De, ahogy az elrendelt nyomozások száma, úgy a regisztrált sértettek száma is e kategóriákban megegyezett. A sértettek száma stagnáló értéket sosem képviselt, az két esetben nőtt, két esetben pedig csökkent, mégis arányaiban a növekedés mértéke sokkal nagyobb, mint a csökkenés együtthatója. Ez arra enged következtetni, és olyan prognosztizációt foglal magában, hogy amennyiben a rendvédelmi erők akárcsak a hazai-, vagy a nemzetközi harcban minőségfejlesztésen nem esnek át, az innovációs intézkedések nem kerülnek bevezetésre, évről évre egyre inkább emelkedni fog a sértettek száma, ami a gyermekek testi-, értelmi, és szellemi fejlődését negatív irányba tereli, sérüléseket szenvedhetnek, a bűncselekmények károkat okozhatnak.

4.5 Tudományos kutatási eredmények

4.5.1 A kutatási eredmények megvitatása

A kutatási eredmények értelmezése során kiemelt figyelmet kell fordítanunk arra, hogy a számadatok, amelyekkel dolgoztam, kizárólag a regisztrált, azaz nyilvántartásba vett bűncselekményekről, elkövetőkről, és áldozatokról adott számot. Sajnálatos módon azonban a gyermekek szexuális kizsákmányolással érintett gyermekpornográf bűncselekmények

becsléseink szerint évente több millió személy testi épségét-, és életet veszélyeztetik, fenyegetik. Mégis azt kell mondanunk, hogy a mély látenciába burkolódzó jelenség kapcsán figyelemfelhívásra okot adó körülményeket sikerült feltérképeznem, amelyeket az alábbiak szerint kívánok megvitatni. Megállapítottam, hogy Magyarország büntetőeljárásainak feljelentés elutasításával, nyomozás megszüntetésével, és a vádemelési javaslattal lezárt eredményei tekintetében a nemi élet, és szabadság elleni büntetőeljárások az összes büntetőeljárás 1 százalékát jelentik. (összes büntetőeljárás 1462614 db vs. nemi élet elleni büntetőeljárás 7736 db.) Országos viszonylatban ezek a számok nem jelentik azt, hogy hazánk igen fertőzött, vagy veszélyeztetett volna, azonban minél részletesebb a vizsgálatot folytatunk, annál inkább látszik annak ambivalenciája. A nemi élet szabadság fejezetén belül a gyermekpornográfiával érintett büntetőeljárások száma viszont már 47 százalékot ölelt fel. (Nemi élet elleni büntetőeljárás 7736 db. vs. gyermekpornográfia büntetőeljárás 7041 db.) Ez azt jelenti, hogy a három kategóriában a nyomozó hatóság által a Büntető Törvénykönyv e fejezetébe ütköző bűncselekmények tekintetében 47 százalékos aránnyal gyermekpornográfia bűncselekmény elkövetése miatt rendelt el nyomozást. (Nemi élet elleni büntetőeljárás 7736 db. vs. gyermekpornográfia büntetőeljárás 7041 db.) E bűncselekményi kategóriában közel (kerekítve) minden második elrendelt nyomozás a gyermekpornográfia bűncselekmény elkövetésével volt érintett. Ez az arányszám az 1 százalékhoz képest máris szignifikáns eltérést eredményez, jelentősen magas értéket képviselt. Ha a kérdést e aspektusból vizsgáljuk, elmondhatjuk, hogy gyermekpornográfia tekintetében a 4 évi intervallumon belül a 47 százalékos arányszám igen nagy fertőzöttségre, és veszélyeztetettségre vall. A váderedményesség tekintetében még kaotikusabb arányszámokat kapunk: az összes vádemelési javaslattal lezárt büntetőeljáráshoz viszonyítva a nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások 1,2-, a gyermekpornográfia bűncselekmény pedig az érték 0,7 százalékát tette ki. (Összes büntetőeljárás vádemelési javaslata 764546 db. vs. nemi élet büntetőeljárás vádemelési javaslata 3257 db; összes büntetőeljárás vádemelési javaslata 764546 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 7041 db.) Ha ezeket az arányszámokat szintén aprópénzre váltjuk, akkor annak az eredményét is megkaphatjuk, miként viszonyul egymáshoz a Büntető Törvénykönyv e fejezete, valamint a gyermekpornográfia bűncselekmény miatt elrendelt nyomozások vádemelési arányszámai. A nemi élet szabadsága, és a nemi erkölcs elleni büntetőeljárások, és a gyermekpornográfia hazai büntetőeljárásainak vádemelési javaslattal lezárt ügyeinek összehasonlításából

megállapítható, hogy a gyermekpornográfia büntetőeljárásainak vádemeléssel lezárt ügyeinek száma a 2012. évben 2-, 2013. évben pedig 70 százalékkal magasabb volt, azonban 2014. évtől kezdődően a vádemelések száma először 16-, majd 29-, végül 19 százalékkal csökkent, és maradt el a többi bűncselekményhez képest. (Nemi élet büntetőeljárás vádemelési javaslata 2012-ben 348 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2012-ben 357 db. Nemi élet büntetőeljárás vádemelési javaslata 2013-ban 366 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2013-ban 5104 db; Nemi élet büntetőeljárás vádemelési javaslata 2014-ben 666 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2014-ben 111 db. Nemi élet büntetőeljárás vádemelési javaslata 2015-ben 832 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2015-ben 249 db. Nemi élet büntetőeljárás vádemelési javaslata 2016-ban 1045 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2016-ban 199 db.) Bár az első év mindösszesen 2 százalékost növekedést ért el, és épphogy nem csúszott el negatív irányba, megjegyzendő, hogy 2013. évben a nyomozó hatóság igen nagyszabású vádemelési javaslattal zárult büntetőeljárást fejezett be. (Gyermekpornográfia büntetőeljárás vádemelési javaslat 5104 db.) A következő években viszont kétséget kizáróan megállapítható, hogy a vádemelési javaslattal érintett ügyek száma nagymértékben csökkent, esetekben még az ¼ százalékos lélektani határt sem érte el. Nemi élet büntetőeljárás vádemelési javaslata 2014-ben 666 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2014-ben 111 db. Nemi élet büntetőeljárás vádemelési javaslata 2015-ben 832 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2015-ben 249 db. Nemi élet büntetőeljárás vádemelési javaslata 2016-ban 1045 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2016-ban 199 db.) A hazai összes büntetőeljárás számadataihoz viszonyítva elenyésző a gyermekprostitúcióval, és a nemi élet szabadságával kapcsolatos bűncselekmények száma, mindannak ellenére, hogy azok évről-évre növekednek. Mindkét összehasonlítás lineáris korrelációját számítani lehetett, amely nemzetközi vonalon majdnem közepes, hazai vonalon pedig majdnem nagy korrelációs együtthatót eredményezett. (Összes büntetőeljárás vádemelési javaslata 764546 db. vs. nemi élet büntetőeljárás vádemelési javaslata 3257 db. korr. -0,11. Nemi élet büntetőeljárás vádemelési javaslata 3257 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 6020 db. korr. 0,54. Összes büntetőeljárás vádemelési javaslata 764546 db. vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 6020 db. korr. 0,48. Nemzetközi gyermekek internetes szexuális visszaélései 182124 db. vs. gyermekpornográfia

büntetőeljárás vádemelési javaslata 6020 db. korr. 0,25.) A nemzetközi adatokhoz viszonyítva a magyar gyermekpornográfiával érintett báncselekmények közepesen erős tábort-, hazai viszonylatban pedig majdnem nagy tábort alkotnak. A korrelációs számítás az arányaiban vizsgált százalékos mutatókat szintén megerősítette. A nyomozó hatóság által lefolytatott nemi élet szabadsága fejezetébe illeszkedő büntetőeljárások tekintetében megállapítást nyert, hogy a gyermekpornográfiával érintett vádemelési javaslattal lezárt ügyek jóval kevesebb darabszámúak, mint a nyomozás megszüntetése, valamint a feljelentés elutasítása kóddal befejezett eljárások. A váderedményesség a megszüntetések, feljelentések elutasítása csoporthoz képest 2013. év kivételével mindig alulmaradt. (Nemi élet büntetőeljárás nyomozás megszüntetése, feljelentés elutasítása 2012-ben 56 % vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2012-ben 44 %. Nemi élet büntetőeljárás nyomozás megszüntetése, feljelentés elutasítása 2013-ban 11 % vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2013-ban 89 %. Nemi élet büntetőeljárás nyomozás megszüntetése, feljelentés elutasítása 2014-ben 91 % vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2014-ben 9 %. Nemi élet büntetőeljárás nyomozás megszüntetése, feljelentés elutasítása 2015-ben 83 % vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2015-ben 17 %. Nemi élet büntetőeljárás nyomozás megszüntetése, feljelentés elutasítása 2016-ban 87 % vs. gyermekpornográfia büntetőeljárás vádemelési javaslata 2016-ban 13 %.) A vádemeléssel lezárt ügyek alacsony száma eredményezheti azt, hogy a magyar rendvédelmi erők a gyermekpornográfia elleni harc nemzetközi élvonalába nem kerülhetnek be. Támasztja ezt alá az az adat is, hogy a gyermekpornográfiával érintett bűncselekmények tekintetében a 7041 darab ügyből csupán 1110 esetben került sor a nyomozó hatóság kezdeményezésére nyomozás elrendelésére, abból is 100 esetben nemzetközi szerv kezdeményezte a felelősségre vonást. Azaz a rendvédelmi szervek az esetek 15 százalékát tudták csak felderíteni, és nyomozást kezdeményezni, amelyből 10 százalék külföldi, nemzetközi szerv indítványozására került lefolytatásra. (Rendőrség bűnügyi szerv felderítő 1110 db vs. külföldi szerv, Europol kezdeményező 100 db.) Ez a magyar rendvédelmi erőket a kötelezettségvállalásban negatívan befolyásolja.

Megállapítást nyert szintén, hogy a magyar gyermekprostitúcióval érintett gyermekpornográfia felvételek száma nemzetközi viszonylatban is tetemes mennyiséget ölel fel. (Nemzeti gyermekpornográf bűncselekmény gyermekpornográf felvételei 6216 db. vs. nemzetközi gyermekpornográfia bűncselekmény gyermekpornográf felvételei 109107 db.)

Akár a bannerekhez, akár a weboldalakhoz viszonyítjuk, a számok a fertőzöttség, és veszélyeztetettség tükrében a nemzetközi viszonylat 10, de közel az 50 százalékát is kiteszik. (Nemzeti gyermekpornográf bűncselekmény gyermekpornográf felvételei 6216 db. vs. nemzetközi gyermekpornográfia bűncselekmény gyermekpornográf felvételei weboldal tekintetében 68356 db. Nemzeti gyermekpornográf bűncselekmény gyermekpornográf felvételei 6216 db. vs. nemzetközi gyermekpornográfia bűncselekmény gyermekpornográf felvételei fájlmegosztó tekintetében 27008 db. Nemzeti gyermekpornográf bűncselekmény gyermekpornográf felvételei 6216 db. vs. nemzetközi gyermekpornográfia bűncselekmény gyermekpornográf felvételei 13743 db.) A helyzet súlyossága a magyar rendvédelmi erők fokozottabb fellépését igénylik. A magyar viszonylatot elemezve megállapítható, hogy a legtöbb eljárást Nógrád megyében regisztrálták, a pornográf felvételek legtöbbje is e régióból származik. (Gyermekpornográf bűncselekmény nyomozás elrendelés Nógrád megye 4906 db; Gyermekpornográf bűncselekmény pornográf felvétel Nógrád megye 4895 db.) A legkevesebb nyomozás elrendelés Zala megyét érintette, míg a legkevesebb pornográf felvétel szintén Zala-, valamint Vas-, és Győr-Moson-Sopron megyéből származott. (Gyermekpornográf bűncselekmény nyomozás elrendelés Zala megye 10 db; Gyermekpornográf bűncselekmény pornográf felvétel Zala-, valamint Vas-, és Győr-Moson-Sopron megye 7 db.) Megyei szintű lebontásban fertőzöttség tekintetében a főváros, valamint Bács-Kiskun-, Békés-, Hajdú-Bihar-, Heves-, Nógrád-, és Somogy megye volt a legérintettebb. E megyékben az elrendelt nyomozások száma a 150 darabot, a pornográf felvételekkel érintett eljárások a 100 darabot is meghaladták. (Gyermekpornográf bűncselekmény nyomozás elrendelés Budapest, Bács-Kiskun-, Békés-, Hajdú-Bihar-, Heves-, Nógrád-, és Somogy megye 162, 311, 166, 112, 4906, 300 db; Gyermekpornográf bűncselekmény gyermekpornográf felvétel Budapest, Bács-Kiskun-, Békés-, Hajdú-Bihar-, Heves-, Nógrád-, és Somogy megye 110, 305, 152, 108, 4895, 256 db.) A megyék között megtaláljuk az ország gazdaságilag elmaradottabb, és szegénységgel sújtott régióit is. A főváros veszélyeztetettsége szintén magas. Megállapítható továbbá, hogy a 2013. év 2014. évhez viszonyított arányszámokon kívül, a pornográf felvételek, és az elrendelt nyomozások szintén emelkedő tendenciát mutatnak. (Nemzeti gyermekpornográf felvétel 2012-ben 621 db; 2013-ban 5170 db; 2014-ben 94 db; 2015-ben 209 db; 2016-ban 122 db.)

Megállapítható volt, hogy Magyarországon, akárcsak a nemzetközi vonalon a gyermekpornográfia bűncselekmény elkövetésének legveszélyeztetettebb korosztálya a

gyermekkorú, a szexuális életre még fel nem készült – ám már lehet annak beleegyezési jogával bíró – lányai, fiai. (Nemzeti gyermekpornográfia gyermekkorú - 0-13 éves korig terjedő korosztály – 5168 db. sértett vs. nemzetközi gyermekpornográfia pubertás korosztály 76 %) A nem szerinti megoszlás arról tanúskodott, hogy a lányok a gyermekpornográfia veszélyének sokkal inkább kiszolgáltatottabb résztvevői, mint a fiúk. Sokkal magasabb százalékos arány rendelkezik a lányok veszélyeztetettségéről, mint a fiúk esetében. (Nemzeti gyermekpornográfia fiú-lány arány 1-99 %) Mindezek viszont, akár a fiúk, akár a lányok vonatkozásában - egyenes arányban - a nemzetközi statisztikákhoz asszimilálódtak. A korrelációs együttható tökéletesen pozitív értéke, valamint a korrelációs mérték nagysága ezt alátámasztotta. (Gyermekpornográfia nemzeti sértett lány-fiú arány 2012-ben 84-16 % vs. gyermekpornográfia nemzetközi fiú-lány arány 2012-ben 75-15 %. Gyermekpornográfia nemzeti sértett lány-fiú arány 2013-ban 99-1 % vs. gyermekpornográfia nemzetközi fiú-lány arány 2013-ban 81-11 %. Gyermekpornográfia nemzeti sértett lány-fiú arány 2014-ben 80-20 % vs. gyermekpornográfia nemzetközi fiú-lány arány 2014-ben 81-13 %. Gyermekpornográfia nemzeti sértett lány-fiú arány korr. nemzetközi gyermekpornográfia sértett fiú-lány arány 1.) A gyermekpornográfia bűncselekménnyel érintett legkevesebb sértettet Magyarország viszonylatában Jász-Nagykun-Szolnok, Vas-, és Zala megyében-, a legtöbb sértettet pedig Nógrád megyében regisztrálták. (Nemzeti gyermekpornográfia sértett Jász-Nagykun-Szolnok, Vas-, és Zala megye 7 db.) De, ahogy az elrendelt nyomozások száma, úgy a regisztrált sértettek száma is e kategóriákban megegyezett. A sértettek száma stagnáló értéket sosem képviselt, az két esetben nőtt, két esetben pedig csökkent, mégis arányaiban a növekedés mértéke sokkal nagyobb, mint a csökkenés együtthatója. (Nemzeti gyermekpornográfia sértettek száma 2012-ben 58 db; 2013-ban 4947 db; 2014-ben 55 db; 2015-ben 218 db; 2016-ban 143 db.) Ez arra enged következtetni, és olyan prognosztizációt foglal magában, hogy amennyiben a rendvédelmi erők akárcsak a hazai-, vagy a nemzetközi harcban minőségfejlesztésen nem esnek át, az innovációs intézkedések nem kerülnek bevezetésre, évről évre egyre inkább emelkedni fog a sértettek száma, ami a gyermekek testi-, értelmi, és szellemi fejlődését negatív irányba tereli, sérüléseket szenvedhetnek, a bűncselekmények károkat okozhatnak.

4.5.2 Következtetések

Hazánkban azt elmúlt évszázadokban-, és évtizedekben végbemenő szexuális célú bűncselekmények jelentős mértékben megváltoztatták a szabályozás jellegét és feladatait.[269] Büntető-, szabálysértési normák változásai-, változtatásai, az uniós jogalkalmazás, és joggyakorlás jogharmonizációs intézkedéseinek bevezetése egytől-egyig hozzájárulhattak ahhoz, hogy ezek a számadatok elemzés-értékelés tárgyát képezhessék. A szexuális kizsákmányolásra-, és ezzel szoros összefüggésben a gyermekek internetes szexuális kizsákmányolásával kapcsolatos gyermekpornográfiával érintett bűncselekményekre épülő szervezett bűnözés, és bűnözői hálózatok olyan problémát generáltak, amely elleni fellépéshez nemcsak az uniónak, hanem -, ahogy a számadatok is bizonyítják - Magyarországnak is kímélet nélkül fel kell lépnie, a szükséges intézkedéseket meg kell tennie. Véleményem szerint a mindenkori normaalkotás elvárt eredményt sosem hozhat akkor, ha az egyébként is látenciába burkolódzó bűncselekményeket, valamint szervezett bűnözői köröket, a jelenséget, a legalacsonyabb szinttől a legmagasabb szintig fel nem derítjük, okait meg nem értjük, és legfőképpen nem teszünk meg mindent azért, hogy az abban résztvevők jogosultságaikat normaszerűen gyakorolhassák, a bűnösök pedig megfelelő mennyiségű-, és minőségű szankcióban részesüljenek. A vizsgálat eredményei szerint hazánkat-, és az Európai Uniót a közeljövőben -, amennyiben nem teszünk ellene – az alábbi veszélyforrások fenyegetik:

- A gyermekek szexuális kizsákmányolása, az internetes gyermekpornográfia bűncselekményekkel érintett áldozatok száma tovább emelkedik.
- Minél kevesebb áldozatról van tudomásunk (regisztráció, felderítés), annál inkább valószínűbb, hogy az áldozatvédelmi intézkedések folyamatosságának biztosítása ellehetetlenül, a sértettek egészséges testi-, lelki-, szellemi fejlődése, valamint az okozott károk helyreállítása veszélybe kerül.
- A gyermekek nemi életének szexuális internetes visszaéléseiből profitáló szervezett bűnözői hálózatok, bűnözői csoportosulások, önálló tettesek tovább terjeszkednek, a kizsákmányolásából adódóan, további milliárdos feketebevételhez jutnak hozzá.
- A milliárdos feketebevételekből további bűncselekményeket követhetnek el, erősödik a fegyver-, a kábítószer-kereskedelem, valamint a terrorizmus, az államok gazdasága-, és összességben a világgazdaság romlik, hanyatlik.

[269] KOVÁCS István: A prostitúció jelensége és társadalmi kontrolljának vizsgálata empirikus módszerekkel PhD értekezés, Budapest, UNI-NKE, 2016. – p.:242-243.

Az emberi élet, a legfontosabb érték, amit a Földön élő összes embernek védenie kell. Az alapvető emberi-, és alkotmányos jogok mindenkit megilletnek, az állam azok érvényesítésére, és az azt megsértők szankcionálására garanciát vállal. Minden országnak érdeke, és kötelessége, hogy az ilyen jellegű cselekményeket felderítse, a sérülést szenvedett személyek önbecsülését, és a sérült (jog)területet, egy átfogó, hatékony és komplex intézkedéssorozattal helyreállítsa.[270]

4.5.3 Hipotézisek bizonyítása

1. Igazoltam, hogy a vizsgált időszakban, a vizsgált kategóriákban az összes elrendelt büntetőeljáráshoz viszonyítva a Büntető Törvénykönyv nemi élet szabadsága, és a nemi erkölcs elleni bűncselekmények fejezetében elrendelt büntetőeljárások alacsony százalékos számértéket képviselnek, azonban a fentiek ellenére a gyermekpornográfiával érintett bűncselekmények e fejezetben kimagaslóan (szignifikáns) magas százalékos arányról adnak tanúbizonyosságot. Alátámasztottam, hogy a gyermekek szexuális kizsákmányolásán alapuló gyermekpornográfia bűncselekmény tekintetében a nyomozások fele zárul csupán eredményesen (különös tekintettel a vádemelési javaslatokra), az a nemzetközi arányszámokhoz viszonyítva is csekély százalékú. Bizonyítottam, hogy a magyar rendvédelmi erők arányszámaiban kevés bűncselekményt derítenek fel, a nemzetközi felderítés és együttműködés a nyomozások felderítését befolyásolja. Igazoltam, hogy a fentiek eredményezhetik azt, hogy a magyar rendvédelmi erők a nemzetközi kötelezettségvállalásban, a gyermekpornográfia elleni küzdelemben az elsők között nem szerepelhetnek.
2. Részben sikerült csak bizonyítanom, hogy Magyarországon a legtöbb büntetőeljárást, és a legtöbb sértettet a gazdaságilag elmaradott, és társadalmi mélyszegénységgel sújtott régióiban regisztrálják, a sértettek száma, és a büntetőeljárások elrendelése évről évre emelkedő tendenciát mutat. Nem sikerült alátámasztanom azt, hogy Budapesten sokkal kevesebb elrendelés történik, mint e régiókban. Igazolnom sikerült, hogy a nemzetközi fiú-lány sértetti százalékos arányszám a nemzeti arányszámokkal korrelál. Alátámasztanom sikerült, hogy Magyarországon (is) a gyermekpornográfia által legveszélyeztetettebb korosztály a gyermekkorú korosztály, azon belül is a kislányok a legfenyegetettebbek. Bizonyítottam, hogy a háttérben megbúvó okok, célok és indítékok feltérképezhetők, mérsékelhetők, és egy jól felépített áldozatvédelmi stratégiával megszüntethetők. Igazolnom sikerült továbbá, hogy a hipotézisben foglaltak vizsgálata az inkriminált időszak magyar eredményes büntetőeljárásai tekintetében a korrelációs együtthatók lineáris szorosságával mérhetők.
3. Alátámasztottam továbbá, hogy a rendvédelmi szervek tekintetében egy olyan intézményesített rendszeren alapuló, és a gyermekek szexuális kizsákmányolásával kapcsolatos gyermekpornográfia bűncselekmények felderítését elősegítő stratégiai koncepció dolgozható ki, amely Magyarországot a nemzetközi viszonylat élvonalába sorolja. Bizonyítottam, hogy a megfelelő minőségű bűnüldözői munka, valamint a sértettek számára elérhető áldozatvédelmi tevékenység maximalizálása az eredményeket nagymértékben pozitív irányban befolyásolja, a látencia mértékét látványosan csökkenti.

[270] KOVÁCS István: A prostitúció jelensége és társadalmi kontrolljának vizsgálata empirikus módszerekkel PhD értekezés, Budapest, UNI-NKE, 2016. – p.:242-243.

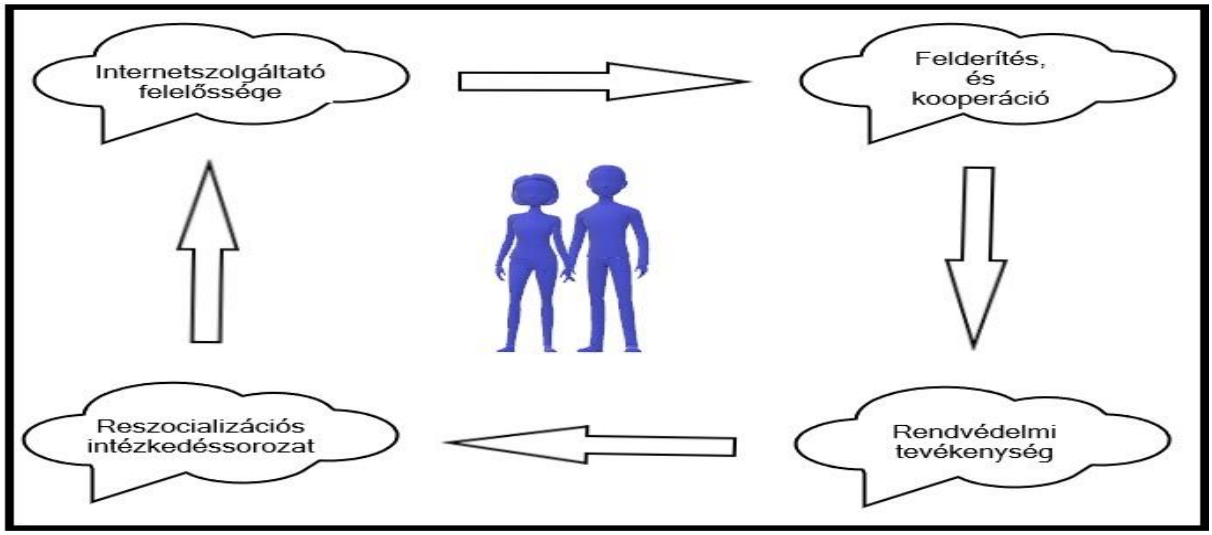
4.5.4 Új tudományos eredmények

Megítélésem szerint az értekezés elkészítése során az alábbi új tudományos eredmények születtek:

1. Elsőként sikerült, és volt lehetőségem arra, hogy a gyermekpornográfiával érintett bűncselekmények tekintetében nemzeti-, és nemzetközi forrásadatbázison alapuló számstatisztikák együtthatóinak lineáris szorosságával mérhető összehasonlítását elkészítsem. E kérdéskörben bizonyítanom sikerült, hogy a nemzeti gyermekpornográfiával érintett bűncselekmények számadatai a nemi élet szabadsága, valamint a nemi erkölcs elleni fejezethez, valamint a nemzetközi számadatokhoz képest jelentősen magas százalékos értéket képviselnek, valamint a nyomozások fele zárul csak (vádemelési javaslattal) eredményesen, a magyar rendvédelmi erők kevés bűncselekményt derítenek fel, a nemzetközi beavatkozás kimagasló.
2. A sértettek, és áldozatok arányszámai évről-évre növekvő tendenciát mutatnak, de a hátterében megbúvó okok, célok és indítékok feltérképezhetők, mérsékelhetők, és egy jól felépített áldozatvédelmi stratégiával megszüntethetők. A gazdaságilag elmaradottabb régiók mellett új forrásként a főváros, valamint az ország egyik gazdaságilag fejlett megyéje Nógrád is megjelent. A gyermekkorú (0-13 éves korig) kislányok a gyermekpornográfia bűncselekmény legveszélyeztetettebb alanyai, arányszámuk a fiúkhoz képest kimagasló. Az arányszámok a nemzetközi arányszámokkal korrelálnak.
3. Bizonyítanom sikerült, hogy a modellezés szintjén javaslat tehető egy olyan stratégiai koncepció kidolgozására, amely Magyarországot a nemzetközi viszonylat élvonalába sorolhatja, a statisztikai számok növekedését biztosíthatja.

4.5.5 Javaslatok

A tanulmány konklúziójaként olyan stratégiai koncepciót szerettem volna kidolgozni, amely a jelenlegi szabályozással összhangban a bűnüldözési tevékenységet hatékonyabbá, a prevencionális munkát eredményesebbé, a reszocializációs intézkedéseket pedig még produktívabbá teheti. Az alábbi folyamatábrán a négy lépcsős, egymásból következő, azaz konzekvens intézkedéseket, és azok magyarázatát illusztrálom.



1. ábra: Az új koncepció kidolgozásáról. Forrás: A szerző kutatásának ábrázolása.

4.5.5.1 Az internetszolgáltatók felelőssége

Személy szerint egyetértek azzal az állásponttal, hogy az internetszolgáltatóknak az interneten megosztott gyermekek szexuális visszaéléseivel kapcsolatos anyagok terjedésében erkölcsi felelősségük van. Számos szolgáltató a probléma súlyosságát már átérezte, és sokat tett azért, hogy az internet sokkal biztonságosabb környezetté válhasson. Az önszabályozási tevékenység viszont nem tűnik elegendőnek ahhoz, hogy a gyermekek sérelmére elkövetett internetes bűncselekményeket sikeresen megakadályozza. 2006-ban az International Centre for Missing and Exploited Children (ICMEC) elhatározta, hogy a gyermekpornográfia terjedésével kapcsolatosan világviszonylatban egy felmérést készít. A felmérésben annak vizsgálatára törekedtek, hogy meghatározzák, hogy a világ országai a gyermekpornográfia bűncselekménnyel kapcsolatban jogi szabályozással rendelkeznek-e, ha igen akkor a joggyakorlatban a gyermekpornográfia meghatározására milyen definíciót alkalmaznak, a törvényi tényálláson belül rendelkezik-e a norma a számítógépekkel kapcsolatos minősített esetről, a birtoklás büntetendő cselekmény-e, valamint, hogy az adott kormány az internetszolgáltatóktól a bűncselekmény észlelése esetén követel-e meg intézkedést, ha igen, akkor az milyen jellegű. A felmérés 2006-ban kezdődött, majd 2009-ben frissült, végső formáját 2011. év tavaszán érte el. A felmérésben 196 országot szerettek volna meginterjúvolni. Az elsődleges adatok szerint 2006-ban a kritériumoknak mindösszesen 27 ország felelt csak meg. 95 országban nem volt olyan jogszabály, ami a gyermekpornográfiát

büntette volna, 54 ország esetében pedig még a gyermekpornográfia fogalmát sem határozták meg. A számítógéppel elkövetett bűncselekmények vonatkozásában 27 olyan ország került górcső alá, akik az alapbűncselekmény minősített eseteként azt a tényállásba nem építették be. A birtoklást, mint elkövetési magatartást, függetlenül a terjesztés szándékától 41 ország még büntetni sem rendelte. A 2011-ben napvilágot látott jelentés a korábbi állapotokhoz képest előrehaladást mutatott. 196 ország közül 45 ország az adatszolgáltatást teljesítette. Ebből 8 ország volt, akik a fenti összes kritériumnak megfeleltek, és 37 ország már az internetszolgáltatókkal kapcsolatos feladatmeghatározásokat is abszolválta, azt saját joghatóságára kiterjesztette. 89 olyan ország volt, akik sajnálatos módon a jogszabályalkotási tevékenységnek nem feleltek meg, újabb 62 országban a gyermekpornográfia meghatározását nem definiálták. Minősített esetet 18 ország nem határozott meg, és 33 olyan ország volt, akik a birtoklást, függetlenül a terjesztés szándékától nem büntették.[271]

A tanulmány szempontjából kiemelten fontos, hogy Magyarország 2006-tól kezdődően hogya teljesített. Hazánk igyekszik a nemzetközi kötelezettségvállalásait a tudásához, és erőforrásaihoz mérten teljesíteni. Az ICMEC felmérés szerint Magyarországon gyermekpornográfiával kapcsolatos büntető jogszabály a nemzetközi jogforrásokhoz hasonul, azzal összehangban fellelhető. A fogalom definiálására jogi környezetben intézkedtek. Olyan minősített eset, amely a számítógépekkel kapcsolatos bűncselekményekről rendelkezik, fellelhető. A birtoklás ugyan olyan elkövetési magatartás, mint a terjesztés. Magyarország vonatkozásában tehát az öt kritériumból négy megvalósul. Nincs azonban olyan jogszabály, vagy együttműködési megállapodás, amely a gyermekpornográfia bűncselekmény vonatkozásában az internetszolgáltatók felelősségét megállapítaná, vagy intézkedések bevezetését tartaná indokoltnak. Bár megjegyzem, hogy a Nemzeti Média-, és Hírközlési Hatóság „hotspotot” üzemeltet, amely az INHOPE tevékenységéhez nagyban hasonlít, de az nem a kormány, és az internetszolgáltatók között kötött direkt együttműködési megállapodás részét képezi.[272] Bár az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény a

[271] ALLEN Ernie: Child Pornography: Model Legislation & Global Review. – United States: International Centre for Missing & Exploited Children, 2013.

[272] 2001. évi CVIII. törvény - az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről - – (hatályba lépett: 2001. december 24-én) (https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv) (letöltés ideje: 2017.08.01.)

szolgáltató felelősségét annyiban megállapítja, hogy az általa rendelkezésre bocsátott jogszabályba ütköző információért mindaddig ő felel, amíg arról tudomással bír. Amennyiben az adatról nem bír tudomással felelősségre nem vonható. A tudomásszerzést követően viszont az információ eltávolításáról, vagy a hozzáférés biztosításának letiltásáról intézkednie kell.[273] Ahogy Magyarország a Nemzeti Kiberbiztonsági Stratégiájában a gyermekvédelmet – különös tekintettel a gyermekek zaklatása és kizsákmányolása elleni küzdelmet, és a biztonságos online környezet megteremtését – kiemelt stratégiai célként kezeli, úgy annak nemcsak a jogalkotás legfelsőbb szintjén, hanem a legalacsonyabb szinten, azaz a végrehajtásban is meg kell mutatkoznia. Ahogy a rendvédelmi szervek, úgy az igazságszolgáltatás is próbál a társadalmi rendeltetésének megfelelni. Tekintettel viszont arra a tényre, hogy számos esetben a rendvédelmi-, és igazságszolgáltatási tevékenység elegendőnek nem bizonyul, a társszervek, és a szolgáltatók munkavégzésére és/vagy segítségére nagy szükség van. Álláspontom szerint olyan együttműködési megállapodásra van szükség, amely egyrészt a rendvédelmi feladatvégzést segíti, másrészt pedig prevenció jellegű intézkedéseket foganatosít.

4.5.5.2 Rendvédelmi tevékenység internetszolgáltatók általi támogatása

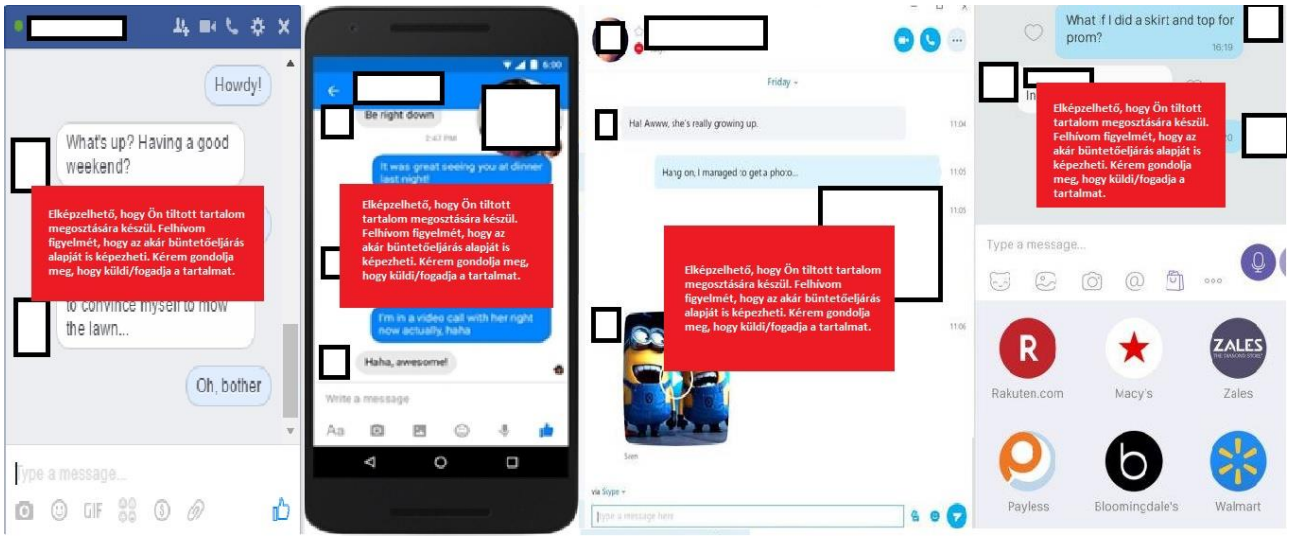
A rendvédelmi feladatok kiszolgálása egyrészt az elkövető személyének beazonosításához szükséges információk továbbítását, másrészt a tárolt adatok további megőrzési idejének hosszabbítását, és az ahhoz kapcsolódó részletes adatforgalom bonyolításának rendjét hívatottak biztosítani. Tekintettel arra, hogy az adat megőrzésének rendje jogszabályi feltételekhez kötött, azt a nyomozó hatóság az 1998. évi XIX. törvény – a büntetőeljárásról – alapján bekérheti, azonban azt a szolgáltató a belső normák szerint nem őrzi meg annyi napig, ameddig esetlegesen a büntető-, vagy polgári peres eljárás során tárgyi bizonyítási eszközként a lefoglalása megkívánná, így annak hosszabbítása kerete, vagy külön

[273] 7. § - a szolgáltató (tartalomszolgáltató) felel az általa rendelkezésre bocsátott, jogszabályba ütköző tartalmú információért. 10. § - a tárhelyszolgáltató akkor nem felel a nála tárolt információért, ha nincs tudomása az információval kapcsolatos jogellenes magatartásról, vagy arról, hogy az információ bárkinek a jogát vagy jogos érdekét sérti és amint az információ jogsértő voltáról tudomást szerzett, haladéktalanul intézkedik az információ eltávolításáról, vagy a hozzáférést nem biztosítja.

biztonsági mentése indokolttá válik.[274] Javaslatomban olyan biztonsági deficittel foglalkozó belső csoport létrehozása is szerepelne, amely, mint egy kapcsolattartó, a rendvédelmi egységek ezen kijelölt tagjaival konzultál. Negyedévente elemző-értékelő tevékenységet lát el, tapasztalataikat a rendvédelmi szervekkel megosztja. A kooperáció keretében innovatív, fejlesztő jellegű intézkedésekre tennének javaslatot. (Az együttműködésre vonatkozó javaslatokat bővebben a rendvédelmi munkavégzés alfejezeten belül kívánom részletezni.)

Konkrét gyakorlati végrehajtásban is kamatoztatható intézkedésként – különös tekintettel a „popup" alkalmazás használatára, és fejlesztésére - az alábbiakra kívánom felhívni a figyelmet: ahogy az a bevezetésben szerepeltetésre került, a legtöbb pornográf felvétel chatprogramokon keresztül jut a világhálóra. Érdemes lenne elgondolkoznunk azon, hogy az internetszolgáltatók képesek volnának-e arra, hogy akár egy rövid üzenet formájában, vagy figyelemfelhívó előugró ablakban a képküldő és/vagy képfogadó felhasználót figyelmeztethetnék, hogy a megosztott tartalmak, akár bűncselekményt is megvalósíthatnak. Amennyiben a felhasználó a figyelmeztetés ellenére úgy dönt, hogy a képet, és/vagy videófelvételt elfogadja úgy máris jogalap nyílik a személy, valamint a kérlelt tartalom hatósági ellenőrzésére. Tekintettel arra, hogy a birtoklás is bűncselekmény, így számos olyan elkövető realizálása válna esélyessé, akik ilyen jellegű anyagokat a világhálón továbbítás céljából megosztanak. Így egyrészt akár már a kezdetleges intézkedés a nyomozás alapját is megteremthetné, sőt bizonyítási eszközként történő felhasználása is indokolttá válhat, másrészt pedig rögtön gátat vethetnénk a megosztások világhálóra juttatásának. Egy „popup" szisztémán működő, előugró „reklámablak" álláspontom szerint a chatprogramok képküldözési funkcióinak figyelemfelhívó hatását erősíthetné. Amennyiben valamely felhasználó ennek ellenére mégis a küldött tartalom fogadása és/vagy küldése mellett dönt, úgy az internetszolgáltató e küldéseket és/vagy fogadásokat naponta feldolgozná, összesítené, majd azokat, összességében az illetékes hatóságnak az adatforgalmi-, és személyi adatokkal megküldené. A rendvédelmi szerv pedig ezeknek az ellenőrzését, és szűrését végrehajtaná, a nem kívánt, tiltott anyagokat pedig szűrhetné, és az eljárást akár büntető-, akár polgári peres úton megindíthatná. A fentieket az alábbi ábrán kívánom illusztrálni.

[274] Ugyan ilyen metódusra épülnek a kamerafelvételek megőrzésére szolgáló adattárak, amelyek maximum 72 órán keresztül biztosítják a felvételek megőrzését.



2. ábra: A „popup" rendszer működtetése. Forrás: A szerző kutatásának ábrázolása.

Mint azt láthatjuk, amennyiben a programok érzékelik, hogy a felhasználók között kép-, vagy más tartalom megosztása, küldése és/vagy fogadása történik, egy előugró, úgy nevezett „popup" ablak jelenik meg. Az ablak szövegezését úgy lehetne elkészíteni, hogy az az ország jogi szabályozásához mérten az arra vonatkozó normák szövegezését megjeleníti. A képek küldése és/vagy fogadása pedig csak úgy működhetne, ha a felhasználó a felhasználási feltételeket elfogadja, azaz a norma ide vonatkozó rendelkezéseit, mint figyelmeztetést elolvasta, és annak ellenére cselekszik és/vagy annak tiltása végett a képküldéstől/fogadástól visszalép. A szoftver a hatályos szabályozásra figyelemmel annak változása esetén automatikusan frissítené magát, így igazodva az érvényben levő normaszövegekhez. Amennyiben a felhasználók a feltételek elfogadása mellett mégis úgy döntenek, hogy a megosztott tartalmat (amely akár bármi lehet) közvetítik, úgy az internetszolgáltató arról automatikusan, vagy rendszerezett jelleggel a rendvédelmi szervnek jelentést, vagy jelzést ad, akinek pedig az információt kötelessége ellenőrizni, szükség esetén az eljárást megindítani. A javaslatot olyan szempontú kritika érheti, hogy az interneten megosztott tartalmak ellenőrzésre a rendvédelmi szerv kellő kapacitással nem rendelkezik, azonban elgondolkodtató, hogy amennyiben egy olyan csúcsszerv kerülne kijelölésre, amely csak a Büntető Törvénykönyv e fejezetében foglalt bűncselekmények felderítésével foglalkozik, akkor a felderítés, és az ellenőrzés arányszáma egymással akár pozitívan is korrelálhat. (A csúcsszerv létrehozásáról a következő alfejezetben olvashatunk.) A kidolgozott szoftver alkalmazásának eredményessége akár elő-, és utóhatás vizsgálat keretében is tesztelhető, bármelyik a fiatalok által használt chatprogram felületén is.

4.5.5.3 Prevenciós tevékenység az internetszolgáltatók körében

Álláspontom szerint az internetszolgáltatók minden szerződés megkötésekor felmérhetnék, hogy az adott felhasználó családjában gyermekkorú az internet által nyújtott lehetőségeket használni fogja-e, vagy lehetősége van-e arra, hogy azokat használhassa. Ha már a gyermekkortól kezdődően biztosítjuk azt, hogy a gyermekek tudatosan és biztonságos internethasználatra törekedjenek, akkor a pedofil-hálózatok tevékenységét jelentős mértékben csökkenthetjük. Amennyiben olyan adat, és információ merül fel, hogy az adott felhasználó körében gyermekkorú személy is van, és annak opcionális lehetősége van arra, hogy az internetet használja, akkor olyan képzést kell tervezni és szervezni, amely a gyerekeket játékos formában az internet veszélyeire felhívja. Oktató jellegű kiscsoportos foglalkoztatások. A szülők részére pedig prezentálni kell, hogy milyen lehetőségeik vannak arra, hogy a gyermekeiket e káros hatásoktól megóvhassák. Amennyiben az internetszolgáltató ilyen jellegű képzést nem tervez, úgy elegendő volna, ha a felméréseket elvégezné, és arról a rendőrhatóságot értesítené. A rendvédelmi szerv pedig bűnmegelőzés keretében a szükséges felvilágosítást megadná, az előadásokat megtarthatná. Ilyen jellegű prevenciós intézkedések és felhívások az alábbiakban érhetők tetten: jelszavak védelme, azaz körültekintő jelszóválasztás, és biztonságos jelszókezelés-, tárolás. A közösségi hálózatok biztonsági beállításai, az adatvédelem jelentősége. Többlépcsős azonosítás, így például kód, telefonszám, biztonsági kérdések megadása.

4.5.5.4 Rendvédelmi tevékenység

Javaslatomban egy olyan nemzeti, regionális – az ország egészére kiterjedő – csúcsszerv létrehozása szerepel, amely a gyermekek szexuális kizsákmányolással érintett gyermekpornográfia bűncselekmények, valamint a hatályos Büntető Törvénykönyv nemi élet szabadsága elleni bűncselekmények fejezetében foglalt tényállások felderítését, az elkövetők szankcionálását, és az áldozatok reintegrálását a társadalomba a reszocializációs intézkedések megtételével biztosítja. Ha a terrorizmus leküzdésére önálló szervet foglalkoztatunk, akkor a gyermekek, és a nők szexuális kizsákmányolása megakadályozásának érdekében miért ne hozhatnánk létre egyet? Ha a számadatok bizonyítják, hogy az önállóan foglalkoztatott nyomozó csoport munkássága nem elég, akkor miért ne javíthatnánk az arányokon azzal, ha a feladatok végrehajtására egy teljes szervet hozunk létre? Azt is látjuk, hogy hiába Magyarország

Nemzetbiztonsági Stratégiája, és a lépcsőzetes jogszabályalkotás, és végrehajtás, ha a számadatok tükrében az áldozatok száma évről évre növekedik, és a nyomozások mindösszesen 10 százaléka indul a magyar rendvédelmi erők kezdeményezésére, a felének megfelelő, azaz 5 százalékban pedig külföldi kezdeményezésre indul meg a büntetőeljárás. Meddig kell még elmennünk, hogy felfogjuk, hogy a szexuális kizsákmányolás az emberi-, és alkotmányos jogok egyik legnagyobb, és legveszélyesebb eltiprója? Mennyi áldozatnak kell még szenvedni, és a sanyargatást eltűrni, hogy ráébredjünk, hogy a szervezett bűnözői csoportok, önálló tettesek által elkövetett szexuális kizsákmányoláson alapuló bűncselekmények ellen hatékonyabb fellépésre van szükség? Nem kell a régi hagyományokat megszüntetni, és kiirtani, csupán az új eszmék összehangolására, és a régiek beépítésére van szükség. Nem kell a nyomozócsoportok munkásságát megszüntetni, csupán a létrehozott új szerv szervezeti struktúrájába integrálni. Álláspontom szerint az országos hatáskörű szerv a szexuális kizsákmányolással érintett bűncselekmények mind nyílt-, mind pedig operatív területen alkalmazott nyomozását, valamint komplex módon az áldozatvédelmi tevékenység mellett, a reszocializációs intézkedések végrehajtását is magában foglalná. A nyílt-, és operatív területű nyomozások az alábbiak szerint alakulhatnak.

- A hatályos büntetőeljárásról-, valamint a rendőrségről szóló törvényben foglalt intézkedések összessége, különös tekintettel a nyomozások egységes és részletes szabályairól szóló utasítások, valamint az operatív tevékenység-, és a titkos információgyűjtés belső utasításainak végrehajtása, a nemzetközi irányelvek figyelembevételével.
- Az adott bűncselekményfajta elkövetési változatainak, illetőleg az adott esemény megvalósulása-, az érintett szereplők (akár elkövetői, akár sértetti kör) tipikus jellemzőinek, az elkövetés eszközeinek, módszereinek, különösképpen az azt elősegítő, és lehetővé tevő okok, körülmények tanulmányozása, a megvalósulás-, és elkövetés jellemzőinek aktív vizsgálata.
- A nyomozások szervezése, és tervezése mellett a rendelkezésre álló tárgyi-, és személyi adat-, információ-, és bizonyítékforrás beszerzése. A hazai és nemzetközi, nyílt-, és operatív területen beszerzett, elemzett és értékelt bűnüldözési információk összegyűjtése, tárolása, feldolgozása és cseréje. Fenyegetés-, és veszélyeztetettség értékelések, stratégiai elemzések elkészítése, amelyhez az általános helyzetjelentés párosításra kerül, amely alapján hazai-, és nemzetközi akciók megszervezése válhat szükségessé.

Az internetezés világában az a szép, hogy mindenki az lehet, aki csak szeretne. Álarcot húzunk, és számítógépek mögé bújunk. Javaslatomban az általános nyílt-, és operatív felhasználás mellett egy olyan konkrét nyomozási metódust szeretnék ismertetni, amely az elkövetők elfogását garantálja, illetőleg emellett prevenciós jelleggel is bír. Ha a pedofil személyek is kihasználják az internet névtelenségét, miért ne alkalmazhatná ezt a rendőrség is, miért ne fordíthatnánk a névtelenség előnyét a saját javunkra is? Véleményem szerint érdemes lenne elgondolkodnunk azon, hogy, ha mi is a névtelenség leplét magunkra öltenénk,

és olyan „fake” profilokat hoznánk létre, amire a bűnözői hálózatok harapnak, akkor egyrészt az elkövetőktől olyan információkat nyerhetnénk, amik hálózatok lebuktatásához vezethetnének, másrészt pedig egy-egy eredményes realizálás elhintené azt a magot, hogy a bűnözők is elgondolkoznának azon, hogy vajon a számítógép másik oldalán valóban az a kislány és/vagy kisfiú ül-e, vagy éppen a nyomozó hatóság egyik tagja, aki majd az elfogását végrehajtja. A „fake” profil megalkotásához, valamint a „csali” alkalmazásához különösebb szakértelem nem szükséges. Olyan legyártott, és előre alkotott tervek megszervezése, és lebonyolítása szükséges, amelyet a rendvédelem bűnügyi területén használt nyomozó személy is alkalmazni tud. A bűncselekmény elkövetésével gyanúsítható személyről is már kezdetlegesen elég információ, és adat áll rendelkezésre, amely az eljárás során felhasználható, illetőleg a bűncselekmény megelőző hatása is - mint a pszichológiai nyomásgyakorlás eszköze - érvényesül, amennyiben annak széles körben való elterjedéséről gondoskodunk.

4.5.5.5 Reszocializációs intézkedéssorozat

Önmagában egy bűncselekmény sértettje jogosulttá válik arra, hogy az elszenvedett – akár anyagi, akár lelki – károkat az állam helyreállítsa. Magyarországon nincs olyan szabályozás, amely a lelki károk enyhítését magára vállalná, és segítené a sértetteket, hogy a traumákat feldolgozzák. Bár az anyagi károk részleges helyreállítását bizonyos áldozatvédelmi tevékenységen alapuló norma biztosítja, az azonban olykor-olykor olyan kritériumokhoz kötött, amelynek teljesítése, vagy az annak való megfeleltetés kiváltságnak tekintendő. Gondoljunk abba bele, hogy életkortól függetlenül milyen érzés is lehet egy bűncselekmény sértettjének lenni, hát még, ha az abból eredendő trauma egy életen át kísért minket. A gyermekek internetes szexuális kizsákmányolása, valamint egyhangúlag a szexuális kizsákmányolással járó bűncselekmények áldozatai álláspontom szerint nemcsak anyagi, hanem lelki kártérítésre is jogosulttá válnak. A normaalkotás során figyelemmel kell arra lenni, hogy ezek az áldozatok az erőszak stigmáját örökre magukon hordják majd. Különös tekintettel arra, hogy az interneten a visszaélésre okot adó anyagok újra, és újra felbukkanhatnak, azzal bárki bármikor szembesülhet. Az áldozatoknak támogatásra van szükségük, hogy egyrészt azt a traumatikus élményt, amely a bűncselekmény okozott feldolgozni tudják, másrészt pedig azt annak tudatában tegyék, hogy a szexuális

kizsákmányolásról készült anyagok a virtuális térben örökre forgalomban vannak, azzal nemcsak ők maguk, hanem a világon élő összes felhasználó, leendő barátjuk és/vagy barátnőjük, családtagjaik, stb. találkozhat. Ezt semmilyen anyagi jellegű kártérítés nem tudja, és nem is tudná megoldani. Speciális segítségre van szükség, amely szakorvosok igénybevételét jelenti. Álláspontom szerint egy olyan rehabilitációs intézet létrehozására van szükség, ahol az áldozatokkal szakpszichiáterek, pszichológusok foglalkoznak, és mindezt egy olyan kidolgozott metódus szerint teszik, amely a sérült személyek egészséges testi-, lelki fejlődését a továbbiakban – a traumák feldolgozása mellett – biztosítja. Egy olyan védett szálláshely, ahol a sértetti gondozás, a szociális ellátással egybekötött.

4.5.5.6 Felderítés és kooperáció

A korábbi alfejezetekben ismertetett tevékenységen túlmenően annak megszervezésére van szükség, hogy az internetszolgáltatók a hazai rendvédelmi szervekkel együttműködjenek, valamint a hazai rendvédelmi szervek a nemzetközi társszervekkel kooperáljanak. Mindkettőben közös tevékenységi pont lehet a felderített visszaélések elemzése-értékelése, valamint az abból levonható konklúziók megosztása. Ezeknek az adatoknak az egymás általi megismerésre van szükség, tekintettel arra, hogy a „több szem, többet lát” metódus, valamint a „brainstorming” munkamorál az esetleges következtetésekből plusz információ levonására képes. Ez a plusz információ hozzásegíthet ahhoz, hogy újabb, még részletesebb javaslatok, és kidolgozott munkafolyamatok kivitelezésére legyen lehetőség. Érdemes megfontolnunk azt, hogy közös csoportok felállítására van-e szükség, akik akár negyedéves jelleggel munkaértekezleten vesznek részt, és az általuk feltárt dolgokat a másik szerv képviselőivel megosztják, majd együtt, közösen új, innovatív javaslatokat fogalmaznak meg. Az együttműködésnek a mennyiségi-, minőségi- a modor-, és a relevancia alapelveire tekintettel kell lennie. Az együttműködő szerveknek a mennyiségi alapelv szerint az összes szükséges, és megfelelő információt át kell adnia, nem adhatnak se kevesebbet, se többet, hiszen egy azonos cél lebeg előttünk, az pedig a bűnözés visszaszorítása. Ezeknek az információknak a minőségi alapelv alapján mindig hitelesnek kell lenniük, azokban torzítás nem szerepelhet. A relevancia mindig a tárgykör témájához kapcsolódik, természetesen a résztől az egészig, vagy az egésztől a részig eljuthatunk, de az információnak a témán belül kell maradnia. Ehhez kapcsolódik a mód alapelve is, hogy a csoportoknak csak olyan információ közlésére van

felhatalmazásuk, amellyel a partnereket nem vezetik félre, és kizárólag egzakt jellegűek. A szervek közötti együttműködés alapja biztosíthatja, hogy a gyermekek internetes szexuális kizsákmányolásával elkövetett bűncselekmények redukálódjanak.

Az ember a legérzékenyebb lény a Földön, s a legnagyobb szenvedést képes átélni. Ezért óriási felelősség, miként bánunk embertársainkkal. Ha az emberek alapvető jogai sérülnek, viselkedésük, gondolkodásuk, stratégiájuk, prioritásaik alapvetően változnak meg. Az emberi jogok sérülése az élet sok területét érinti: csorbul a gondolati szabadság, ami a legemberibb és az egyik legfontosabb emberi tulajdonság, gondolataink emelnek ki bennünket, általuk jutunk előre. Az ember alapvető szükséglete a testi-lelki szabadság. A szabadságának korlátozása, a lelek, személyiség, gondolkodás torzulását okozza. Az emberiség fejlődésének, fennmaradásának és jólétének alappillére a kultúra fennmaradása és fejlődése. Mindez háttérbe szorul. Az emberi kapcsolatok, az emberi közösségek, a társadalmi kapcsolatok leépülnek, torzulnak. Ez a jelen és az eljövendő nemzedékekre egyaránt negatív hatással van. A gazdaság teljesítménye csökken. Egyfajta ellenállás nyomán, ahol a közösségi célok háttérbe szorulnak, az egyéni célok, ill. a túlélést, az alkalmazkodást szolgáló célok kerülnek előtérbe. A környezetre szintén romboló hatással van. Az alapvető jogokért való küzdelem során, ill. a sérelmek elszenvedésekor a megváltozott prioritások között háttérbe szorul a környezet védelme, amely jóléti társadalmak esetében is extra erőfeszítéséket igényel. Miért fontos ez mindnyájunk számára, hiszen nem feltétlenül érintenek közvetlenül bennünket, távoli, ismeretlen emberekkel és országokban történnek? A népességnövekedés és a technikai fejlődés nyomán a távolságok lecsökkentek, egymásra ható globális rendszer alakult ki, melyben a gazdasági, politikai és kulturális egymásra hatás nagyban megnövekedett. A gazdasági és kulturális mellett a környezeti hatásokra ez fokozottan igaz. Az emberi jogok megsértőit / elnyomóit alantas és önző érdekek vezérlik. Mindig erőszak áll mögötte és erőszakot teremt. A történelem számtalanszor bebizonyította, hogy a társadalmi jólét és biztonság megteremtéséhez nincs szükség az emberi jogok tiprására, sőt ellenkezőleg, ahol tiporják e jogokat, ott sosem alakul ki jóléti, fenntartható társadalom. Ezért nélkülözhetetlen, hogy a szervezett bűnözéshez kapcsolódó szexuális kizsákmányolással érintett bűncselekmények ellen közösen fellépjünk.[275]

[275] KOVÁCS István: Az emberkereskedelemhez szorosan kapcsolódó prostitúciós bűncselekmények – különösképpen a gyermekprostitúció áldozatai emberi jogaiknak hazai és nemzetközi vonatkozásai. In: Polgári Szemle, 2014., 10. évf. 5-6. sz. – p.:418-431.

4.5.6 Záró gondolatok

A tanulmány elkészítésekor igyekeztem minden elméletben-, és gyakorlatban megszerzett tudásomat kamatoztatni, és azt a tudomány szolgálatába állítani, mindezt azért, hogy a társadalom perifériájára szorult szexuális kizsákmányolással érintett áldozatok, és sértettek megnyugvást lelhessenek. Igaz, hogy ebben a rendszerben nem vagyok más, mint egy homokszem, de tudjuk mire képes egy homokszem, ha az egy olajozott gépezetbe bekerül. A sivatag is sok-sok apró homokszemből épül fel, és milyen erőt rejt magában. A lelkem megnyugodott, már csak azért is, mert igyekeztem, és a mai napig próbálok tenni azért, hogy a társadalmi kirekesztés-, és a szexuális kizsákmányolással érintett bűncselekmények áldozatain segíthessek, akár erőmön felül is. A jövőben, és ezek után is próbálok azért tenni, hogy minél rövidebb idő alatt, minél hatékonyabb, és eredményesebb munkát végezhessünk, kivívva ezzel a társadalom megbecsülését. A tanulmány megjelentetésével, valamint annak felhasználásával oktatási anyag is készíthető, amit széles körben, akár nevelő intézményekben, szociális kulturális környezetben, és a rendvédelem gyakorlatának számára is mérföldkövet jelenthet. A tanulmány befejeztével számos kérdés még nyitottan maradt, amelyet további kutatásra ajánlanék. További kutatásra ajánlanám például a statisztikai mérőszámok részleteiben gazdag vizsgálatát, valamint a civil szervezetekkel, szerveződésekkel történő együttműködés kereteinek, és létjogosultságának megteremtésének igényét is.

Felhasznált irodalom

Szakirodalom

1. ALLEN Ernie: Child Pornography: Model Legislation & Global Review. – United States: International Centre for Missing & Exploited Children, 2013.
2. ATTWOOD Feona: Reading porn: The paradigm shift in pornography research. In: Sexualities, 2002., 5. évf. 1. sz. – p.:91-105
3. BAGNALL Roger, BRODERSEN Kai, CHAMPION Craige, ERSKINE Andrew, HUEBNER Sabine: The Ecyclopedia of Ancient History. – United States: Wiley-Blackwell, 2012.
4. BERGER Fred: Pornography, sex, and censorship. In: Social Theory and Practice, 1977., 4. évf. – p.: 183-209
5. BLASKÓ Béla, MIKLÓS Irén, PALLAGI Anikó, POLT Péter, SCHUBAUER László: Büntetőjog különös rész I. – Budapest-Debrecen: Rejtjel Kiadó, 2013.
6. BRAUN_CUORVILLE Debra et al: Exposure to sexually explicit web sites and adolescent sexual attitudes and behaviors. In: Journal of Adolescent Health, 2009., 45. évf. – p.: 156–162.
7. BROWNMILLER Susan: Against our Will: Men, Woman and Rape. – New York: Simon & Schuster, 1975.
8. CALDERONE Mary: Pornography as a public Health Problem. In: American Journal of Public Health, 1972., 62. évf. 3. sz. – p.: 374-376.
9. CAMERON Samul: Economics of pornography. In: BOWMAKER Simon (szerk.): Economics Uncut: A Complete Guide to Life, Death, and Misadventure. Cheltenham: Edward Elgar Publishing, 2005.
10. COHEN Jacob: Statistical Power Analysis for the Behavioral Sciences. – New Jersey: Lawrence Erlbaum Associates, 1988.
11. COOPERSTMIH Jonathan: Does your mother know what you really do? The changing image and nature of computer-based pornography. In: History and Technology, 2006., 22. évf. 1. sz. – p.:1–25.
12. COWAN Glen et. al: Dominance and inequality in X-rated videocassettes. In: Psychology of Women Quarterly, 1988., 12. évf. 3. sz. – p.:299-311.
13. CROFTS Thomas, LEE Murray: „Sexting", Children and Child Pornography. In: Sydney Law Review, 2013., 35. évf. 85. sz. – p.: 85-106.
14. DIÓS István, VICZIÁN János: Magyar Katolikus Lexikon I. – Budapest: Szent István Társulat, 2004.
15. DISLEY Emma, IRVING Barrie, HUGHES William, PATRUNI Bhanu: Evaluation of the implementation of the Europol Council Decision and of Europol's activities. – Santa Monica: Rand Corporation, 2012.
16. DONNERSTEIN Edward et al.: The findings and recommendations of the Attorney General's Commission on Pornography: Do the psychological "facts" fit the political fury? In: American Psychologist, 1987., 42. évf. p.: 946−953.; BALMER Steven: The Limits of Free Speech, Pornography and the Law. In: Aberdeen Student Law Review, 2010., 13. évf. 1. sz. – p.: 66-82
17. DONNERSTEIN Edward, BERKOWITZ Leonard: Victim reactions in aggressive erotic films as a factor in violence against women. In:Journal of Personality and Social Psychology, 1981., 41. év. 4. sz. – p.: 710-724
18. DWORKIN Alice, MACKINNON Andrea: Pornography and civil rights. – Minneapolis: Organizing Against Pornography, 1988.
19. ECK Beth: Nudity and framing: Classifying art, pornography, information, and ambiguity. In: Sociological Forum, 2001., 16. évf. 4. sz. – p.: 603-632

20. EGAN Timothy: Technology sent Wall Street into market for pornography. - New York: Routledge, 2000.
21. FAGAN Patrick: Internet pornography by the numbers; a significant threat to society. – Broomfield: Webroot Cyber Security, 2009.
22. FERGUSON Christopher, HARTLEY Richard: The pleasure is momentary the expense damnable? The influence of pornography on rape and sexual assault. In: HASSELT van Vincent (szerk.): Aggression and Violent Behaviour, 2009., 14. évf. 5. szám – p.: 323-329.
23. FEYERABREND Paul: A módszer ellen. – Budapest: Atlantisz Kiadó, 2002.
24. FINCKENAUER James, VORONIN Yuri: The Threat of Russian Organized Crime. – Rockville: National Institute of Justice, Issues in International Crime, 2001.
25. FISHER William, BARAK Azy: Pornography, erotica, and behavior: More questions than answers. In: International Journal of Law and Psychiatry, 14. évf. 1-2. sz. – p.: 65-83.
26. FISHER William, BARAK Azy: Sex education as a corrective: Immunizing against possible effects of pornography. In: ZILMANN Dolf, BRYANT Jennings (szerk.): Pornography: Recent Research, Interpretations, and Policy Considerations. – Hillsdale: Lawrence Erlbaum Associates, 1989.
27. FREDERICK Danny: Pornography and Freedom. In: Kritike, 2011., 5. évf. 2. sz. – p.: 84-95.
28. GAGNON John: Sexuality and Sexual Learning in the Child. In: GAGNON John (szerk.): Sexual Deviance. – New York: Harper and Row, 1967.
29. GILBERT Martin: Churchill: A life. – United States: Holt Paperbacks, 1992.
30. GLADFELDER Hal: Literature and Pornography 1660–1800. – United Kingdom: Oxford Handbooks, 2013.
31. GŐCZE István: A tudományos kutatás módszerei. In: Hadtudományi Szemle, 2011., 4. évf. 3. sz. – p.:157-166.
32. HAGGERSTRÖM-NORDIN Elizabeth et. al: Associations between pornography consumption and sexual practices among adolescents in Sweden. In: International Journal of STD and AIDS, 2005., 16. évf. – p.: 102-107.
33. HERTZBERG Hunt: Ed Meese and his pornography commission. In: New Republic, 1986., 14. évf. – p.: 21-24.; PALYS Ted: Testing the common wisdom: The social content of video pornography. In: Canadian Psychology, 1986., 27. évf. – p.: 22−35;
34. HOLDEN William: Mobile to adult: Personal services. – United Kingdom: Juniper Research, 2000.
35. HUER Jon: Art, Beauty, and Pornography: A Journey Through American Culture. - Buffalo: Prometheus Books, 1987.
36. HUGHES Donna: Men create the demand; Women are the supply. In: Safety at Work, 2000., 7. évf. – p.:10-14.
37. KÁROLI Gáspár: Szent Biblia. – Bp.: Magyar Bibliatársulat, 2010.
38. KATONA Tamás, LENGYEL Imre, PETRES Tibor, CSENDES Tibor: Statisztikai ismerettár. – Szeged: JATEPress, 1999.
39. KENDRICK Walter: The Secret Museum: Pornography in Modern Culture, Berkeley: University of California Press, 1987.
40. KIPNIS Laura: Bound and Gagged: Pornography and the Politics of Fantasy in America, Durham: Duke University Press, 1999.
41. KORPÁS Attiláné: Általános statisztika. – Budapest: NTK, 1996.
42. KOVÁCS István: A prostitúció jelensége és társadalmi kontrolljának vizsgálata empirikus módszerekkel PhD értekezés, Budapest, UNI-NKE, 2016.
43. KOVÁCS István: Az emberkereskedelemhez szorosan kapcsolódó prostitúciós bűncselekmények – különösképpen a gyermekprostitúció áldozatai emberi jogaiknak hazai és nemzetközi vonatkozásai. In: Polgári Szemle, 2014., 10. évf. 5-6. sz. – p.:418-431.
44. KOVÁCS István: Gésa kultúra, és japán prostitúció. In: Hadtudományi Szemle, 2017., 10. évf. 2. sz.
45. KOVÁCS István: Is the prostitution a threat/danger to a country's (national)security? In: National Security Review, 2017., 5. évf. 1. sz. – p.:12-24.

46. KOVÁCS László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák. – Budapest: Nemzeti Közszolgálati Egyetem, 2012.
47. KRONHAUSEN Eberhard, KRONHAUSEN Philips: The Psychology of Pornography. In: ARBARBANEL Aliza (szerk.): The Encyclopedia of Sexual Behavior. – New York: Hawthorn, 1967.
48. LANE Frederick: Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age. – New York: Routledge, 2000.
49. LEEUW Edith, HOX Joop, DILLMAN Don: International Handbook of Survey Methodology. - United Kingdom: Routledge, 2008.
50. LOCKE John: The second Treatise of civil Government. – England: Industrial Systems Research, 2009.
51. LUMBY Chatarine: Bad Girls: The Media, Sex and Feminism in the '90s. Australia: Allen and Unwin, 1997.
52. MACKINNON Catharine: Not a moral issue. In: Yale Law & Policy Review, 1983., 2. évf. 2. sz. – p.: 321-345.
53. MALAMUTH Neil et al: Developmental pathways into social and sexual deviance. In: Journal of Family Violence, 2010., 25. évf. – p.:141–148.
54. MALAMUTH Neil, BILLINGS Victoria: Why Pornography? Models of Functions and Effects. In: Journal of Communication, 1984., 34. évf. 3. sz. – p.: 117-129.
55. MALAMUTH Neil: Pornography. In: KURTZ Lester (szerk.): Encyclopedia of Violence, Peace, & Conflict. – Amsterdam: Elsevier Inc., 2008.
56. MASLOW Abraham: Motivation and Personality. – New York: Harper, 1954.
57. MCELROY Wendy: A Woman's Right to Pornography. – New York: St. Martin's Press, New
58. MICHELSON Peter: The Aesthetics of Pornography. – New York: Herder and Herder, 1971.
59. MILL John Stuart: On Liberty. – London: Longman, Roberts and Green, 1869.
60. MORIAS Richard et. al: Porn goes public. – New York: Forbes, 1999.
61. NARVESON Jan: Moral Matters. – Ontario: Broadview Press, 1993.
62. NAYLOR Thomas: From cold war to crime war. In: Transnational Organized Crime,1995., 1. évf. 4. sz. – p.:37-56.
63. OLEN Jeffrey et al.: Applying Ethics: A Text with Readings. – Belmont: Wadsworth Publishing Company, 2005.
64. OWENS Eric et al.: The Impact of Internet Pornography on Adolescents: A Review of the Research. – United Kingdom: Routledge, 2012.
65. PETIT Miguel Juan: Rights of the Child. – United Nations: Economic and Social Council, 2004.
66. PETRES Tibor, TÓTH László: Statisztika. – Budapest: KSH, 2006.
67. PUKLI Péter, VÉGVÁRI Jenő: A statisztika: tudomány és szakma. In. Statisztikai Szemle, 2004., 82. évf. 1. sz. – p.:5-30.
68. REA Michael: What is pornography? In: Noûs, 2001., 35. év., 1. sz. – p.: 118-145.
69. ROLPH Harris: Does Pornography Matter? – London: Routledge and Kegan Paul, 1961.
70. SIGEL Lisa: Governing pleasures: Pornography and social change in England, 1815–1914. – Piscataway: Rutgers University Press, 2002.
71. SLADE Joseph: Pornography and Sexual Repression: A Reference Guide, Westport: Greenwood Press, 2001.
72. SMITH Dwight: Some Things that may be more important to understand about Organized Crime than Cosa Nostra. In: University of Florida Lax Review, 1971., 24. sz. – p.: 1-30.
73. SOBLE ALAN: Pornography, defamation, and the endorsement of degradation. In: Social Theory and Practice, 1985., 11. évf. –p.: 61-87
74. SUSSMAN Steven: Sexual addiction among teens: A review. In: Sexual Addiction & Compulsivity, 2007., 14. évf. – p.: 257–278.
75. SZAKONYI Péter: A 100 leggazdagabb magyar 2015. – Budapest: Online Kft, 2015.
76. VARGHA András: Matematikai statisztika pszichológiai nyelvészeti és biológiai alkalmazásokkal. Budapest: Pólya Kiadó, 2000.

77. VATSZJAJANA Mallanaga: Kámaszútra. – Budapest: Librotrade Kft, 2002.Jacobellis vs. Ohio, 378 U.S. 184, 197 (1964)
78. WILSON Cody: Can pornography contribute to the Prevention of Sexual Problems? In: QUALLS Brandon et al. (szerk.): The Precention of Sexual Disorders: Issues and Approaches. – New York: Plenum, 1978.
79. WOLAK Janis et al.: Trends in youth reports of sexual solicitations, harrassment and unwanted exposure to pornography on the Internet. In: Journal of Adolescent Health, 2007., 40. évf. – p.: 116–126.
80. YBARRA Mitchell et al: Exposure to Internet pornography among children and adolescents: A national survey. In: CyberPsychology and Behavior, 2005., 8. évf. – p.: 473–486.
81. YEN Chang et al: Multi-dimensional discriminative factors for Internet addiction among adolescents regarding gender and age. In: Psychiatry Clinical Neurosciences, 2009., 63 évf. 3. sz. – p.: 357–364.
82. York, 1995.
83. ZÁVOTI József: Matematikai statisztikai elemzések 5., Kapcsolatvizsgálat: asszociáció, vegyes kapcsolat, korrelációszámítás. Varianciaanalízis (egyszeres osztályozás). – Nyugat-Magyarország Egyetem, TAMOP 4.2.5 pályázata, 2010.
84. ZILMANN Dolf, BRYANT Jennings: Effects of massive exposure to pornography. In: MALAMUTH Neil, DONNERSTEIN Edward (szerk.): Pornography and Sexual Aggression. – Orlando: Academic Press, 1984.
85. ZILMANN Dolf, BRYANT Jennings: Effects of prolonged consumption of pornography on family values. In: Journal of Family Issues, 9. évf. – p.: 518-544.

Jogszabályok

86. 2001. évi CVIII. törvény - az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről - – (hatályba lépett: 2001. december 24-én) (https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0100108.tv) (letöltés ideje: 2017.08.01.)
87. 2004/68/JHA - Combating of the sexual exploitation of children and child pornography - (hatályba lépett: 2003. december 22-én) (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33138&from=HU) (letöltés ideje:2017.08.01.)
88. 2012. évi C. törvény – a Büntető Törvénykönyvről – (hatályba lépett: 2012. július 13-án) (https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV) (letöltés ideje: 2017.08.01.)
89. 97/154/JHA - Joint action to combat trafficking in human beings and sexual exploitation of children – (hatályba lépett: 1997. február 24-én) (http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:l33072) (letöltés ideje:2017.08.01.)
90. A Kormány 1139/2013. (III. 21.) Korm. határozata - Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. (http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf) (hatályba lépett: 2013. március 22-én) (letöltés ideje: 2017. augusztus 05.)
91. Amszterdami Szerződés - Az Európai Unióról szóló szerződés, az Európai Közösségeket létrehozó szerződések és egyes kapcsolódó aktusok módosításáról -, 1997. október 02-án, (letöltés ideje: 2017. 07. 12.)
92. Convention on Cybercrime – Council of Europe - (hatályba lépett: 2001. november 23-án) (http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf) (letöltés ideje: 2017.08.01.)

93. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse - Council of Europe - (hatályba lépett: 2007. október 25-én) (https://rm.coe.int/168046e1e1) (letöltés ideje: 2017.08.01.)
94. Convention on the Rights of the Child - Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20. November 1989. – (hatályba lépett: 1990. szeptember 02-án) (http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx) (letöltés ideje: 2017.08.01.)
95. Directive 2011/93/EU - of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework- Decision 2004/68/JHA – (hatályba lépett: 2011. december 17-én) (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0064&from=HU) (letöltés ideje:2017.08.01.)
96. Hágai Program – A szabadság, a biztonság, és a jog érvényesülésének erősítése az Európai Unióban – 2005. március 03-án (http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52005XG0303(01)), (letöltés ideje: 2017. 07. 12.)
97. Maastrichti Szerződés – Az Európai Unióról szóló szerződés -, 1992. február 07-én, (https://europa.eu/european-union/law/treaties_hu), (letöltés ideje: 2017. 07. 12.)
98. Nizzai Szerződés – A Bizottság összetételének módosításáról, illetve a tanácsi szavazási rendszer átalakításáról -, 2001. február 26-án, (https://europa.eu/european-union/law/treaties_hu), (letöltés ideje: 2017. 07. 12.)
99. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography - Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25. May 2000. – (hatályba lépett: 2002. január 18-án) (http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx) (letöltés ideje: 2017.08.01.)
100. Szerződés az Európai Alkotmány létrehozásáról – Rómában -, 2004. október 29-én, (https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_hu.pdf) (letöltés ideje: 2017. 07. 12.)
101. The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2014. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014), (Letöltés ideje: 2017. augusztus 20.)
102. The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2015. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015), (Letöltés ideje: 2017. augusztus 20.)
103. The EU Internet Organised Crime Threat Assessment's (iOCTA) report in 2016. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016), (Letöltés ideje: 2017. augusztus 20.)
104. The International Association of Internet Hotlines (INHOPE) report 2012-2014. (http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx), (Letöltés ideje: 2017. augusztus 20.)

DÉRI ATTILA

NAPJAINK INFORMATIKAI KIHÍVÁSAI - GONDOLATOK A KRITIKUS INFRASTRUKTÚRÁK INFORMATIKAI SÉRÜLÉKENYSÉGÉRŐL ÉS VÉDELMÉRŐL

1. Bevezetés

A XXI. században a technikai fejlődésével az informatika az élet újabb területeit hódította meg. Ez a változás megjelenik a mindennapjainkban is. Könnyítheti, kényelmesebbé teheti az életünket, de nehézségeket, biztonsági kihívásokat is hozhat.

Napjainkban előtérbe került az interneten keresztüli ügyintézés. Az elektronikus ügyintézésnek jelentős előnyei vannak, ilyen lehet például a kényelmes, otthonról történő ügyintézés. Azonban a hátrányairól sem szabad megfeledkezni. Ezek lehetnek az ügyintézéshez szükséges programok nem megfelelő minősége, digitális kompetenciák hiánya, stb. A dolgozatom első részében ezzel foglalkozom, a felhasználói oldalra helyezve a hangsúlyt.

A dolgozatom második részében az informatikai biztonság kérdéskörét járom körül, részletezve két idei, az informatikai rendszerek elleni támadást.

Az informatika elterjedésével új biztonsági kihívások jelentkeztek, mivel megjelentek a számítógépes adatlopások, vírusok, stb. A bűnözők felismerték az ebben rejlő lehetőségeket. Dr. Bencsik Balázs, a Nemzeti Kibervédelmi intézet vezetőjének becslése szerint, jelenleg a kiberbűnözéssel okozott kár a világgazdaság 1%-val mérhető össze, és megelőzi a kábítószer-kereskedelemből származó bevételt is (https://www.vasarnapihirek.hu/fokusz/ a_drognal_is_nagyobb_uzlet).

Az elektronikus ügyintézés megjelenése is új biztonsági intézkedéseket igényel. Ma már az interneten keresztül el lehet érni azokat a hatóságokat, állami-, illetve a versenyszférában működő cégeket, melyek biztonságkritikus rendszereket üzemeltetnek. Ezeknek a rendszereknek a működtetése fokozott biztonságot tesz szükségessé.

Nem csak napjaink jelensége a terrorizmus. Az idősebb nemzedék emlékezhet a Vörös brigádok, ETA, stb. terrorszervezetekre, melyek Európa különböző országaiban hajtottak végre merényleteket. A terrorizmus az utóbbi években újra felütötte fejét.

A terrortámadások célpontjai lehetnek a kritikus infrastruktúrák informatikai rendszerei. Eddig nem jutott tudomásomra sikeres terrortámadás a kibertérben a kritikus informatikai rendszerekkel szemben.

A biztonság növelése érdekében új, megelőző lépéseken is el kell gondolkozni. Az eddig tudomásomra jutott esetekből kitűnik a fokozott sértetti közrehatás. A lehetséges sértettek felvilágosításával, oktatásával az informatikai biztonság nagymértékben növelhető lenne.

A technológia fejlődésével létrejött egy új hadviselési forma a kiberhadviselés. A szakértők a hadviselés új, ötödik hadszínteréről beszélnek a föld, a víz, a levegő és a világűr után. Ez az új hadszíntér a kibertér. Itt említeném meg, mint tipikus példát, az iráni atomprogram elleni kibertámadást. A kritikus infrastruktúrák is lehetnek a kiberhadviselés célpontjai, hiszen így megbénítható egy ország közüzemi (víz, gáz, villany) hálózata, lakosságának ellátása, vasúti hálózata, légiközlekedése, egészségügyi rendszere, stb. A pályamunkámban a jelentőségétől függetlenül a kiberhadviselést nem részletezem.

Sajnos az informatikai támadások kapcsán megjelent a politika is. Példaként említeném a BKV bérlet- és menetjegyvásárlási rendszere elleni támadást, és az azt követő politikai csatározást. A dolgozatomban a politikai oldallal nem foglalkozom, csak az informatika oldaláról mutatom be a sérülékenységeket, a támadásokat.

2. Elektronikus ügyintézés előnyei és hátrányai

Az informatikai rendszerek fejlődésével, elterjedésével az állami és a magánszférában is felismerték, hogy az ügyintézést érdemes átterelni informatikai útra. Az ügyfelek az interneten keresztül, a weboldalakon lévő információk alapján tájékozódhatnak, elektronikus úton adhatják be irataikat (pl.: kérvények, panaszok, stb.), e-mailben kaphatják meg számláikat. Az elektronikus ügyintézés előnyei mellett megjelentek hátrányai is. Meglátásom szerint az elektronikus ügyintézést a lehető legegyszerűbbé kell tenni, hogy vonzó legyen az emberek számára. Ebben a fejezetben erről lesz szó.

2.1. Informatikai háttér megteremtése

Az elektronikus ügyintézés alapfeltétele a megfelelő informatikai háttér megteremtése. Gondolok az internet felől elérhető, interaktív weboldalak megírásától, beüzemelésétől, az elektronikus ügyintézés miatt várhatóan megnövekvő e-mail forgalom kiszolgálását végző munkaállomások beállításáig. Gondoskodni kell a weboldalak, számítógépek frissítéséről. Az informatika fejlődésével naponta jelennek meg új technológiák. Ezek bevezetése is jelentős plusz feladatot, költséget eredményezhet. Példaként említeném meg, hogy a régebben fejlesztett Java nyelven írt programok között van olyan, ami nem kompatibilis az újabb Java futtató környezettel.

Az informatikai háttérnél meg kell külön említeni, hogy az ügyintézésre szolgáló webszervereken futó programoknak hozzá kell férni az adott szervezet belső szerverein lévő adatbázisokhoz, a bejövő leveleket továbbítani kell a belső rendszeren lévő munkatársakhoz. Ez biztonsági kockázatot hordozhat magában.

Az informatikai hátteret – ha a fogalmat bővebben értelmezzük – a felhasználóknak is meg kell teremteni. Környezetemben az idősebb korosztály nem rendelkezik számítógéppel, okostelefonnal, internethozzáféréssel, valamint informatikai tudással.

Azt tapasztalom, hogy az elektronikus ügyintézés lehetősége nem elég motiváló számítógép vásárlására, bővítésére, informatikai tudás elsajátítására.

2.2. Azonnali rendelkezésre állás

A XXI. században sok helyen rendelkezésünkre áll az internet, és sok embernek van internet használatra alkalmas számítástechnikai eszköze (számítógép, mobiltelefon, stb.). A mobiltelefonhálózatok fejlődésével egyre több helyen érhető el telefonról is az internetet. Azonban vannak még olyan helyek, ahol nem tudjuk használni a mobiltelefonunkat. Ilyenek lehetnek például a magas hegyeken lévő lefedetlen helyek, repülőgépek fedélzete, stb. Külföldi kiránduláskor nehézséget okozhat a mobilinternet használatának jelentős költsége. Az előző részben már esett szó arról, hogy az idősebb korosztály nem rendelkezik

internetelőfizetéssel és számítógéppel. Ezek a tényezők nehezítik az elektronikus ügyintézés elérését.

Az informatikai rendszeren végzett ügyintézésnek nagy előnye, hogy bármikor tudjuk az ügyintézést kezdeményezni. Nem kell várnunk a hivatal kinyitására, nem kell sorba állni, nem kell szabadságot kivenni, nem kell utazni.

Az ügyek feldolgozását sok esetben lehet algoritmizálni, gépesíteni, ezért ezekben az esetekben nem szükséges az emberi beavatkozás. Példaként említeném a tantárgyak felvételét az egyetemeken működő Neptun programban, vagy a banki átutalást. Abban az esetben, ha az ügyintézéshez emberi beavatkozás szükséges, az rendszerint munkaidőben történik. Ritka az elektronikusan beküldött anyagok azonnali feldolgozása 7/24 órás rendszerben.

Az elektronikus ügyintézésben a kommunikáció kiterjeszthető oly módon, hogy az okostelefon, vagy a megfelelő szenzorokkal felszerelt számítástechnikai eszköz, bizonyos események bekövetkezésekor automatikusan küldjön sms-t, e-mailt. Lehetséges más jellegű internetes kommunikáció is. Erre jó példa a vészhívások helyének lokalizálására szolgáló, az Android operációs rendszerű mobiltelefonokra telepíthető Advanced Mobile Location (AML) alkalmazás. Az alkalmazás a segélyhívó központ hívásakor automatikusan, sms-ben elküldi a telefon földrajzi koordinátáit. Az alkalmazás a GNSS (global navigation satelit system), köztudatban lévő nevén GPS alapján határozza meg a telefon helyzetét. Az ügyintézés ilyen irányú kiterjesztése esetén a fogadó központnak, illetve a mögötte álló kiszolgáló rendszernek is fel kell készülni az üzenetek fogadására. Az AML alkalmazás esetén a segélyhívó központnak és az általa irányított egységeket is fel kell szerelni megfelelő technikával, informatikai alkalmazásokkal, ki kell alakítani az új munkamódszereket. Ebben az esetben olyan alkalmazásra gondolok, amely térképen mutatná a hívás helyét, illetve a helyszínre kivonuló járművekben is lenne egy térképes megjelenítő eszköz. Az ilyen alkalmazásokkal lehetne csökkenteni az operátorok leterheltségét, illetve a helyszínre vonuláshoz szükséges időt.

2.3. Az AVDH szolgáltatás egyszerűsítése

Az elektronikus ügyintézés térhódítása, valamint a jogszabályi környezet változása miatt úgy gondolom, hogy egyre többen fogják használni az elektronikus aláírást. Sajnos az informatikai szakemberek egy része sincs tisztában az elektronikus aláírás fogalmával, annak részeivel, funkciójával. Itt gondolok az aláírt irat megváltoztathatatlanságát biztosító hash adatra, időbélyegzőre, az aláíró azonosítására szolgáló adatokra.

Az Ügyfélkapurendszerben felhasználói fiókkal rendelkezők az irataikat elektronikusan aláírhatják az Ügyfélkapuhoz kapcsolódó Azonosításra Visszavezetett Dokumentum Hitelesítés (AVDH) szolgáltatással. Személyes tapasztalatom alapján fontosnak tartom a szolgáltatás megújítását, hogy az informatikában járatlan személyek is könnyebben írhassák alá irataikat. Az AVDH szolgáltatás elérése sokkal könnyebb lenne, ha az Ügyfélkapu felületére is ki lenne rakva. Az aláírható dokumentumok formátumának bővítését is fontosnak érzem. A pdf formátum mellett jó lenne, ha a program fogadni tudná a word, szövegszerkesztő program doc, docx formátumát, valamint az open office ODF formátumát is. Előre mutató lenne az AVDH honlapján történő szövegszerkesztési lehetőség megteremtése is.

Jelentős akadálynak gondolom, hogy az Ügyfélkapu a legtöbb ügyintézési formánál egyirányú. Nagy könnyebbség lenne, ha az Ügyfélkapun keresztül be tudnánk nyújtani elektronikusan aláírt iratokat. Jelenleg az ABEV Java program segítségével tudunk küldeni iratokat, viszont – tapasztalataim alapján – annak telepítése, az űrlapok letöltése sokszor nehézségbe ütközik az átlagos felhasználónak. Ez utóbbi miatt lenne könnyebbség az iratok Ügyfélkapun keresztüli benyújtása.

Az AVDH használata biztonsági problémákat is felvet. Az Ügyfélkapus bejelentkező nevünkkel és jelszavunkkal tudjuk használni az AVDH szolgáltatást. Az Ügyfélkapus azonosító adatainkra nagyon kell vigyáznunk, mert ha azok illetéktelen kezekbe kerülnek, akkor a nevünkben bármilyen elektronikus iratot alá tudnak írni. Javaslom az AVDH szolgáltatáshoz a dupla autentikáció bevezetését a biztonság növelése érdekében.

3. Kritikus infrastruktúra

A pályamunkám további részében az informatikai támadásokkal foglalkozok. Az informatikai sérülékenység és a támadások bemutatásakor sokszor lesz szó a kritikus infrastruktúráról, ezért először azt definiálom.

Általánosságban infrastruktúrán azon eszközök, intézmények összességét értjük, amelyek bár nem részei a közvetlen termelési folyamatnak, viszont annak nélkülözhetetlen feltételei. (Belügyi Szemle 2011/2 szám 27. old.)

Az infrastruktúrát többféleképpen csoportosíthatjuk. Beszélhetünk energia-, közlekedési-, telekommunikációs infrastruktúráról. Tágabb értelemben oktatási, egészségügyi, honvédelmi, rendvédelmi, stb. intézmények hálózatát is infrastruktúrának nevezhetjük.

Hagyományosan biztonságkritikusnak nevezzük azokat az egyedülálló (stand-alone) mérnöki rendszereket vagy alkalmazásokat, amelyek működése emberéleteket veszélyeztető baleseti kockázatokat rejt, és/vagy a hibás működésük nagyon jelentős gazdasági, környezeti vagy akár szociális károkat okozhat (Biztonsági kihívások a 21. században 345. old.).

A kritikus infrastruktúra: a nemzeti és uniós infrastruktúra azon létfontosságú elemei, melyek jelentős károsodása, üzemzavara vagy megsemmisülése esetén, súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére (Belügyi Szemle 2011/2 szám 27. old.).

Teljesség igénye nélkül a kritikus infrastruktúrák:

- energiatermelő és elosztó infrastruktúrák
- banki és pénzügyi infrastruktúrák
- vízellátó és közmű infrastruktúrák
- távközlési és kommunikációs infrastruktúrák

- szállító infrastruktúrák
- katasztrófavédelmi infrastruktúrák (rendőrség, tűzoltóság, egészségügy, stb.)
- honvédelmi, katonai infrastruktúrák
- élelmiszer-ellátási infrastruktúrák

A kritikus infrastruktúra működését számítógépes rendszerek segítik. Ezek lehetnek teljesen automatizáltak is, természetesen emberi felügyelet mellett. Ilyenek működnek például az energiaelosztó infrastruktúrában. A kritikus infrastruktúrában működő rendszerekről sokszor elmondható, hogy biztonságkritikusak is.

A mai világban gyakran lehet hallani informatikai támadásokról. Sajnos ezek a kritikus infrastruktúrát sem kímélik. A kritikus infrastruktúra elleni informatikai támadás irányulhat a szerverek, a számítógépes hálózat ellen, de irányulhat az adatok felhasználási helyén lévő munkaállomások ellen is. Azt gondolhatjuk, hogy a munkaállomások elleni támadás nem okoz jelentős kárt, mert a fontos adatok a szerveren tárolódnak. Azonban a munkaállomásokon is lehetnek olyan adatok, melyek törlése nagy veszteséget jelent. A munkaállomások tömeges kiesése is károkat okoz, azok újratelepítése jelentős időt igényel, és a költsége sem elhanyagolható. A munkaállomások kiesését egy példával szemléltetném. Képzeljük el azt az esetet, hogy bemegyünk az orvoshoz és nem működik a számítógépe, nem látja a leleteinket, nem tud receptet felírni, röntgenfelvételt készíteni, stb.

4. Kiberfizikai rendszerek

Az infrastruktúrák kérdéskörét tárgyalva nem mehetünk el a kiberfizikai rendszerek mellett. A hétköznapi eszközeinkben is használunk beágyazott számítógépeket. Ezek a számítógépek az eszközeink működését szabályozzák. A szabályozások lehetnek nagyon egyszerűek, de nagyon bonyolultak is. Ezeknek a számítógépeknek az összekapcsolását hívjuk kiberfizikai rendszereknek. Ilyen értelemben például egy okos ház is kiberfizikai rendszer.

Tudományos definíció: kiberfizikai rendszer alatt (angolul „cyber-physical system“ - CPS) az informatikai, szoftvertechnológiai, valamint mechanikai- és elektronikai elemek egységbe kapcsolását értjük, ahol az elemek egy olyan „adat-infrastruktúrán” keresztül kommunikálnak egymással, mint pl. az internet. A kiberfizikai rendszer egyik legfőbb jellemzője az igen magas fokú összetettség (komplexitás). A kiberfizikai rendszerek kialakítása beágyazott rendszerek hálózatba kapcsolása révén jön létre vezetékes illetve egyre inkább vezeték nélküli kommunikációs hálózatok segítségével.

Az életünk számos területét átszövik a kiberfizikai rendszerek. A kiberfizikai rendszerek biztosítják több kritikus infrastruktúrának a működését, pl.: a villamosenergia hálózat működését. A kiberfizikai rendszerek jelentős része biztonságkritikus, ezért ezeknek a hibás, sérült vagy rosszindulatúan módosított működése emberéletet követelő baleseteket, ellátási zavarokat, környezeti katasztrófákat eredményezhet. Ezért elvárás, hogy ezek a rendszerek megbízhatóan működjenek. Ez a megbízhatóság messze felülmúlja a hétköznapi életben használt programoktól megszokott megbízhatóságot. Ha a Windows operációs rendszer alatt futó program lefagy, vagy munka közben újra kell indítani a Windowst, az általában nem okoz gondot. A biztonságkritikus kiberfizikai rendszereknél az ilyen újraindítás elképzelhetetlen.

Az informatika és a mérnöki tudományok fejlődésével új kiberfizikai rendszerek fognak megjelenni, amik új biztonsági kihívásokat is tartogatnak. A jövőben ezeknek a biztonsági kihívásoknak is meg kell felelnünk.

5. Informatikai kockázatok és azok csökkentése

Az informatikai támadások igyekeznek kihasználni az informatikai rendszerek, programok sérülékenységeit, gyenge pontjait. Ezek a gyenge pontok eredhetnek a programok, valamint a felhasználók hibáiból is. A következő részben ezekről a hibákról, mint kockázati tényezőkről és azok csökkentésének lehetséges módjairól lesz szó.

5.1. Sértetti közrehatás

Az informatikai bűncselekmények közül az eddig tudomásomra jutott esetek jelentős részében meghatározó volt a sértetti közrehatás. A sértettek informatikai biztonsági ismereteinek alacsony szintje, és ebből eredően a programok kezelésének és karbantartásának hiányosságai jelentősen növelik az elkövetők esélyeit. A teljesség igénye nélkül néhány főbb hiányosságot vázolok fel. Ezek a hiányosságok nemcsak a munkahelyeken, hanem otthoni környezetben is növelik az esetleges támadások sikerét.

A sikeres támadások első okaként kell megemlíteni a programok elavultságát. Legfontosabb lenne az operációs rendszer frissítése. Az operációs rendszerekhez a kibocsájtásuk után több évig készítenek frissítő állományokat. A támogatási időszak operációs rendszerenként változik. A felhasználói szoftvereket gyártó cégek – egy idő után – a már nem támogatott operációs rendszereken futó programjaikat sem frissítik. Lehetőleg ne használjunk olyan operációs rendszert, melyre már nem készítenek frissítéseket.

Sok cégnek inhomogén gépparkja van. Számítógépeiket eltérő időpontokban, és más-más cégektől vásárolták, ezért különböző időpontokban avulnak el. Sok helyen az a gyakorlat, hogy a számítógépeken az operációs rendszert ritkán cserélik le, gyakorlatilag egy számítógépen a rendszerbe állítástól a kivonásig ugyanaz az operációs rendszer fut. Ez abból is adódhat, hogy az új operációs rendszereknek gyakran magasabb a hardver igénye, mint a régieknek. Elmondható, hogy sok helyen a régi, elavult operációs rendszerek száma az adott cég hardver beruházásainak függvénye. Ezért fordulhatnak elő jelentős számban a régi, már nem támogatott operációs rendszerekkel működő számítógépek.

Fontos, hogy az operációs rendszerre kiadott minden frissítést lehetőleg minél hamarabb futtassuk le. A frissítések futtatását sokszor a felhasználók is elvégezhetik. Viszont nem egy felhasználónál látom, hogy a frissítések futtatását rendszeresen kihagyja. Halottam olyan vélekedést, hogy minek azt futtatni, értékes időt vesz el a munkától. Ők valószínűleg nem tudják, hogy a frissítések elhanyagolása is hozzájárulhat több vírus terjedéséhez, ez történhetett például a WannaCry vírus esetében is. Itt említeném meg, hogy a Windows alapú hálózatokat be lehet úgy állítani, hogy a

munkaállomásokon a frissítéseket csak rendszergazdai jogosultsággal rendelkező felhasználó tudja lefuttatni. Ez a beállítás nagy hálózatok esetében nagyon leterheli az informatikusokat, az összes számítógépen a frissítések futtatása nagyon sok időt vesz igénybe, extrém esetben – a gépek nagy száma miatt – lehetetlen a frissítés elvégzése.

A Windows operációs rendszer verziójáról a parancssorba begépelt winver utasítással győződhetünk meg. Ez a parancs nemcsak a fő verziót (pl.: Windows 7, Windows 8, Windows 10), hanem az alverziót (pl.: 1703) is kiírja. A Windows 10-nél az alverzió az adott módosítás kiadásának dátumára utal. A Windows XP operációs rendszer SP2 verziójában jelent meg az új parancssor, a powershell. Ezt a régi, DOS-ból örökölt parancssor utódjának szánta a MicroSoft. A powershell-ben a get-hotfix paranccsal tudjuk kiíratni, hogy milyen frissítések futottak le az adott operációs rendszeren.

Az operációs rendszeren kívül a többi programot is fontos frissíteni. Az internet felöl jövő támadások kivédése szempontjából fontos a webböngésző és ahhoz kapcsolódó megjelenítő programok (pl.: Adobe Flash) frissítése. Ide sorolnám a Java futtató környezetet is. Sajnos ezeknek a programoknak a frissítését nem, vagy csak késve követik a felhasználói programok. Példaként említem, hogy az idei év szeptember 21- én kiadott Java SE 9 alatt – e sorok írásakor – nem fut a NAV nyomtatványkitöltő programjának aktuális verziója (v2.77) (http://www.uzletresz.hu/penzugy/20170927- nem-kompatibilis-a-java-a-nav-nyomtatvanykitoltojevel.html). A programok frissítése, újabb verziókra történő áttérés azért is fontos, mert több szoftvercég a régi verziójú programjaiban kevésbé törődött a biztonsággal. A felhasználói programoknál is előfordulhat az, hogy a frissítések futtatásához rendszergazdai jogosultság kell, ami szintén megnehezítheti a programok frissítését.

Azt is el kell ismerni, hogy a napi munkához egy szervezet számtalan programot használhat, amikhez rendszeresen érkeznek frissítések. A frissítések telepítése előtt szükséges azok tesztelése, hogy használatuk nem akadályozza-e a napi munkát. A frissítő állományok tesztelése, telepítése jelentős humánerőforrást igényelhet, ami nem biztos, hogy rendelkezésre áll.

Szintén biztonsági kockázatot hordoz magában a nem megfelelő felhasználói szoftverek választása. A szoftverek jelentős része tartalmaz biztonsági réseket. Figyeljünk

oda, hogy megfelelő biztonságú programokat használjunk. A víruskereső megválasztása is fontos, hiszen az biztosítja a számítógép megfelelő védelmét.

A felhasználók gondatlansága is biztonsági kockázatot hordozhat. Nagyon sok felhasználó gondolkodás nélkül nyitja meg az e-mailekhez kapott csatolmányokat. Ezek a csatolmányok lehetnek rosszindulatú kódot tartalmazó programok is. A rosszindulatú programok lehetnek különböző vírusok, akár zsarolóvírusok, de nyithatnak úgynevezett hátsó kaput (back door) az operációs rendszeren, melyen keresztül a bűnözők kívülről, az internet felől be tudnak jelentkezni az operációs rendszerbe, és rendszergazdai jogokkal tudnak kárt okozni.

Azoknál a cégeknél, hivataloknál, ahol ügyfélforgalom is van különösen fontos az informatikai eszközök elhelyezése, fizikai védelme is. Ez különösen igaz a kritikus infrastruktúrához tartozó cégeknél, hivataloknál. Sajnos azt tapasztalom, hogy ez a szemlélet még nem ment át a köztudatba. Az egyik kórházban láttam, hogy a lokális hálózat switcheit tartalmazó üvegfalú rack szekrényt a betegek, illetve a vizsgálatokra érkezők által elérhető helyen, kb. 1 méter magasságban helyezték el. Szintén kórházban láttam, hogy a szerverhelyiség a betegfelvételi pulttal szemben található, amire az ajtón olvasható felirat hívta fel a figyelmet.

Végül, de nem utolsó sorban a mentések fontosságára hívnám fel a figyelmet. A számítógépünkben található adathordozók (merevlemez, SSD) tartalmát rendszeresen mentsük külső eszközre. Az informatikai eszközök fejlődésével a vírusok is fejlődtek. Már nem jelent biztonságot a NAS-ra illetve a felhőbe végzett mentés. Vírusfertőzés esetén a NAS-on illetve a felhőben lévő adataink is károsodhatnak. Sok munkahelyen csak a szerver merevlemezeiről készül biztonsági mentés. A munkaállomások adathordozóit nem mentik. Sajnos sok munkáltató a szerverein nem biztosít elegendő tárhelyet a munkavállalóknak, ezért a munkavállalók a saját munkaállomásukon lévő merevlemezt, SSD-t használják adataik tárolására. Ezek az adatok megsemmisülhetnek egy meghibásodás illetve egy vírusfertőzés következtében.

5.2. Oktatás fontossága

Az informatika gyors fejlődése megkívánja, hogy az informatikai szakemberek is és a felhasználók is tovább képezzék magukat. A folyamatos tanulást az is indokolja, hogy az iskolarendszerű oktatásból kikerült fiatal munkavállalók a legújabb technológiát ismerik és velük kell felvenni a versenyt az idősebb korosztálynak. Sajnos elmondható, hogy sokan önerőből nem akarnak tanulni és azt várják, hogy a munkáltatója iskolázza be őket.

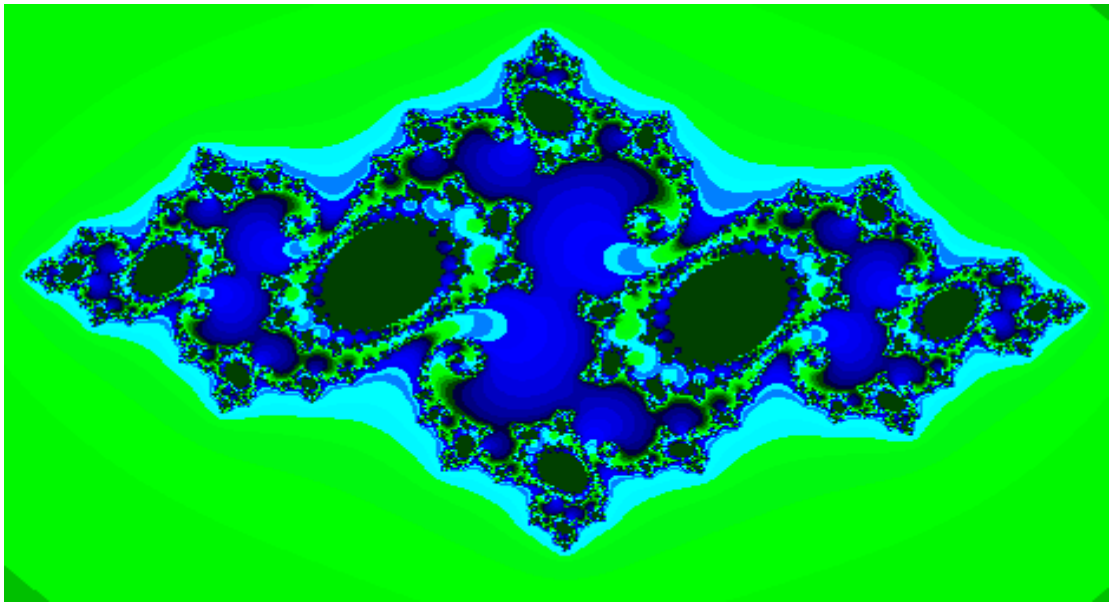
A számítógépes biztonság is olyan terület, ahol szintén szükséges a rendszeres tanulás. Az ismeretek nagyrészét újságcikkekből, internetről lehet elsajátítani. Sajnos kevés a tanfolyam és azok is viszonylag drágák. Néhány éve még a legmagasabb szintű nemzetbiztonsági átvilágításnak kellett átesniük a számítógép biztonsági tanfolyamra jelentkezőknek (Forbers NEXT magazin 2017. nyár 35. old.).

Az informatikai szakembereknek az informatikai biztonság széleskörű oktatása különösen fontos lenne, hiszen sokaknak hiányos ismerete van ezen a területen. Erre az eddig tudomásomra jutott esetek is utalnak. Több esetben, a sértettek által alkalmazott informatikusok, a biztonságra nem gondolva, gondatlanul alakították ki az informatikai rendszereket és ez segítette a kiberbűnözőket a bűncselekmény elkövetésében. Az oktatás során figyelembe kell venni a szakmai sajátosságokat, hiszen egy rendszergazdának más ismeretre van szüksége, mint egy programozónak.

A felhasználók informatikai ismeretei is sok esetben hiányosak. A 45 évesnél idősebb korosztály esetében a legfőbb okot abban látom, hogy nem nőttek bele az informatikába, gyerekkorukban nem volt lehetőségük elérni a számítógépeket. Az informatika elérhetővé válásával a 80-as, főleg a 90-es években sokan vásároltak számítógépet gyerekeiknek, de a szülők annak használatát ritkán tanulták meg. Később az élet kényszerítette ki, hogy elsajátítsák a munkához, életükhöz szükséges informatikai ismereteket. Általánosságban – életkortól függetlenül – elmondható, hogy a hiányos ismeretekhez az érdeklődés hiánya is vezethet. Sokan nem természettudományos, vagy műszaki érdeklődésűek, idegen tőlük az informatika, a számítógép világa. A gondolkodásuk is távol áll a matematikai vagy a mérnöki gondolkodástól. Ezekhez az emberekhez közelebb kell vinni az informatikát. A programok minősége is szülhet

nehézségeket, ami elfordítja az embereket az informatikától. Sokszor hallok olyan vélekedést, hogy ez a probléma sem lenne, ha a „… programot” nem kellene használni.

A következő képpel egy olyan oldalról szeretném megmutatni a matematikát, ami sokkal izgalmasabb és nem olyan „száraz”, mint a számok világa. Természetesen itt is komoly „számtan” van, de remélem, hogy ezt feledteti a látvány.



1. A matematika „színes” világa – Julia halmaz ábrázolása a szerző programjával

A leírtak miatt a felhasználókat is szükséges az ő szintükhöz igazodó oktatásban részesíteni. Ez nemcsak az új programok kezelésének elsajátítása, illetve a régi programok használatának elmélyítése, begyakorlása miatt fontos, hanem azért is, mert az így elsajátított biztonsági ismeretek alapján megvédhetik a számítógépeiket, adataikat a különféle támadásoktól. A szervezett oktatás mellett fontosnak tartom az önképzést is. A felhasználók kellő ismeret hiányában nem akarnak, nem képesek, vagy nem mernek önállóan a munkájuk, otthoni számítógépük használata során felmerült informatikai problémákra – az interneten – megoldást keresni, és a kapott megoldásokat kipróbálni.

Az oktatásra meg kell találni a megfelelő csatornát. A munkahelyi programok használatának oktatását munkahelyi keretek között kell megoldani, viszont szélesebb kört megcélzó oktatásnak más csatornákat kell keresni.

A hétköznapi élet különböző területeiről jövő szakembereknek az informatikusokkal történő együttműködés is nehézségekbe ütközhet az eltérő szakmai nyelvezet, illetve gondolkodásmód miatt. Példaként említeném, azoknál a munkahelyeken, ahol az informatika kiszolgáló szerepet tölt be, az informatikusnak a szakkifejezések helyett hétköznapi kifejezéseket kell alkalmaznia, hogy szót értsen kollegáival.

5.3. A matematika szerepe a védelemben: hatványfüggvények jelentősége az informatikai támadások kivédésében

A számítógépek hálózatba kapcsolása napjaink technológiája. Itt nemcsak az internetre gondolok, hanem vállalati hálózatokra (intranetre) is. Barabási-Albert László erdélyi származású fizikus munkássága nyomán ismerjük, hogy a számítógépes hálózatok aktív eszközeinek (router, switch) eloszlása hatványfüggvényhez hasonló. Ez az eloszlás a véletlen meghibásodásokkal szemben biztonságot ad, de nem ad biztonságot a szándékos károkozás ellen.

Barabási Albert László 1999-ben végzett kísérletét ismertetném a hálózatok sebezhetőségével kapcsolatban. A kísérletben 40000 elemből álló hálózatot hoztak létre. A hálózati elemek kapcsolatait leíró függvény hatványfüggvényhez hasonló. P(k) jelentette annak valószínűségét, hogy egy véletlenül kiválasztott elemnek k kapcsolata van. A kísérletben $P(k) \sim k^{-3}$. A kísérlet során megvizsgálták a véletlenszerű meghibásodásokat. A meghibásodások nem okoztak jelentős hibát a hálózat működésében. A rendszer elleni célzott támadásokat is tanulmányozták. Ennek során kivették a hálózatból azt a 10 db elemet, melyek a legtöbb kapcsolattal rendelkeztek. Ekkor a hálózat 500 részre (komponensre) esett szét. (Barabási-Albert László: A hálózatok tudománya 31. oldal) A kísérlet eredményéből látható, hogy a hálózat mennyire sebezhető a támadásokkal szemben.

Barabási Albert László mérései alapján az internet működését biztosító aktív eszközök eloszlása hasonló a 3,42 kitevőjű hatványfüggvényhez. Ez a kritikus infrastruktúrába tartozó vállalatoknak, szolgáltatóknak, hatóságoknak rossz hír, mert ha a nyílt internetet használják például a telephelyei közötti kapcsolattartásra, akkor egy célzott támadással megbénítható az informatikai hálózatuk. Magánhálózat esetében viszont a hálózat kialakítása az adott cég

kezében van. Célszerű a hálózat nagy forgalmú, sok kapcsolódással rendelkező, fontos elemeit földrajzilag messze telepíteni egymástól, hogy egy természeti katasztrófa esetén ne essen szét a hálózat. A kibertámadás ellen a megfelelő informatikai védelmet, például víruskereső programok használatát, valamint a redundancia növelését látom megoldásnak.

A jelentős számú munkavállalót foglalkoztató cégeknél előfordulhat, hogy nem mindenkit tudnak megfelelő informatikai oktatásban részesíteni. Ilyen esetben kockázatelemzést érdemes alkalmazni. Első körben javaslom azok oktatását, akiknél jelentős a külső partnerekkel történő levelezés. Ilyen lehet például a sajtós és a személyzetis munkatárs.

Az e-mailekkel terjedő vírusok visszaszorítása érdekében is igénybe vehetjük a hálózatkutatás legújabb eredményeit. Az e-mailek forgalma is hatványfüggvényhez hasonló eloszlást követ. A bejövő e-mailek címzettek szerinti eloszlása hasonló a 3,43 kitevőjű hatványfüggvényhez. (Barabási-Albert László: A hálózatok tudománya 144. oldal) Másrészről a közösségi média elemzéséből ismert, hogy az emberek kapcsolatai számának eloszlása is hatványfüggvényhez hasonló. Az e-mailekkel terjedő vírusok visszaszorítását a célzott oktatás is segítheti. Az oktatás célcsoportja a legtöbb külső kapcsolattal rendelkező munkatársak, felhasználók csoportja. Az oktatás középpontjába javaslom helyezni az e-mailek biztonságos kezelésével kapcsolatos ismereteket.

6. Informatikai támadások

Az informatikai támadások többfélék lehetnek. A támadók kárt okozhatnak különféle programokkal. Kihasználhatják az operációs rendszer illetve a felhasználói programok hibás kódjait a számítógépbe történő behatolásra. Ellophatják adatainkat. Ezek az adatok lehetnek saját számítógépeinken vagy különböző hivatalok, szolgáltatók, cégek szerverein. Én a károkozó programok közül a vírusokat emelném ki.

Az első számítógépes vírusokat az 1980-as években alkották meg. Azóta a kárt okozó programok széles köre fejlődött ki. Cégek alakultak a számítástechnikai eszközeink biztonságának növelésére. Ezektől a cégektől ingyen vagy anyagi ellenszolgáltatás

fejében tölthetjük le a víruskereső programokat. Más cégek a programok biztonsági bevizsgálására szakosodtak.

Az elmúlt években megjelentek a zsarolóvírusok. Ezek a vírusok a sértett merevlemezén található állományokat titkosítják, és pénzt kérnek a dekódolásért. Idén júliusban az sg.hu honlapon megjelent cikk szerint a San-Diego-i és a New York-i egyetem, valamint a Chainalysis és a Google szakemberei szerint az elmúlt két esztendőben összesen 25 millió dollárt fizettek ki a bűnözőknek a zsarolóvírusok áldozatai. (https://sg.hu/cikkek/it-tech/126459/zsarolovirusok-25-millio-dollar- bevetel-ket-ev-alatt).

A Cisco hálózati eszközök fejlesztésével, gyártásával foglalkozó cég weboldalán megjelent cikk szerint 2016-ban a zsarolóvírusokból származó bevétel elérhette az 1 milliárd dollárt (https://www.cisco.com/c/dam/global/hu_hu/solutions/ security/ransomware/pdf/ransomware-infographic_hun.pdf). A becslések nagy szórást mutattak, de látható, hogy a zsarolóvírusok jelentős bevételt hozhattak a bűnözőknek.

A Magyarországi tapasztalatok is azt mutatják, hogy a zsarolóvírusok jelentősen elterjedtek. A Nemzeti Kibervédelmi Intézet által felügyelt rendszerekben 2016. I. negyedévében több száz zsarolóvírus-fertőzést regisztráltak (https://www.vasarnapihirek.hu/fokusz/a_drognal_is_nagyobb_uzlet).

A zsarolóvírusok általában e-mail csatolmányaként vagy különféle programokkal jutnak el a számítógépekbe. 2016 tavaszán a népszerű uTorrent kliens program tartalmazott zsarolóvírust. A vírus képes különféle folyamatok leállítására a Windows operációs rendszerben (https://pcworld.hu/szoftver/virusos-a-%C2%B5torrent- 176272.html).

A zsarolóvírusok kódolás alapján három félék lehetnek: aszimmetrikus kódolást használók, szimmetrikus kódolást használók, vagy mindkét kódolást használók. Azok a vírusok, amik mind a két kódolást használják, a szimmetrikus kódolást használják az állományok titkosítására, és csak a szimmetrikus kódolás kulcsát rejtjelezik aszimmetrikus kódolással, ezáltal optimalizálják a kódolásra fordított erőforrásokat (processzor idő, memória).

Az idei évben a zsarolóvírusok új nemzedéke jelent meg. A WannaCry és a NotPetya névű vírusok ehhez az új nemzedékhez tartoznak és óriási pusztításokat hajtottak végre a

kritikus infrastruktúrákban is. A következőkben támadás részletes leírásával rámutatok arra, hogy a károkozás nagy mértékéhez a rendszerek üzemeltetői és felhasználói egyaránt hozzájárultak.

6.1. WannaCry vírus

A WannaCry vírus 2017. május 12-én bukkant fel. A vírus óriási károkat okozott világszerte. A szakirodalom által ismertté vált támadások közül említek néhányat. Nagy Britanniában a National Health Service egészségügyi szolgáltató számítógépes rendszerét érte támadás. A vírustámadás a számítógépeken kívül orvosi műszereket (MRI scannert, robotsebészeti rendszereket, stb.) is érintett. A károkozás nagyságát mutatja, hogy néhány kórházban teljes szárnyakat kellett bezárni, orvosi beavatkozásokat elnapolni, mentőket átirányítani. Spanyolországban a Telfónica telekommunikációs szolgáltatót, valamint több nagyobb méretű vállalatot bénított meg a vírus. Németországban a Deutsche Bahnt (Német Vasúttársaság) érte támadás. Franciaországban a Renault egyik gyárában állt le a termelés szintén a WannaCry vírus miatt. A támadásra jellemző, hogy a vírus egy hétvége alatt több mint 10000 cég, szervezet több mint 200000 számítógépét fertőzte meg, összesen 150 országban (https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware- attack-spread-150-countries). Magyarországon a Telenort érintette a kibertámadás.

A megtámadott intézmények között több volt a kritikus infrastruktúrához tartozó szolgáltató, egészségügyi intézmény, vállalat. A vírus két fertőzési módot ötvözött, amire eddig nem volt példa, ezért a szakirodalomban az ilyen jellegű vírusra megjelent a ramsomworm név.

A WannaCry titkosította a gép merevlemezén lévő állományokat, melyek feloldásáért először 300 USA dollárnak megfelelő bitcoint kért. Ha ezt nem fizették ki, akkor a fizetendő összeg 600 USA dollárnak megfelelő bitcoinra emelkedett. Ha pedig egy hét után sem fizettek a zsarolóknak, akkor – a technika mai állása szerint – örökre elveszett a remény az állományok dekódolásra.

A vírus által használt sérülékenységet az elérhető szakirodalom alapján feltehetően az NSA (az Amerikai Egyesült Államok elektronikai hírszerzéssel foglalkozó szervezete) fedezte fel. A szakirodalomban EthernalBlue néven vált ismertté. Az EthernalBlue a puffertúlcsorduláson (buffer overflow) alapuló biztonsági rések közé tartozik. A sérülékenység abból eredt, hogy a Windows operációs rendszerben rosszul implementálták az SMB (Server Message Block) protokollt. Az SMB protokollt a számítógépes hálózatokban az erőforrások, file-ok, nyomtatók, soros portok, stb. megosztására használják. A Windows operációs rendszerben úgy implementálták az SMB protokollt, hogy az érkező adatcsomagok hosszát nem vizsgálta az operációs rendszer. Abban az esetben, ha az adatcsomag meghaladta a puffer hosszát, akkor az adatcsomag átírhatta az operációs rendszer kódjának egy részét. A WannaCry vírus ennek a sérülékenységnek a segítségével volt képes terjedni a lokális hálózaton kapcsolódó számítógépek között.

A sérülékenységre 2017. április 14-én hívta fel a figyelmet a The Shadows Brokers hackercsoport. A MicroSoft 1 hónappal korábban 2017. március 17-én adta ki az MS17-010 jelű biztonsági frissítést (security update) a Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows RT 8.1,

Windows Server 2012, Windows Server 2012 R2, Windows 10, Windows Server 2016 operációs rendszerekre. A frissítés az SMB protokoll implementációját javította. A WannaCry fertőzés bekövetkezése után – a fertőzés súlyosságára való tekintettel – a MicroSoft a már nem támogatott operációs rendszerekre (Windows XP, Windows 8, Windows Server 2003) is elkészítette a javítást, amit a támadás után 1 nappal ki is adott. Ebből világosan kitűnik, hogy a WannaCry nem Zero Day sérülékenységet használt ki, a felhasználók többségének lett volna idejük felkészülni a támadás elhárítására.

Az előző bekezdésben szereplő operációs rendszerek listájából látható, hogy a sérülékenység a szervereket is érintette, ezért a szervereken tárolt adatok is veszélybe kerültek. A cégek, illetve a szolgáltatók a szervereken tárolt adatokat általában rendszeresen mentik, ezért a sikeres támadás csak az utolsó mentés és a támadás időpontja között keletkezett adatokat érintette. Viszont a céges környezet munkaállomásain lévő adatokról sokkal ritkábban készül mentés, így az ott tárolt adatok sokkal kiszolgáltatottabbak, ugyanez elmondható az otthoni környezetről is.

A továbbiakban a WannaCry vírus működését és a kódjában talált hibákat mutatom be.

A vírus általában egy e-mailben érkező állománnyal kerül a számítógépre (https://pcworld.hu/pcwpro/wannacry-ransomware-228438.html). A vírus a sikeres fertőzés után az SMB protokoll sérülékenységét kihasználva szabadon szétterjed a számítógépes hálózat többi gépére is. A vírus működése során generál egy RSA kulcspárt. A vírus 176 féle állományt keres a merevlemezen, és azokat az állományokat titkosítja AES-128 kulccsal. Minden állományhoz új AES kulcsot generál. Az AES kulcsot is titkosítja az RSA kulcspár nyilvános kulcsával. Az így kapott titkosított kulcsot hozzámásolja a titkosított állomány elejéhez.

2. WannaCry vírussal fertőzött számítógép képernyője (Forrás: wikipedia.com)

Szerencsére a WannaCry vírus is tartalmazott bug-ot. A vírus az RSA titkosítási kulcs kiszámításának első lépéseként prímszámokat generált. Ezekből a prímszámokból számolta ki a kulcspárt. A kulcspár kiszámolása után a prímeket nem törölte ki a számítógép memóriájából, így lehetséges volt később azokat egy másik programmal

megkeresni és elmenteni. Az elmentett prímszámokból és a nyilvános kulcsból a titkos kulcsot az

$$\text{??} + l(\text{?} - 1)(\text{?} - 1) = 1$$

lineáris diofantoszi egyenlet megoldása adja, ahol ? a nyilvános kulcs, ? a titkos kulcs, ? és ? prímszámok. A kódolás műveletigényének csökkentése érdekében gyakran Fermat prímeket használnak nyilvános kulcsnak, ezért a nyilvános kulcs ismerete nélkül is van esélyünk a titkos kulcsot kiszámolni.

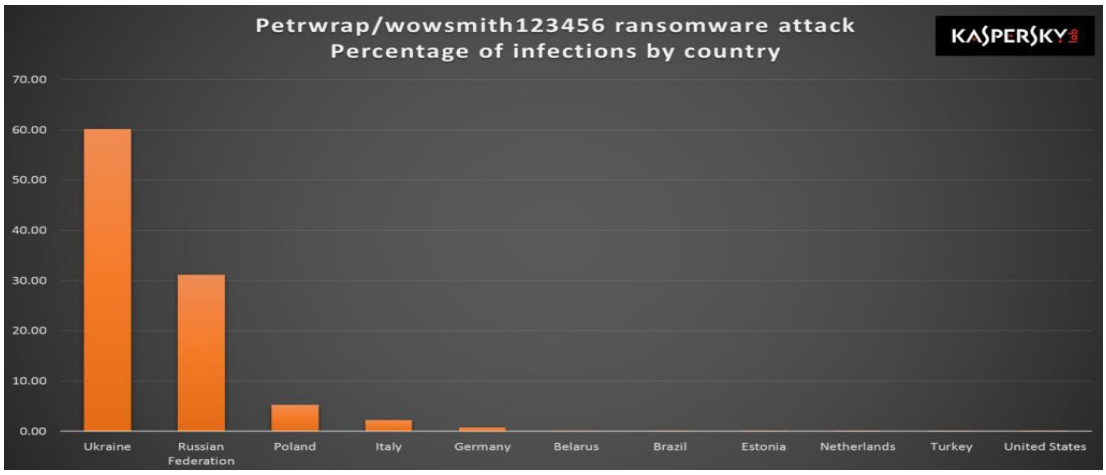
A vírus hibáját kódjának elemzésekor fedezték fel. Adrien Guinet francia biztonsági kutató készítette a Wannakey nevű programot (letölthető: https://github.com/aguinet/wannakey weboldalról), mely a prímszámokat megkeresi a számítógép memóriájában. A prímszámokból és a nyilvános kulcsból a program kiszámolja az RSA kódpár másik tagját és kikódolja a gépen lévő titkosított állományokat (https://sg.hu/cikkek/it-tech/125410/wanna-cry-mar-valtsagdij-fizetes- nelkul-is-kikodolhatok-a-fajlok). A programot csak akkor lehet eredményesen futtatni, ha a gépet nem kapcsolták ki, illetve nem resetelték. Sajnos megeshet, hogy a jövőben minket is ér zsarolóvírus-fertőzés. Ebben az esetben célszerű a számítógépet tovább működtetni, hátha annak a vírusnak a kódjában is előfordul az előbb említett hiba, és dekódolni tudjuk a titkosított állományainkat. Ilyen fertőzés esetén feltörő programot kell rögtön keresni az interneten.

A WannaCry vírus kódjában találtak egy másik hibát is. A kód elemzésével a szakértők észrevették, hogy a vírus minden fertőzéskor megpróbál csatlakozni a www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com címre. Abban az esetben, ha a csatlakozás sikeres, akkor a vírus leállítja magát (http://24.hu/tech/2017/05/13/egy-hetunk-maradt-visszaszerezni-az-adatainkat/). A biztonsági szakértők regisztrálták a domain nevet, és így megállították a vírus terjedését. Később több domain nevet is azonosítottak, aminek regisztrálásával szintén le tudták állítani a vírus terjedését (http://www.cert-hungary.hu/node/370). A siker ideiglenesnek bizonyult a regisztrációk után pár nappal a vírust új, módosított kóddal regisztrálták a biztonsági cégek.

6.2. NotPetya vírus

A másik vírus, ami szintén az EthernalBlue sérülékenységet használja ki, NotPetya néven vált ismertté. A vírus támadását 2017. június 27-én észlelték. A járvány Ukrajnában tört ki. Az első fertőzéseket egy elterjedt számlázó-, illetve könyvelő program, az M.E.Doc egy manipulált, trójai programmá alakított frissítése okozta. A frissítés telepítésekor a vírus megfertőzte a gépet. Ez a terjedési mód megmagyarázza, hogy a vírusnak miért sikerült számos, köztük védett környezetben lévő számítógépet megfertőzni. A fertőzött gépek között volt az ukrán miniszterelnök-helyettes, számos bank, köztük az Ukrán Nemzeti Bank és az OTP ukrán leányvállalatának számítógépei is. A felsoroltakon túl a fertőzés fennakadásokat okozott a közlekedési hálózatban, a kijevi metróban, a kijevi repülőtéren, továbbá a csernobili atomerőmű állapotát monitorozó rendszerben (manuális mérésre álltak át), az orosz Rosznyeft kőolajipari nagyvállalat kitermelési és fimonítási rendszerében (tartalék rendszerre kapcsoltak), a TNT szállítmányozási cég rendszerében. A sort még hosszasan lehetne folytani.

A támadások 60%-át Ukrajnában észlelték, de jelentős arányban észlelték Oroszországban (több mint 30%), Lengyelországban (kb. 5%), Olaszországban, Németországban. Igen kis arányban még az Amerikai Egyedült Államok és Magyarország is érintett volt (https://www.hwsw.hu/hirek/57452/microsoft-windows-ransomware-kriptovirus-petya.html). A támadások országok közötti megoszlását mutatja a következő grafikon.



3. A vírus támadásának országok közötti megoszlását mutató grafikon (Forrás: securelist.com)

A vírus a terjedéshez az EthernalBlue sérülékenységen kívül más módot is használ. Megpróbálja visszafejteni a Windows operációs rendszer jelszavait. A jelszavak visszafejtéséhez a Mimikatz jelszófeltörő programot vagy annak kódbázisát használja. A kiberbűnözők a vírust arra az esetre is felkészítették, ha szerverhez vagy tartományvezérlőhöz nyer hozzáférést. Ebben az esetben a vírus igyekszik megkeresni a tartományban lévő összes számítógépet és megpróbálja ezeket a gépeket megfertőzni. Ehhez a távoli indítási mechanizmust (RPC) használja fel. Az RPC a Windows része, ez szolgál arra, hogy az adott gép erőforrásait más gépekről is használni lehessen.

A vírus által végrehajtott titkosítás módja attól függ, hogy a vírus milyen jogosultságot tud szerezni az adott gépen, és milyen környezetben találja magát. A támadás során összehasonlítja egy előre meghatározott listával a megtámadott számítógépen futó folyamatokat, valamint ellenőrzi saját jogosultságait és ennek alapján dönt a további működéséről. Az első támadási mód, hogy átírja a fő meghajtó master boot recordját, és a gépet újraindítja. Ekkor rögtön a vírus indul el és az NTFS filerendszer Master File Tábláját kódolja le. Ezt a folyamatot azzal álcázza, hogy a képernyőn a chkdsk program futása látható. Abban az esetben, ha a vírus nem fut megfelelő jogosultságokkal, és nincs hozzáférése a Master File Táblához, akkor a merevlemezen lévő állományokat titkosítja. A titkosítás során meghagyja az állományok eredeti nevét és kiterjesztését. A vírus törli a Windows naplóállományait, ezzel álcázza a tevékenységét.

A vírus írói 300 dollárnak megfelelő bitcoint kértek az állományok kikódolásáért. Ezt a sértettek már nem tudják befizetni, mert az ESET informatikai biztonsági cég értesítése szerint a támadók által megadott e-mail címet a szolgáltató törölte. Egyes szakértők a könnyen kikapcsolható e-mail fiókból és más jelekből feltételezik, hogy a vírus készítőinek nem a pénzszerzés, hanem inkább a káosz keltése és az ukrán gazdaságban történő károkozás volt a célja.

A NotPetya vírus elleni védekezés is több lépést követel meg. A legfontosabb a Windows operációs rendszer rendszeres frissítése. A vírus működését blokkolni lehet, ha a Windows mappában létrehozzuk a perfc, perfc.dat és perfc.dll állományokat és ezeknek az írás és végrehajtási jogát blokkoljuk. Amennyiben nem használjuk a WMIC szolgáltatást, akkor tiltsuk le a „net stop winmgmt” paranccsal. A vírus e- mailek

segítségével is terjed. Az e-mailek csatolmányában lévő káros kód a vírust az internetről tölti le, ezért az alábbi címek elérését érdemes letiltani a tűzfalon: french- cooking.com, benkow.cc, 185.165.29.78, upd.me-doc.com.ua, 95.141.115.108, 111.90.139.247, 84.200.16.242, 185.165.29.78, yadi.sk (http://www.cert-hungary.hu/node/381, http://www.cert-hungary.hu/node/382).

7. Összefoglalás

A pályázati anyagból látható, hogy mindannyian válhatunk informatikai támadás áldozataivá. Az is látható, hogy odafigyeléssel, a rendszerek beállításával, frissítésével a támadások nagyrésze kivédhető, károkozásuk csökkenthető. A rendszerek tervezésekor, üzemeltetésekor azt kell eldöntenünk, hogy mennyi időt, pénzt és energiát áldozunk a védelemre. Ez igaz otthoni, és vállalati környezetben is. Fő szabály, hogy minden informatikai fejlesztésre szánt összegnek 5-8, esetenként 10 százalékát kell a biztonságra fordítani. Minden fejlesztésnél fel kell tenni a kérdést: mekkora kárt okozhat, ha az adott informatikai rendszer a felhasználók számára elérhetetlenné válik, és így nem tudnak hozzáférni számos fontos adathoz? Mennyit érhetnek a számítógépes rendszerben tárolt információk? Otthoni rendszerre vetítve, hétköznapi nyelvre lefordítva, mennyit érnek a számítógépemen tárolt családi fotók? Ha ezt mérlegeljük, nagyjából kiszámítható, mennyit kell költeni az adatok védelmére. A védelem megteremtése a víruskereső program beszerzésétől, az operációs rendszer frissítésén keresztül, az új operációs rendszer és az ehhez szükséges hardverbővítés megvásárlásig terjedhet.

A két informatikai támadás (WannaCry és a NotPetya) leírásából látszik, hogy a támadás időpontjában már ismert sérülékenységet használtak ki a vírus írói. Az is látszik, hogy a támadás a kritikus infrastruktúrát sem kímélte. Többek között bankok, egészségügyi intézmények, a szállító infrastruktúra szereplői (pl.: Német Vasúttársaság, kijevi metró és repülőtér, TNT) is áldozatául estek a támadásnak. A kritikus infrastruktúra esetében különösen fontos a folyamatos működés fenntartása, ezt a megfelelő redundancia, és támadás esetén a gyors reagálás biztosíthatja. A kritikus infrastruktúrákat működtető hivatalok, cégek alkalmazottjai közül is sokan dolgoznak számítógéppel. Abban az esetben, ha nem mindenki tartja be a biztonsági intézkedéseket, akkor sokkal könnyebb

dolguk van a kibertámadóknak. A pályázati anyagomban megpróbáltam összegyűjteni azokat a biztonsági javaslatokat, melyek a sikeres támadás esélyét csökkenthetik.

Pályamunkámban nem tértem ki az adatlopásokra és az adatlopásokkal összefüggő visszaélésekre, csalásokra. Gyakran fordul elő, hogy a felhasználókat hamis e- mailekkel ráveszik személyes adataik, jelszavaik megadására. Az ilyen e-maileket mindig fenntartással kell fogadni.

Az Európai Unióban a személyes adatok biztonsága kiemelt helyen szerepel. A különböző hatóságok, szolgáltatók, magáncégek szerverein tárolt személyes adatok biztonságát szigorítja az EU Általános Adatvédelmi Rendelete (GDPR), amely az Európai Parlament és a Tanács 2016/679 rendelete. A tagállomoknak 2018. május 25- ig kell eleget tenni a rendeletben foglaltaknak.

Az első részben néhány gondolatban írtam az elektronikus ügyintézés előnyeiről és hátrányairól. Részben felhasználói szemmel nézve, részben a felhasználóktól kapott információk alapján azt látom, hogy az elektronikus ügyintézés egyszerűsítésre szorul. Az AVDH szolgáltatást emeltem ki az elektronikus ügyintézések közül. Javasoltam az AVDH szolgáltatást jobban összekapcsolni az elektronikus ügyintézés többi elemével.

Remélem, hogy pályázati anyagommal sikerült rávilágítanom az informatikai biztonság kiemelt fontosságára.

Irodalomjegyzék

Önálló mű

Barabási-Albert László: A hálózatok tudománya, Libri Kiadó, Budapest, 2016

Tanulmánykötet

Biztonsági kihívások a 21. században, szerk.: Finszter Géza, Sabjanics István, Dialóg Campus Kiadó, Budapest, 2017

Folyóiratban megjelent tanulmány

Laza Bálint: Minden szombaton dolgozik, Forbes NEXT magazin, 2017. nyár, 32. old.
Mezey Nándor Lajos: Kiberterrorizmus: Valós veszély, Belügyi Szemle, 2011/2 szám, 21. old.

Internetes forrás

Bercze András: Brutális zsarolóvírus söpört végig a neten, pár óra alatt több tízezer gépet fertőzte meg, PC World, 2017. Forrás: https://pcworld.hu/pcwpro/wannacry-ransomware-228438.html

(2017. 10. 01.)

Berta Sándor: Több millió dollárt lehet keresni egy zsarolóvírussal, 2017. Forrás: https://sg.hu/cikkek/it-tech/126459/zsarolovirusok-25-millio-dollar-bevetel-ket- ev-alatt (2017. 10. 01.)

Berta Sándor: Wanna Cry – már váltságdíj nélkül kikódolhatók a fájlok, 2017. Forrás: https://sg.hu/cikkek/it-tech/125410/wanna-cry-mar-valtsagdij-fizetes-nelkul-is- kikodolhatok-a-fajlok (2017. 10. 01.)

Cisco: Zsarolóvírusok: Valóság nem mese Köztünk vannak, kifinomultak – és rafináltak Forrás: https://www.cisco.com/c/dam/global/hu_hu/solutions/security/ ransomware/pdf/ransomware-infographic_hun.pdf (2017. 10. 01.)

Gállfy Csaba: Petya: Minden, amit tudunk a támadásról, 2017. Forrás: https://www.hwsw.hu/hirek/57452/microsoft-windows-ransomware-kriptovirus-petya.html (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Az SMB sérülékenységet kihasználó PetrWarp Ramsomware kampány, 2017. Forrás: http://www.cert-hungary.hu/node/381 (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Az SMB sérülékenységet kihasználó WannaCry Ramsomware kampány, 2017. Forrás: http://www.cert-hungary.hu/node/370 (2017. 10. 01.)

Kormányzati Eseménykezelő Központ: Közlemény a PetrWarp zsarolóvírusról, 2017. Forrás: http://www.cert-hungary.hu/node/382 (2017. 10. 01.)

Kövesdi Péter: A drognál is nagyobb üzlet - A Nemzeti Kibervédelmi Intézetben beszélgettünk a kibertámadásokról, 2016. Forrás: https://www.vasarnapihirek.hu/fokusz/ a_drognal_is_nagyobb_uzlet (2017. 09.01)

Andrew Liptak: The WannaCry ransomware attack has spread to 150 countries,

2017. Forrás: https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries (2017. 10. 01) PC World: Vírusos az uTorrent, PC World 2016. Forrás: https://pcworld.hu/szoftver/virusos-a-%C2%B5torrent-176272.html (2017. 10. 01)

Pintér Mónika: Egy hetünk maradt visszaszerezni az adatainkat, 2017. Forrás: http://24.hu/tech/2017/05/13/egy-hetunk-maradt-visszaszerezni-az-adatainkat/ (2017. 10. 01.)

Origo: Frissítette a Javát? Hiba volt, 2017. Forrás: http://www.uzletresz.hu/penzugy/20170927-nem-kompatibilis-a-java-a-nav-nyomtatvanykitoltojevel.html (2017. 10. 01)

Wikipedia: WannaCry Forrás: https://hu.wikipedia.org/wiki/WannaCry (2017.10.01.)
Wikipedia: WannaCry ransomware attack Forrás: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (2017.10.01.)