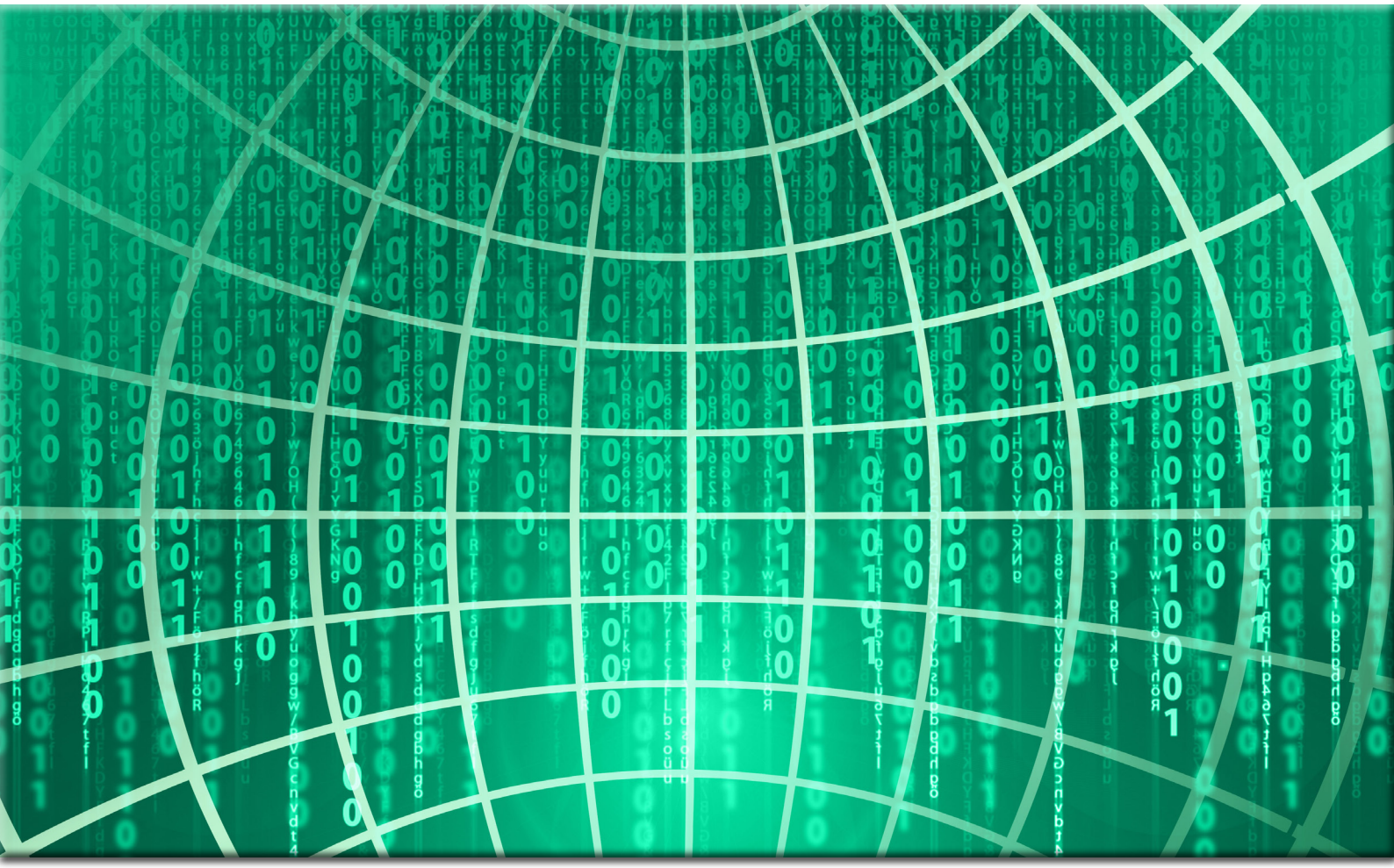
BÓDI ANTAL – JERABEK GYÖRGY
KRASZNAY CSABA – TÓTH KORNÉL



AZ IBTV. GYAKORLATA

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2020

Nemzeti Közszolgálati Egyetem, Budapest

AZ IBTV. GYAKORLATA

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2020

Szerzők:
Bódi Antal
Dr. Krasznay Csaba
Jerabek György
Tóth Kornél

Szakmai lektor:
Dr. Szádeczky Tamás

Szerkesztő:
Deák Veronika

A kézirat lezárásának dátuma:
2020. szeptember 16.

A hatályosított kézirat lezárásának ideje:
2022. február 25.

Hatályosítást 2022-ben végezte:
Mikula Fanni

Hatályosításért felelős szakmai szakértő:
Legárd Ildikó

TARTALOM

1. KRASZNAY CSABA – NEMZETKÖZI KAPCSOLATOK A KIBERTÉRBEN

1.1. Bevezetés

A kibertér a 2010-es évek végére minden kétséget kizáróan a valós, fizikai tér mellett második életterünkké vált. Amellett, hogy az emberiség közel fele napi szinten használja az internetet magán- és hivatalos teendőinek elvégzésére, a vállalatok és az állami szervezetek is függenek infokommunikációs rendszereik megbízhatóságától. Ez a függés pedig már régen továbbjutott annál a szintnél, amelyet egy szervezet a saját hatáskörén belül kezelni tud, egymagában nem tudja megoldani a működéséhez szükséges elektronikus információs rendszereinek védelmét. A digitális ellátási láncolatok hihetetlen komplexitása alakult ki, melynek sérülékenységét teljes egészében egyelőre el sem tudjuk képzelni. Márpedig ez az évtized bebizonyította, hogy akár egy véletlen számítógépes hiba, akár egy jól megtervezett kibertámadás az ellátási láncban komoly gazdasági károkat, sőt emberéleteket veszélyeztethet. Ilyen körülmények között pedig az egyes államhatalmaknak reagálniuk kell, meg kell védeniük nemzetük biztonságát.

Az internet tömeges elterjedésével együtt tehát az egyes államok folyamatosan törekedtek arra, hogy belső biztonságukat a kibertérben is szavatolni tudják. Kialakultak azok a rendészeti, titkosszolgálati eljárásrendek, illetve az ezeket szabályozó jogi normák, amelyek segítségével a digitális úton elkövetett bűncselekményeket kezelni lehetett. Felállították azokat a szervezeteket, amelyek műszaki úton is képesek voltak az információbiztonságot veszélyeztető eseményeket elhárítani. A kiberbűncselekmények számának és főleg az okozott kárnak az emelkedésével azonban minden szakember számára világossá vált, hogy a nemzetközi szervezett bűnözés felfedezte magának ezt a területet is, így nemzetközi rendészeti együttműködések szükségesek ahhoz, hogy a virtuális létet egyre nagyobb számban felfedező állampolgárok biztonsága szavatolható legyen. Megjelent tehát az igény arra, hogy az egyes nemzetállamok közösen lépjenek fel a kibertér fenyegetéseivel szemben. Az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye volt az első olyan jelentős nemzetközi megállapodás, amely ezt a közös fellépést segítette.

A közös fellépés azonban nem minden esetben érdeke a kormányzatoknak. A számítógépes bűnözés visszaszorítása kivétel nélkül minden ország célja, de nem feltétlenül áll érdekükben annak teljes megszüntetése. Bizonyos esetekben ugyanis a bűnözői csoportok által használt eszközök és technikák jól hasznosíthatók az állami érdekek szolgálatában is. Már a 2007-es, Észtországot ért kibertámadás is fontos jelzés volt arra, hogy ezek a csoportok és az ő erőforrásaik jól használhatók abban az esetben, ha egy kormányzat nem kíván közvetlenül részt venni egy nyomásgyakorló akcióban, de mégis érvényesíteni kívánja saját érdekeit. Ezek a proxy csoportok jól használhatók akkor is, ha egy ország pénzügyi egyensúlyának fenntartása érdekében a klasszikus kiberbűnözési módszerekhez nyúl, ahogy azt a 2017-es Wannacry kártékony kód kampány során is lehetett tapasztalni. A nemzetközi rendészeti együttműködés rendszerét pedig felkészületlenül érte az a tény, hogy a bűncselekmények károsultjai és elkövetői földrajzilag nem azonos országban, sőt sokszor nem is egy földrészen vannak, így rá vannak szorulva az elkövető tartózkodási helyén működő bűnüldözők

támogatására, de ezt a támogatást nem mindig kapják meg. Míg ugyanis a hagyományos alvilággal jellemzően szembe tudnak szállni a fizikai térben, itt sokszor olyan bűnözői csoportokkal találkoznak, akik bizonyos szempontból védelem alatt állnak. A digitális térben elkövetett visszaélések így sokszor büntetlenül maradnak, a kiberbűnözők és az államilag támogatott titkosszolgálati és katonai csoportok között pedig elmosódott a határ.

Tovább bonyolítja a helyzetet az, hogy mind a hírszerzés, mind a katonai műveletek terén, amelyek állami monopóliumnak számítanak, hangsúlyosan jelenik meg napjainkban a kibertér adta lehetőségek maximális kihasználása. Ez teljesen természetes akkor, amikor az információk szinte kivétel nélkül digitális formában keletkeznek és léteznek teljes életciklusuk során. Ez az emberiség történelme során korábban nem tapasztalt információbőség, illetve az infokommunikációs rendszerektől való függés egyes kormányzatokat arra csábított, hogy stratégiai érdekeik érvényesítése érdekében túllépjen azokon a határokon, melyet az erkölcs, a jóérzés és az etika egyébként megkövetelt volna. Hangsúlyosan nem a nemzetközi jog és az évszázados normák, hiszen a nagyhatalmak versengésében a kibertér egyfajta Vadnyugatnak számított, ahol senki nem törekedett a közös játékszabályok kialakítására, a meglevő nemzetközi normák pedig nem adtak egyértelmű útmutatást arra vonatkozóan, hogy mit szabad és mit nem. Emellett nem is állt rendelkezésre az a kényszerítő erő, amivel a szabályrendszert be lehetett volna tartatni a normaszegő országokkal szemben.

Az elmúlóban levő évtizedben a nemzetközi kapcsolatok rendszere a kibertérben egy olyan területté vált, amelyet a széles közvélemény is érzékel, globális hatása van a nemzetközi kapcsolatok rendszerére, a biztonságpolitika egészére, tudományos háttere azonban csak kevesek számára ismert, súlyához mérten kisszámú szakértő foglalkozik vele a nyilvánosan elérhető tudományos szakirodalomban. Magyarországon, a hazai perspektívából pedig gyakorlatilag semmilyen publikáció nem született a témában. Jelen tanulmány ezt a hiányt igyekszik bepótolni, bemutatva mindazokat az eredményeket, amelyek a nemzetközi szaksajtóban elérhetők, összefoglalva a tudományos diskurzus jelenlegi állapotát, egyben irányt mutatva a nemzetközi joggal és biztonságpolitikával foglalkozó közösségnek a kibertér kihívásainak megismeréséhez.

A tanulmány alapja a NATO Kooperatív Kibervédelmi Kiválósági Központjának (NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE) *International Cyber Norms – Legal, Policy & Industry Perspectives* című kiadványa, amely Anna-Maria Osula és Henry Rõigas szerkesztésében jelent meg 2016-ban. A könyv áttekinti a nemzetközi kiberkapcsolatok legégetőbb problémáit a téma legismertebb kutatóinak publikációin keresztül. A tallinni székhelyű NATO CCD COE egy olyan NATO-akkreditált tudásközpont, think-tank és oktatóközpont, ahol a kiberbiztonság interdiszciplináris megközelítését alkalmazzák, elsősorban a NATO, a tagállamok és az egyes partnerek képességfejlesztésének, együttműködésének és információmegosztásának érdekében. Létrehozását a 2007-es, Észtország elleni kibertámadás indokolta. Jelenleg a tanulmány által tárgyalt téma szempontjából a legfontosabb tudományos műhelynek minősül. Jelen írásmű követi a NATO CCD COE kiadványának a hazai szempontból releváns problémafelvetéseit, kivonatolja a szerzők megállapításait, a szükséges mértékben kiegészíti azt más szerzők munkáival és szükség esetén szemléltető esettanulmányokkal, valamint hozzáadja a magyar nézőpontból fontos további információkat. A tanulmány célja, hogy felkészítse a magyar közszolgálatban jelenleg dolgozó vagy ott elhelyezkedni kívánó szakembereket a nemzetközi kiberkapcsolatok érzékeny kérdéseire, kihívásaira, ezzel segítve Magyarország stratégiai érdekeinek érvényesítését a legfiatalabb műveleti térben.[1]

[1] A NATO 2016 óta a kiberteret is műveleti térnek tekinti a föld, a víz és a levegő után. Az amerikai katonai doktrína ehhez még hozzáteszi a világűrt is, így terjedt el a *fifth domain of warfare*, azaz az ötödik hadviselési színtér elnevezés a szakirodalomban, bár az Egyesült Államok esetén a kibertér helyett az információs tér megnevezést használják.

1.2. Normák a kibertérben

„*A nemzetközi jog a nemzetközi közösség tagjai – elsődlegesen a döntő mértékben az államok – közötti kapcsolatokat, viszonyokat szabályozó jogi normák rendszere. A nemzetközi jog tehát azoknak a magatartási szabályoknak az összessége, amelyek a nemzetközi jog alanyai közötti kapcsolatokat rendezik*" – foglalja össze Cserny és Téglási a nemzetközi jog fogalmát a magyar szakirodalom alapján. Majd így folytatják: „*A nemzetközi eredetű normák és a belső jogszabályok viszonyával kapcsolatban elmondható, hogy:*

- *a szabályszerűen megkötött nemzetközi szerződések arra kötelezik az államot, hogy a belső jogalkotást a nemzetközi szerződéseknek megfelelően alakítsa.*
- *A belső jogszabállyal kihirdetett nemzetközi szerződések a belső jogszabály formájának megfelelő szinten helyezkednek el a jogszabályok hierarchiájában, azzal, hogy az azonos formában elfogadott szabályok között a nemzetközi eredetű megelőzi a belső eredetű jogszabályt.*
- *Minthogy nemzetközi szerződést nem lehet alkotmányként kihirdetni, a nemzetközi szerződés szabálya nem mondhat ellent az alkotmánynak (Alaptörvénynek), de más belső jogszabállyal kihirdetett nemzetközi szerződés ellentmondhat az azonos vagy alacsonyabb szintű belső jogszabályoknak.*
- *A belső jogszabállyal kihirdetett nemzetközi szerződés a belső jog integráns része lesz.*" (Cserny–Téglási 2014)

De mi történik akkor, ha robbanásszerűen megjelenik egy új technológia, amelyre a nemzetközi kapcsolatok rendszere nem tudott felkészülni, de feszültséget szül a nemzetállamok és nemzetközi közösségek között? Pontosan ezzel a dilemmával szembesült a nemzetközi közösség az információs rendszerek elterjedése miatt. Miközben már az ezredfordulón is voltak jelei annak, hogy egyes országok kormányzati szervezetei előszeretettel támadnak nem egyértelműen katonai célpontnak minősülő információs rendszereket információszerzési vagy pusztítási szándékkal, először 2011-ben, a Müncheni Biztonságpolitikai Konferencián beszéltek nagy nyilvánosság előtt arról vezető politikusok, hogy ezzel a problémával valamit kezdeni kell. Ban Ki-moon ENSZ-főtitkár hangsúlyozta, hogy a nemzetközi közösségnek közösen kell fellépnie a kibertámadások ellen. A felszólalók arról is szót ejtettek, hogy a határ a kiberbűnözés, a kémkedés és a terrorizmus között kezd elmosódni az interneten. (Munich Security Conference 2011) Lattmann így foglalta össze a 2010-es évek első felének jogalkalmazási problémáját:

„Jelenleg nincsenek egyértelműen kötelező, írott hadijogi szabályok, amelyek az informatikai hadviselésre alkalmazhatók lennének. E hiányosságnak több oka van. Egyrészt a létező humanitárius jogi szabályaink kodifikációjának idejében az informatikai hadviselés a mai formájában nem volt realitás. 1949-ben a Genfi egyezmények, vagy 1977-ben a két Kiegészítő jegyzőkönyv elfogadásakor a jogalkotó államok nem kellett, hogy ezzel a kérdéssel foglalkozzanak. Ennek eredményeképpen szerződésalkotó akaratuk nem terjedt ki e sajátos helyzetre, így a humanitárius nemzetközi jog alapelvei (és a hadijog szokásjogi normái) által fedett kérdéseken túlmenően nehezen érvelhető bármilyen kötelező erő.

Másik jelentős probléma a »megfogható« tér mint elem hiánya. Mi az a »kibertér«, és hogyan tudjuk szabályozási területként kezelni? Az egész modern nemzetközi jogrendünk a területük felett szuverenitást gyakorló államokon nyugszik, ennek eredményeképpen mind az erő alkalmazását szabályozó jogrend, mind pedig a humanitárius nemzetközi jog elválaszthatatlan az államterület kérdésétől. Márpedig az informatikai hadviselés területén bajosan tudunk a területiségre alapozni: míg a fizikai csatatereken vannak valamiféle vonalak és államhatárok, ezek nehezen értelmezhetők a kibertérben, ami számos problémára vezethet.

A fentiekből következik, hogy nehezen dönthető el, mi minősül jogszerű katonai célpontnak, valamint hogy ki minősül jogszerű harcosnak, utóbbiakkal szemben pedig milyen intézkedéseket tartunk megengedhetőnek az államok részéről. Ehhez kapcsolódó probléma az esetleges jogsértésekkel szembeni

fellépés nehézsége – a tényleges, »fizikai« hadviselés során például a harcokba közvetlenül bebocsátkozó civil személy cselekményének jogsértő jellege a genfi egyezmények meghatározta kritériumok hiányában a helyszínen könnyen felismerhető, valamint a vele szemben való büntetőjogi fellépés az egyezmények szabta keretek között biztosítható. Ám több száz, vagy akár ezer kilométeres távolságból ez nehezen elképzelhető." (Lattmann 2013)

A NATO a 2014-es Walesi Csúcson egyértelmű választ adott ezekre a kérdésekre. A csúcs zárónyilatkozatának 72. pontjában így fogalmaznak:

„*Politikánk szintén elismeri, hogy a nemzetközi jog, így a nemzetközi humanitárius jog és az ENSZ Alapokmány érvényes a kibertérben is.*" (NATO 2014)

A nyugati, elsősorban angolszász országok nyilatkozataiban azóta folyamatosan visszaköszön az, hogy a kibertér is hasonló a fizikai térhez, a nemzetközi jogi normák pedig itt is érvényesek. Ez természetesen egy fontos politikai állásfoglalás, azonban számos gyakorlati problémát vet fel, melyek megoldására valószínűleg évtizednyi időre lesz szükség.

A NATO CCD COE 2008-ban kezdte meg azt a munkát, melynek során ajánlásokat tett a nemzetközi jog alkalmazására a kibertérben. Ennek eredménye lett az úgynevezett Tallinn Manual, azaz Tallinni Kézikönyv, amelynek első kiadása 2013-ban, frissítése 2017-ben jelent meg. Ez természetesen nem kötelező jellegű, mégis fontos munka abból a szempontból, hogy támpontot, vitaalapot jelent az egyes nemzetállamoknak azzal kapcsolatban, hogyan lehet értelmezni a fennálló nemzetközi jogi kereteket. A jog azonban a közösen elfogadott normákból következik, így először a viselkedési játékszabályokban kell megállapodni. Tekintettel arra, hogy minden ország, kivétel nélkül sebezhető az információs rendszerein keresztül, ez a kiegyezés néhány éven belül meg kell hogy történjen. Osula és Rõigas kétfajta normát különböztet meg. Egyrészt vannak olyan normák, amelyek jogilag kötelező érvényű kötelezettségek, pl. a nemzetközi egyezmények. Másrészt vannak olyan nemzetközi normák, amelyek referenciapontként szolgálnak az elvárt viselkedéssel kapcsolatban, de nem kötelező érvényű jogi aktusok és elsősorban diplomáciai megállapodásokban érhetők tetten. (Osula- Rõigas 2016)

A normák kialakítása történhet kétoldalú, úgynevezett bilaterális, és többoldalú, úgynevezett multilaterális megállapodások keretében. A kibertér, jellegéből adódóan, nem ismer nemzeti határokat, egyes kibertéri eseményeknek mégis van nemzeti hatása. Munk ezt a következőképp fogalmazza meg:

„A harmadik kérdés úgy fogalmazható meg, hogy a kibertér globális jellegű, vagy egy adott szereplő szempontjából értelmezett, körülhatárolt. A legtöbb meghatározásban nincs utalás a szereplő-orientált megközelítésre, így ezek – bár nem zárják ki a másik változatot – a globális jelleget sugallják. Több esetben találkozhatunk azonban a szereplő-orientált megközelítéssel is, amelyek nemzeti kibertérről beszélnek. A két megközelítés nem zárja ki egymást, ugyanis egy szereplő-orientált kibertér nyilvánvalóan a globális kibertér valamely szempontok alapján körülhatárolt része, azonban egy meghatározásból – ha nem tartalmaz jelzős megkülönböztetést – egyértelműen ki kell tűnnie, hogy melyik megközelítésre épül." (Munk 2018)

A kibertér esetében tehát van létjogosultsága mindkét megállapodástípusnak. Egyrészt a globális normákat szabályozni szükséges annak érdekében, hogy minden kibertéri szereplő elfogadjon bizonyos alapszabályokat. A Budapest Egyezmény egy jó példa arra a közös szándékra, ami egy multilaterális egyezményhez vezethet. De ugyanígy van indoka a bilaterális megállapodásoknak például, ha egyes nemzeti létfontosságú rendszerek vagy rendszerelemek a nemzeti határokon túl üzemelnek, mint ahogy Magyarország esetében ez a távközlési szektor esetében megtörténik. Az egyes országok diplomáciai kapcsolatán túl tehát kiemelt fontossága van azoknak a nemzetközi szervezeteknek, melyek a globális vagy régiós, multilaterális normák kialakításában vesznek részt.

1.3. A nemzetközi szervezetek szerepe a kibertér biztonságának garantálásában

1.3.1. Egyesült Nemzetek Szervezete (ENSZ)

A globális biztonsági megállapodások létrehozásának elsődleges terepe az Egyesült Nemzetek Szervezete, az ENSZ. A 193 tagország folyamatos párbeszéde lehetőséget biztosít arra, hogy minden szempont és érvrendszer napvilágra kerüljön, szakosított intézményein keresztül pedig a fejlett országok számára egyébként rejtett kihívásokra is fény derülhet. Éppen ezért kiemelt fontosságú az ENSZ tevékenysége a globális kiberbiztonság megteremtésében.

Az ENSZ már az új évezred elejétől kiemelt célként tekint az infokommunikáció elterjesztésére. A 2000 és 2015 közötti időszakra megfogalmazott Millenniumi Fejlesztési Célok (Millennium Development Goals – MDG) között is szerepel a hozzáférés segítése az új technológiákhoz, mérőszámként pedig a 100 főre jutó internetfelhasználók számát jelölték meg. Ezt követte a 2030 Agenda for Sustainable Development program, amely a fenntartható fejlődés érdekében jelöl meg 17 Fenntartható Fejlődési Célt (Sustainable Development Goal – SDG). Ezek között nem szerepel direkt infokommunikációs cél, viszont minden egyes cél mögött ott van az informatika mint a megvalósítást lehetővé tevő eszköz, illetve mint paradigmaváltó megoldás, amely hozzájárul a célok újszerű, innovatív eléréséhez. Ha tehát az informatika alapköve a globális jólét biztosításának, akkor ennek az alapkőnek a biztonsága is fontos.

Az ENSZ kiberbiztonsággal kapcsolatos tevékenysége két fő csapásirány felé indult el. Maurer ezt politikai-katonai és gazdasági irányoknak nevezte el, praktikusan a kiberhadviselés és a kiberbűnözés kezelése szerepel a nemzetközi szervezet napirendjén. (Maurer 2011) Ide tartozhat még az internetirányítással kapcsolatos tevékenység és a gyermekek online védelme is, bár ezek nem elsősorban kiberbiztonsággal kapcsolatos tevékenységek. A kiberbiztonsággal kapcsolatos érdemi tevékenység az ENSZ-ben 1998-ban kezdődött, amikor az orosz kormány kért állásfoglalást az ENSZ Közgyűlést támogató Első Bizottságtól, amely a Leszerelési és Nemzetközi Biztonsági Bizottság nevet viseli. A nézetkülönbségek már ekkor megjelentek az Egyesült Államok és az Orosz Föderáció között. Az USA mélyebb együttműködést várt volna el a kiberbűnözés területén, ez azonban az orosz álláspont szerint az alkotmányukba ütközne, hiszen idegen rendőri erők vizsgálnák a szuverén orosz kiberteret. Oroszország a kibertérben használatos fegyverek korlátozására vonatkozó kérelemmel állt elő, amerikai vélemények szerint azért, hogy megakadályozzák az USA erőfölényének kialakulását. Szintén problémás terület a két Biztonsági Tanács-tag között az interneten megjelenő szólásszabadság kérdése, ami az orosz fél szerint politikailag destabilizálhatja az országot. Ez megegyezik Kína álláspontjával is, bár az ázsiai fél a két ország közötti vitában viszonylag ritkán nyilvánított véleményt. Az első határozatot egyébként 1999-ben adták ki, 53/70, „Developments in the Field of Information and Telecommunications in the Context of International Security" címmel, orosz kezdeményezésre.

A téma komplexitását mutatja, hogy a kibertérben megjelenő normákkal kapcsolatban a hat bizottság közül három is javaslatot nyújtott be, az Első Bizottság mellett a Második Bizottság (Gazdasági és Pénzügyi Bizottság) és a Harmadik Bizottság (Szociális, Humanitárius és Kulturális Bizottság) is foglalkozott a kérdéssel. 2018-ig összesen öt, úgynevezett kormányzati szakértői csoport (Group of Governmental Experts – GGE) ült össze, hogy megvizsgálja az infokommunikációs technológiákban rejlő lehetséges veszélyeket. Ezek az ENSZ Közgyűlés 58/32 határozata alapján működtek, amelyet 2003-ban fogadtak el.

2009-től új lendületet kapott a korábban sikertelen GGE testület, hiszen az észtországi kibertámadás, illetve a 2008-as grúziai háború megmutatta, milyen hatással lehetnek a nemzetközi kapcsolatokra a kibertérben történő műveletek. A rendszeressé váló, kétéves mandátumokkal rendelkező GGE-k az alábbi eredményeket érték el:

- 2010: A GGE együttműködést szorgalmazott a tagállamok, a privát szektor és a civil társadalom között, valamint ajánlásokat fogalmazott meg az infokommunikációs leállásokból fakadó félreértések elkerülése végett. Ezek magukban foglalták a bizalomerősítő és kockázatcsökkentő lépéseket, a nemzeti jogrendbe ültetett információmegosztást, a szabályalkotást és jó gyakorlatok megosztását, valamint a kevésbé fejlett országok képességfejlesztését.
- 2012/2013: A Közgyűlés 66/24 számú határozatával a harmadik GGE is mandátumot kapott, és 2013-ban egy konszenzusos nyilatkozatot tett közzé. Eszerint a nemzetközi jog, különösen az ENSZ Alapokmány érvényes a kibertérben is, az állami szuverenitást garantáló normák és kötelezettségek minden, a tagállamok által a kibertérben végrehajtott műveletre érvényesek, beleértve ebbe a tagállamok területén levő infokommunikációs infrastruktúrák használatát is. A GGE tagok abban is megállapodtak, hogy nem megengedett a proxyk használata a szándékosan jogellenes cselekmények végrehajtásához, valamint ezen csoportok számára nem lehet átengedni a nemzeti kiberteret. A nyilatkozat felszólít a további párbeszédre, valamint a bizalomépítéssel és képességfejlesztéssel kapcsolatos ajánlásokat is tesz. Bátorítja továbbá a nemzeti CERT-ek együttműködését is.
- 2014/2015: A negyedik GGE a 68/243 számú határozat alapján alakult meg 20 taggal, konszenzusos beszámolóját 2015 júniusban adta közre. Épít a korábbi GGE-riportokra, de kiegészíti azokat az önkéntes, nem kötelező normák, szabályok és elvek alkalmazásának javaslatával. A korábbi nemzetközi jogi elveket kiterjesztve foglalkozik a hadijog kérdéseivel is a kibertérben. Az ENSZ Közgyűlés elfogadta a jelentést, és felhívta a tagállamokat az abban foglaltak betartására, ami minden korábbinál erősebb jelzés volt.
- 2016/2017: Az ötödik GGE a 70/723 számú határozattal alakult meg, de nem sikerült konszenzusos nyilatkozatot tennie. Az Egyesült Államok nyilatkozata szerint a sikertelenség oka az volt, hogy a tagállamok nem tudtak megegyezni abban, hogyan vonatkozik a nemzetközi jog az államok válaszaira és ellenintézkedéseire a kiberbiztonsági incidensek során. Az USA álláspontja szerint azzal, hogy nem ismerik el jogosnak egy állam válaszát a rosszindulatú kibertevékenységekkel kapcsolatban, nem lehet a szükséges elrettentést megvalósítani a technológiák rosszindulatú használatának elkerülése érdekében. A másik oldalon a kubai delegáció fejezte ki azon félelmét, hogy egy ilyen felhatalmazással egyes országok egyoldalú akciókat indíthatnak kibertámadásokra hivatkozva, ezzel militarizálva a kiberteret. Valószínűleg az orosz és a kínai delegációk is ezt a véleményt osztották, bár az ő állásfoglalásuk nem került nyilvánosságra. (Korzak 2017) (Nuclear Threat Initiative 2018)

A sikertelenség után egyelőre nem adtak felhatalmazást további GGE létrehozására. Jelen tanulmány írásának idején az egyes tagállamok egyoldalúan, illetve kisebb tömbökben keresik a választ arra, hogyan valósítható meg a nemzeti elrettentés, illetve válaszadás egy kibertámadás után. Ezek a nem konszenzuális válaszok rombolják a nemzetközi együttműködés légkörét, jelezve a GGE-k és az ENSZ tevékenységének fontosságát, annak ellenére, hogy a három sikeres GGE munkája sem eredményezett jogilag kötelező nemzetközi keretrendszert. Ennek ellenére, bár látszólag kis lépésekkel halad előre a globális megállapodás, néhány fundamentumban már egyetértenek a felek.

1.3.2. Nemzetközi Távközlési Egyesület (ITU)

A Nemzetközi Távközlési Egyesület (angolul International Telecommunication Union, ITU) az ENSZ infokommunikációs technológiákra szakosított szervezete. Kiemelt szerepe van az elektromágneses

spektrumgazdálkodás és a műholdpályák globális kezelésében, emellett hatáskörébe tartozik az infokommunikációs területen az összekapcsolódást segítő interoperabilitási szabványok kiadása és általánosságban a technológiához való hozzáférés elősegítése. Jelenleg 193 tagországa és közel 800 privát szektorba tartozó, illetve akadémiai tagja van. Székhelye Genfben található.

Mint az ENSZ szakosított szervezetének, elsősorban az ITU-nak a feladata a globális kibertérrel kapcsolatos műszaki megfontolások kezelése, így szerepet vállal a kiberbiztonság elterjesztésében is. Ennek fő hajtóereje a Connect 2020 Agenda for Global Telecommunication/ICT Development, amely a tagországok stratégiai céljait fogalmazza meg az infokommunikációs területen. Magyarország Connect 2020-szal kapcsolatos nemzeti vállalása a következő:

„Mindannyian büszkék vagyunk arra, hogy a közelmúltban indult két, az ágazatra vonatkozó kezdeményezés: a Nemzeti Infokommunikációs Stratégia és a Digitális Jólét Program. Mindkét stratégia négy pillérre épül – teljes összhangban az ITU stratégiai gondolkodásával. Ezek az elemek biztosítják majd azt, hogy az IKT-ágazat szolgálni fogja a munkahelyteremtést, a kutatást és fejlesztést, a fenntartható gazdasági növekedést és a társadalmi szolidaritást. Az iparági tendenciák és a horizontális fejlesztési célok azonosítása alapján számos, a nemzeti stratégiákban megjelölt célkitűzés tökéletesen illeszkedik a Connect 2020 négy egymást kiegészítő céljához." (ITU 2014)

A stratégiai célok között szerepel a fenntarthatóság, mely a telekommunikációs és IKT-fejlődésből eredő kihívások kezelését hivatott megoldani. Ezen belül az egyik indikátor a kiberbiztonsági felkészültség 40 százalékkal történő javítása. Ennek érdekében az ITU számos, kiberbiztonsággal kapcsolatos programot indított el:

- A nemzeti eseménykezelő központok (Computer Incident Response Team – CIRT) közötti együttműködés támogatása, melynek jelenleg 103 teljes jogú tagja van, köztük Magyarország.
- A Globális Kiberbiztonsági Index (Global Cybersecurity Index) évenkénti elkészítése, mely objektív szempontok alapján mutatja be a tagországok felkészültségét. Magyarország a 2017-es felmérésben az európai középmezőnybe került, ez azonban elsősorban az adatszolgáltatás hiányosságának köszönhető, nem a valós képet mutatja.
- Az online gyermekvédelem (Protecting Children Online) elősegítése, melyre az ITU létrehozott egy olyan kezdeményezést, ami a tagországokban a gyermekek online védelmét hivatott terjeszteni. Magyarország aktív részese a kezdeményezésnek.
- A nemzeti kiberbiztonsági stratégiák létrehozása, melyet az ITU keretrendszere (National Cybersecurity Strategy Framework) támogat. A magyar kiberbiztonsági stratégia összhangban van ezzel a keretrendszerrel.
- A kiberbiztonsággal kapcsolatos területek szabványosítása, mely a Study Group 17 csoporton belül történik, és már közel 170 olyan ajánlást fogalmaztak meg, ami hozzájárulhat a biztonságosabb kibertér kialakításához.
- Az ITU történelmi mandátumához igazodva a rádiókommunikációs rendszerek biztonságának megerősítése is szerepel a kiberbiztonsággal kapcsolatos feladatok között. (ITU 2018)

Ahogy korábban említettük, az ENSZ 2030 Agenda for Sustainable Development programban megfogalmazott Fenntartható Fejlődési Céljainak az infokommunikációs technológiák nélkülözhetetlen hátteret jelentenek. Az ITU a World Summit on the Information Society (WSIS) Forum keretében ad teret az SDG-k és a technológia kapcsolatának megvitatására. A WSIS 2004 óta évente kerül megrendezésre, a globális információs társadalom fejlesztésének legjelentősebb globális fóruma, ahol állami és nem állami szereplők osztják meg egymással véleményüket. A WSIS úgynevezett Akcióvonalakat (Action Lines) jelöl ki, amelyek mentén a diskurzus halad. Ezek közül az ötödik foglalkozik a kiberbiztonsággal, pontos neve Bizalom és biztonság építése az IKT-technológiák használata során (Building Confidence and Security in the use of ICTs). Az itt folyó munkának a 2007-ben kiadott ITU

Globális Kiberbiztonsági Agenda (Global Cybersecurity Agenda – GCA) ad alapot. Ennek öt stratégiai pillére a jogi, a technológiai és eljárásbeli, szervezeti, képességépítési és nemzetközi együttműködési kérdésekkel foglalkozik.

A kibertér nemzetközi kapcsolatrendszerében azonban a legfontosabb olyan töréspont, ami az ITU fennhatósága alá tartozik, az internetirányítás, azaz internet governance kérdése. A WSIS a következőképpen határozta meg az internetirányítás fogalmát:

„Az internetirányítás azon fejlesztések és alkalmazások összessége, melyet a kormányok, a magánszektor és a civil társadalom saját szerepkörükben hajtanak végre, megosztott elvek, normák, szabályok, döntéshozatali eljárások és programok mentén az internet fejlődésének és használatának érdekében." (ITU 2005)

Leegyszerűsítve viszont annak problémáját hozza felszínre, hogy valójában ki irányítja az internet működéséhez nélkülözhetetlen erőforrások szétosztását. Mivel az internet amerikai találmány, a történelmi hagyományok szerint az olyan nélkülözhetetlen információk kiosztása, mint a felső szintű doménnevek, az IP-címek és tartományok, az alkalmazásokhoz csatolt portszámok jelenleg a Los Angelesben működő Internet Corporation for Assigned Names and Numbers (ICANN) nonprofit szervezet kezében vannak. Egészen 1998-ig ezt Jon Postel egy személyben tette meg. Bár az ICANN igyekezett függetlenül és átláthatóan működni, működésének jogi háttere elvileg lehetővé tette azt, hogy az USA kormányzatára szálljon át a felső szintű doménnevek kezelése, ami elfogadhatatlan lett volna más nagyhatalmak számára. Ennek megoldására az ITU elindította az Internetirányítási Fórumot (Internet Governance Forum – IGF), amelynek a célja egy globálisan elfogadható irányítási modell kidolgozása. 2016-ban végül az ICANN és az amerikai kormányzat közötti függőségi viszony megszűnt, jelenleg egy többszereplős testület irányítja a globális internetet.

1.3.3. Európai Biztonsági és Együttműködési Szervezet (EBESZ)

Az Európai Biztonsági és Együttműködési Szervezet (EBESZ) a világ legnagyobb, kizárólag biztonsággal foglalkozó kormányközi szervezete. Mandátumához tartozik a fegyverzetellenőrzés, az emberi jogok támogatása, a sajtószabadság ellenőrzése és a választások tisztaságának kontrollja. Titkársága Bécsben működik. 57 tagja elsősorban Európából kerül ki, de részt vesznek benne az európai biztonságra hatással bíró nagyhatalmak, illetve a volt Szovjetunió több tagországa is. 11 társult tagországa van. Gyökerei 1973-ig nyúlnak vissza, az Európai Biztonsági és Együttműködési Konferenciára (Conference on Security and Co-operation in Europe – CSCE). Jelenlegi formájában 1995-ben jött létre az 1994-es, Budapesten tartott kongresszus folyományaként.

Az EBESZ kiberbiztonsággal foglalkozó tevékenysége kiemelten fontos a kibertér globális biztonságának megteremtésében, hiszen az itt kötött megállapodások jogilag nem kötelező érvényűek, a kialkudott normák önkéntesek, elsősorban politikai kötelezettséget jelentenek. Az egyes tagállamoknak így nagyobb mozgásterük van, mint például az ENSZ-ben. Az ilyen normákat bizalomerősítő lépésnek, azaz confidence-building measure-nek (CBM) nevezik, amelyek eredetileg a hidegháború feszültségének enyhítésére jöttek létre. Mivel a kibertérben történő akciók jellegüknél fogva hasonlóképp rontják az országok közötti bizalmat, mint ahogy azt a nukleáris fegyverkezés idejében láthattuk, a CBM-ek jó megoldást jelenthetnek egy kontrollálhatatlan kiberkonfliktus kitörésének megelőzéséhez, már csak azért is, mert az államok joga az erőszak használatához a kibertérben egyelőre nem tisztázott teljeskörűen.

Az ENSZ korábban említett GGE jelentései közül a 2013-as és a 2015-ös is kiemeli az államok közötti transzparencia, együttműködés és stabilitás növelésének igényét bizalomerősítő lépések útján. Mivel ez az EBESZ elsődleges küldetései közé tartozik, ráadásul történelmileg komoly eredményeket ért el a szervezet a hidegháború során az amerikai és szovjet felek között, 2012-ben formálisan is felvállalta a kiberbiztonság kérdésének kezelését. Az EBESZ Állandó Tanácsa a PC.DEC/1039 számú döntésével indította útjára azt az informális munkacsoportot, mely a kibertérben történő bizalomerősítést kapta feladatául. A határozat címe „Development of confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies" azaz Bizalomerősítő lépések létrehozása az infokommunikációs technológiák használatából eredő konfliktusok kockázatának csökkentése érdekében. Ennek első eredményeit a 2013-ban kiadott PC.DEC/1106 határozatból ismerhette meg a nagyvilág, majd 2016-ban a PC.DEC/1202 tartalmazta a végső eredményeket. Az ebben szereplő CBM-ek a következők:

- Magatartással kapcsolatos CBM-ek:
  - Információmegosztás az IKT-használatból adódó nemzeti és transznacionális kockázatokkal kapcsolatban (CBM 1).
  - Információmegosztás a nyílt, interoperábilis, biztonságos és megbízható internet létrehozásának érdekében tett lépésekről (CBM 4).
  - Információmegosztás a nemzeti szervezetekről, stratégiákról, szabályokról és programokról (CBM 7).
  - Az IKT-val kapcsolatos nemzeti terminológiák listája (CBM 9).

- Kommunikációval kapcsolatos CBM-ek:
  - Konzultációk megtartása a politikai és katonai feszültségek csökkentése érdekében (CBM 3).
  - Az EBESZ mint platform használata a párbeszédre, a jó gyakorlatok cseréjére, a tudatosságnövelésre és a képességfejlesztéssel kapcsolatos információmegosztásra (CBM 5).
  - Nemzetközi munkacsoport létrehozása, amely évente legalább háromszor ülésezik, illetve további CBM-eket javasol (CBM 11).
  - Nemzeti kapcsolattartó kinevezése, akinél a vitás eseteket jelezni lehet (CBM 8).
  - A kommunikációs vonalak azonosítása és azok hatékonyságának ellenőrzése (CBM 13).

- Felkészültséggel kapcsolatos CBM-ek:
  - A releváns nemzeti szervezetek közötti együttműködés elősegítése (CBM 2).
  - Hatékony jogszabályalkotás a határokon túlnyúló műveletek támogatása érdekében azon hatóságok között, melyek az IKT-eszközök segítségével végrehajtott terrorista és bűnözői tevékenységek elhárításával foglalkoznak (CBM 6).
  - Együttműködési tevékenységek azonosítása a kockázatcsökkentés érdekében (CBM 12).
  - A létfontosságú információs rendszerek védelmének megerősítése (CBM 15)[2]
  - Az IKT-sebezhetőségek jelentése, beleértve ebbe a privát szektort is (CBM 16).

Az EBESZ által kidolgozott CBM-ek hatékonyan segítik az ENSZ céljainak gyakorlati megvalósulását. Ezt támasztja alá az a tény, hogy az EBESZ-tagok 90%-a, 52 delegált vesz részt egy vagy több CBM-ben. A CBM 8 alapján például mind az 52 tag kijelölt egy nemzeti kapcsolattartót, de a CBM 7 szerinti információmegosztás a nemzeti szervezetekről és jogszabályokról is 42 résztvevőt vonzott. Jelen tanulmány írásának idején a PC.DEC/1039 által létrehozott informális munkacsoport vezetője Magyarország állandó képviselője. (Dán 2018)

[2] A létfontosságú információs rendszerek fogalmát 2021. évi XXXI. törvény hatályon kívül helyezte.

1.4. A nemzetközi jog szerepe a kibertérben

A nemzetközi szervezetek fontos szerepet töltenek be az egyes államok viselkedési normáinak kialakításában, de ezek önkéntes, politikai szintű kötelezettséget jelentenek csupán, amelyek fontosak ugyan, de a jogi garanciák nélkül nem tudják teljes értékűen garantálni a kibertér biztonságát. Ezeket a jogi garanciákat a már meglevő nemzetközi jogban kell keresni, hiszen a 2013-as GGE-riportban és azóta többször és többen kijelentették, igaz, csak általánosságban az egyes országok, hogy a nemzetközi jog érvényes a kibertérben is. A gyakorlatban azonban a kibertevékenységeknek vannak olyan sajátosságai, amelyek nem teszik egyértelművé a nemzetközi jog alkalmazását. A Tallinni Kézikönyv ezt a megértést hivatott segíteni, de ez egyelőre inkább egy fontos tudományos mű, semmint az államok közötti együttműködés elfogadott kódexe. Lattmann a következőképp foglalja össze a Tallinni Kézikönyv szerepét:

„A kodifikált szabályok hiánya ugyanakkor nem jelent teljes szabályozatlanságot. A nemzetközi humanitárius jog szokásjogi alapon kötelező elveinek alapul vételével kialakíthatók olyan szabályok, amelyek alkalmazhatósága nehezen megkérdőjelezhető egy informatikai támadás, vagy akár egy átfogó »kiberháború« során. Ehhez alapként az 1977-ben elfogadott I. Kiegészítő jegyzőkönyvet lehet használni, amely számos olyan hadviselési normát foglalt írásos, nemzetközi szerződési formába, amelyek informatikai támadások esetében is alkalmazhatóak. E munka első eredménye a 2013-ban megjelent Tallinni Kézikönyv, amely első alkalommal tett kísérletet e szabályok rendszerbe foglalt megjelenítésére, majd ezt 2017-ben egy újabb kiadás követte. Ezek a munkák olyan szakértői értelmezést jelentenek, amelyek célja, hogy a létező hadviselési jogi normák felhasználásával állítsanak elő egy olyan szabálygyűjteményt, ami egyrészt tükrözi a jelenleg létező alkalmazható szabályokat, másrészt pedig egy későbbi nemzetközi szerződés alapjául is szolgálhatnak akár. Nemzetközi jogi értelemben a kézikönyvek tartalma nem kötelezi az államokat – ám a szokásjogi erejű normák alkalmazásától nem térhetnek el." (Lattmann 2018)

Schmitt és Vihul véleménye szerint két olyan területe van a nemzetközi jognak, ahol a kibertéri cselekmények értelmezése aránylag előrehaladott, legalábbis a Tallinni Kézikönyv ezeket a területeket tárgyalja részletesen. Ezek az erő alkalmazását szabályozó joganyag (jus ad bellum) és a nemzetközi humanitárius jog (jus in bello). Mindkét esetben olyan szabályozásokról beszélünk, amelyek akár egy évszázaddal ezelőtt jöttek létre, bőven az infokommunikációs eszközök és a számítógépes hálózatok megjelenése előtt. (Schmitt–Vihul 2016) Alapelveik azonban, ha nehezen is, adaptálhatók a virtuális térre is. Bódi, Kádár és Petruska a jus in bellót az alábbiak szerint foglalja össze:

„Az államközi viták erőszakos rendezése egyidős az államok alapításával. A klasszikus nemzetközi jogban a háború indításának joga (ius ad bellum) az állami szuverenitás részét képezte.

- *A hadüzenet átvételével a hadviselő országok között beállt a hadiállapot.*
- *Ultimátum küldése esetén az abban foglalt követelések teljesítésének elmaradása esetén állt be hadiállapot.*
- *A hadiállapot beálltakor a hadviselő felek közötti szerződések megszűntek, és a diplomáciai kapcsolatok megszakadtak, még akkor is, ha tényleges harccselekményekre nem került sor. Minden kívülálló ország köteles volt semleges maradni. […]*

A II. világháború pusztításai és a nukleáris fegyverek megjelenése nyilvánvalóvá tették, hogy egy jövőbeni világháború akár az emberiség pusztulását is eredményezheti, ezért a háború indításának jogát mindenképpen korlátozni kellett. Az ENSZ Alapokmányának 2. cikk (4) bekezdése (államok közötti erőszak teljes tilalma) ezért kimondja, hogy »a szervezet összes tagjának nemzetközi érintkezései során más állam területi épsége vagy politikai függetlensége ellen irányuló, vagy az ENSZ céljaival

össze nem férő bármely más módon megnyilvánuló erőszakkal való fenyegetéstől, vagy erőszak alkalmazásától tartózkodnia kell«. […] Az ENSZ elismeri az államok önvédelemhez való jogát, azaz fegyveres erőik önvédelmi helyzetben való alkalmazását. Az ENSZ Alapokmányának alapján a nemzetközi béke és biztonság fenntartásának elsődleges felelőssége az ENSZ Biztonsági Tanácsánál van, amelynek hatásos és érdemi döntéséhez a megtámadott, önvédelmet gyakorló államnak is igazodnia kell."

A jus in bello összefoglalása a következő:

„A háború nemzetközi joga (ius in bello) a háborúskodással járó pusztítást az elkerülhetetlenül legcsekélyebb mértékűre korlátozta. A hadijog a szabályozás tárgya alapján két nagy csoportra (hágai és genfi jog) osztható fel mind a mai napig. A hágai jog a katonai célpontok és a bevethető fegyverek korlátozását írja elő. […] A hágai jog kötelezi az egyezményt aláírókon kívül azokat a hadban álló feleket is, akik ellenfele egyoldalú nyilatkozattal a rendelkezéseit elismeri, vagy legalábbis ténylegesen alkalmazza. A hágai jog előírta, hogy a háborút hadüzenetnek vagy ultimátumnak, azaz feltételhez kötött hadüzenetnek kell megelőznie. A semleges államok hadicselekményben nem vehetnek részt, sőt nem tehetnek semmilyen, valamelyik fél számára kedvező intézkedést (például felvonulási terület, repülőtér átengedése, rádióállomások telepítése). […] A hágai jog egyik pillére a harcosok (kombattánsok) megkülönböztetése a polgári személyektől ez utóbbiak kímélése érdekében. A IV. számú hágai egyezmény és az azt kibővítő 1949-es genfi jog értelmében a reguláris és irreguláris (önként fegyvert fogó lakosság, ellenálló szabadcsapatok, gerillák) csapatok bárhol kifejthetik harctevékenységüket, ha élükön felelős személy áll, messziről felismerhető megkülönböztető jelvényt viselnek, fegyvereiket nyíltan viselik, valamint hadműveleteik során a háború törvényeihez, szokásaihoz alkalmazkodnak. Egy partizánháború esetén a nyílt jelvény- és fegyverviselés elképzelhetetlen, azért az 1977-es I. számú kiegészítő jegyzőkönyv óta csak az összecsapás és az azt megelőző felfejlődéskor követeli meg a nyílt fegyverviselést a jog. A totális háborút a hágai egyezmények kizárják, és megtiltják az ellenséges tulajdon elpusztítását is, kivéve, ha azt a háború követelményei mindenképpen megkívánják. Katonai célpontok kizárólag azok az objektumok lehetnek, amelyek az ellenséges katonai erőfeszítéseket szolgálják. A »feleknek nincs korlátlan joguk az ellenségnek ártó eszközök megválasztásában«, ezért a megkülönböztetés nélkül ható, tömegpusztító, nem csupán katonai célpontok ellen használható nukleáris eszközök alkalmazását a nemzetközi jog eleve kizárja.

A genfi jog tárgya a háború áldozatainak védelme, amelynek rendezésére 1949-ben, Genfben négy átfogó egyezményt kötöttek: az elsőt a hadra kelt fegyveres erők sebesültjei és betegei helyzetének javítására, a másodikat tengeri haderők sebesültjei, betegei és hajótöröttjei helyzetének javítására, a harmadikat a hadifoglyokról való bánásmódra, a negyediket pedig a polgári lakosság háború idején való védelmére. […] A genfi jog személyi hatálya a háborús áldozatokra terjed ki, akik alatt nem csupán a polgári személyeket, hanem azokat a személyeket is értjük, akik valamilyen ok miatt (például sebesülés, fogság, betegség) a fegyveres konfliktusból kiváltak (például hadifoglyok, sebesültek, hajótöröttek). A genfi jog alapelveit egyaránt be kell tartani államok közötti és államon belüli (polgárháború) fegyveres konfliktus során. A nem nemzetközi háborúk során is a konfliktusban közvetlen részt nem vevőkkel megkülönböztetés nélkül emberségesen kell bánni, tilos megölni, megcsonkítani őket, kegyetlenkedni velük. Tilos túszokat szedni, szükséges garanciák nélküli eljárás nélkül ítéletet hozni és azokat végrehajtani. A védett személyek nem mondhatnak le a genfi egyezmény által garantált jogokról (például hadifogoly státusz)." (Bódi–Kádár–Petruska 2014)

Ez a két rövid összefoglalás is számos olyan példát juttat a szakértő eszébe, amelyek rámutatnak a nemzetközi jog körülményes használatára a kibertámadások során. A teljesség igénye nélkül néhány olyan esetet sorolunk fel, amely indokolttá teszi nemzetközi jog alkalmazhatóságának alapos vizsgálatát a kibertámadások esetében:

- A 2016-os amerikai elnökválasztás során az USA álláspontja szerint Oroszország beavatkozott a választási folyamatba, behatolt az egyes pártok és kampánystábok által használt elektronikus információs rendszerekbe, valamint a közösségi hálózatokon keresztül próbálta befolyásolni az amerikai választók döntését. Ezzel szemben Oroszország és Kína kiemelt lépéseket tesz azért, hogy az amerikai bázisú cégeket, mint a Facebook, a Google vagy az Apple kiszorítsa a hazai piacairól, de legalábbis elfogadtassa velük a honos jogukban elvárt normák betartását. Teszik mindezt attól a nem alaptalan félelemtől vezérelve, hogy az amerikai kormányzatnak ezeken a platformokon keresztül befolyásoló hatása lehet az orosz és kínai társadalmakra nézve. A „politikai függetlenség" biztosítása az államhatárokat nem ismerő szolgáltatások esetében tehát nem valósítható meg könnyen. Külön bonyolítja a kérdést az, hogy a korábban említett cégeknek az államoktól függetlenül is van bizonyos szabadságfokuk, amivel sem a nemzetállami, sem a nemzetközi szabályozás nem tud egykönnyen mit kezdeni. A Facebook moderálási elvei, azaz a szólásszabadság foka ezen a platformon nem teljesen transzparens, nem tudja jól lekövetni a különböző kulturális kontextusokat, de mivel 1 milliárdnál is több ember használja, bizonyos esetekben döntő befolyása van fontos politikai döntések meghozatalában, dacára annak, hogy nem állami szereplő.
- Talán a legtöbbet emlegetett kérdés az önvédelemhez való jog alkalmazásának lehetősége. Bár a laikusok számára úgy tűnhet, hogy a „kiberháború" már zajlik, melynek során államok támadnak államokat, valójában ritkán lehet olyan támadásokkal találkozni, amelyek egy országot próbálnak ellehetetleníteni. Ilyen támadásnak minősülhet a 2007-es, Észtország elleni támadás vagy a 2017-es NotPetya kampány. Viszont mindkét eset azt mutatta meg, hogy a gyakorlatban egyáltalán nem egyszerű az állami érintettséget bizonyítani a támadások mögött. Nem véletlen, hogy 2017-ig az attribúció, azaz a támadó megnevezése a sajtó feladata volt, hivatalos politikai szereplők ezt nem tették meg, tekintettel az ezzel járó diplomáciai nehézségekre. Az attribúció komoly politikai döntés, amelyet a rendelkezésre álló technológiai és hírszerzési információk alapján hoznak meg, mérlegelve az ezzel járó politikai előnyöket és hátrányokat. Az „önvédelemhez való jog" alkalmazására egy összetett kibertámadás után viszont még nem láttunk példát, bár az Egyesült Államok már évek óta lebegteti a kinetikus, azaz fizikai világban történő válaszadást egy információs rendszereket érintő támadásra. Ezt megerősítve, körülbelül 2016-tól kezdve több ország is kilátásba helyezte a válaszadást, kiberbiztonsági vagy katonai stratégiájának elemeként. Ezt nevezzük elrettentésnek (deterrence), amely egyben mutatja több ország szándékát arra, hogy offenzív képességeket építsen. Az önvédelem megvalósítása erő nélkül ugyanis nem lehetséges.
- Elvileg a kibertérben is csak katonai célpontokat lehetne támadni, mégis több olyan államilag támogatottnak tekintett kártékony kód kampányról lehet tudni, amelyek szándékosan vagy véletlenül, de civil célpontok működését lehetetlenítették el. A 2015-ben és 2016-ban egyes ukrán erőműveket támadó BlackEnergy nevű trójai mögött Oroszországot sejtik, a brit egészségügyi rendszert ellehetetlenítő WannaCry zsarolóvírust pedig Észak-Koreának tulajdonítják. Mindkét esetben olyan kritikus információs infrastruktúrák estek áldozatul, amelyek civil mivolta megkérdőjelezhetetlen. Különösen a WannaCry aggasztó ebből a szempontból, hiszen a támadó feltehetőleg nem szándékosan célozta meg az egészségügyi információs rendszereket, ráadásul ezt nem is katonai szándékkal tette, amennyiben azonban tényleg államilag motivált volt a támadás, az felveti a számon kérhetőség kérdését.
- Nem egyértelmű, hogy kik a harcosok. Bár egyre több hadsereg alkalmaz olyan informatikai szakembereket, akik a támadó műveletek végrehajtásában vesznek részt, a kiberkatonák többsége nem visel egyenruhát. A kibertérben különösen gyakran használnak olyan közvetítőcso-

portokat, azaz proxykat, akik nem kötődnek a hadsereghez. Ezek lehetnek egyéni szereplők vagy kisebb-nagyobb bűnözői csoportok is, működhetnek a támadó ország határain belül, de akár azon kívül is, hiszen az internet nem ismer határokat. De a „támadó" lehet egy olyan végfelhasználó is, akinek az informatikai infrastruktúráját tudtán kívül használják, például egy botnet részeként. A fizikai világban viszonylag ritkán fordul elő, hogy egy harcos nem tud arról, hogy ő éppen egy harci cselekmény részese, a kibertérben viszont több millió olyan számítógép van, amely egy kártékonykód-fertőzés után egy összetett művelet részese lehet.

- Ez utóbbihoz kapcsolódik a semleges országok területéről végrehajtott cselekmények kérdése. A 2007-es, Észtország elleni támadás utólagos elemzése például bebizonyította, hogy a világ számos országából, így Magyarországról is érkeztek olyan hálózati forgalmak, amelyek hozzájárultak az észt infrastruktúra lebénításához. Természetesen a kor technológiája sokat segített abban, hogy az illetékes hatóságok le tudják kapcsolni a támadásban részt vevő számítógépeket, de a felhő-számítástechnika (cloud computing) megjelenésével a nemzeti hatóságok feladata sokkal nehezebbé vált, hiszen egy támadó erőforrás a felhőszolgáltató bármelyik fizikai adatközpontjában lehet, tehát az sem egyértelmű, hogy melyik ország tartozik felelősséggel a támadás megszüntetésében.

A sok alapvető kérdés közül talán a legfontosabb, hogy mit is jelent tulajdonképpen a támadás fogalma a kibertérben. Az incidensek mögött ugyanis több különböző motivációt találhatunk. A legtöbb esetben anyagi haszonszerzés motiválja az elkövetőket, a kiberbűnözés tehát az, amivel legtöbbször találkozunk. Ennek megítélése egyértelműen a Budapesti Egyezmény körébe tartozik, nincsen vita arról az államok között, hogy ez üldözendő cselekmény, bár az akarat nyugatról keletre, a képesség pedig északról délre csökken ezen bűncselekményág megfékezésére. Szintén gyakran lehet hallani információszerzési célzattal véghezvitt támadásokról. Amennyiben állami szereplő hajtja ezt végre, a cselekmény nemzetközi jogi megítélése szürke zónába tartozik, ahogy azt a későbbiekben látni fogjuk. Nagyon ritkán, de találkozhatunk a hacktivista, illetve elméletileg a kiberterrorista cselekedetekkel is, ilyenkor a csoport célja valamilyen politikai ideológia terjesztése, esetleg ennek az ideológiának a támogatására valamilyen kiberfizikai rendszeren keresztül pusztítás végrehajtása. Ezeket a nemzeti jog kezeli, az eddig ismert esetekben ugyanis vagy államoktól független csoportosulások, például az Anonymous csoport, vagy államokhoz nem egyértelműen, inkább patrióta alapon kapcsolódó csoportok, mint például a Szír Elektronikus Hadsereg (Syrian Electronic Army) tevékenységét lehetett megfigyelni. Katonai műveletek, azaz a nyilvánosság számára is ismert kiberhadviselés esetén azonban fontos annak megállapítása, hogy mikor beszélhetünk támadásról.

Schmitt és Vihul ezt a kérdést az ENSZ Alapokmány 51. cikkéből vezetik le, mely lehetővé teszi az államok számára az erő használatát önvédelem céljából fegyveres támadás esetén:

„A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye." (ENSZ 1945)

A legtöbb kibertámadás, ahogy láthattuk, nem éri el azt a szintet, hogy állam elleni támadásnak nevezhessük, habár egyértelműen nincsen lefektetve az a határ sem, ahol már az egész államot érintő tevékenységről beszélhetünk. Általánosságban a tulajdon megsemmisülése vagy az ember sérülése lehet az a kulcsmomentum, ami kiválthatja az erő alkalmazását egy viszontválaszban, ami lehet kine-

tikus a fizikai világban vagy informatikai jellegű a kibertérben. De ez még mindig nem háború a szó jogi értelmében. Schmitt és Vihul arra is felhívják a figyelmet, hogy a „háború", így a „kiberháború" fogalma is meghaladott a nemzetközi jog fogalmi keretei között, ugyanis a 20. század közepétől a „fegyveres konfliktus" szóhasználat terjedt el a négy Genfi Egyezménnyel párhuzamosan, a humanitárius jog szempontjából ugyanis nem számít, hogy a hadviselő felek betartották-e a hadüzenet formai követelményeit, vagy nem. A katonai jellegű kibertámadások megítélése abban az esetben egyértelmű, amikor egy hagyományos fegyveres konfliktus kísérőjeként jelennek meg, ahogy történt 2008-ban a grúz–orosz konfliktusban vagy a szíriai polgárháborúban. Ezekben az esetekben minden hadviselő félnek be kell tartania a humanitárius jog szabályait. A kiberháborút tehát szerencsésebb „kibertérben történő fegyveres konfliktusnak" nevezni, így különböztetve meg azt a békeidőben végrehajtott kibertéri műveletektől a nemzetközi jog szempontjából.

További kérdéseket vet fel a „támadás" fogalmának meghatározása. Míg mérnöki szempontból egyértelműen (informatikai) támadást hajtanak végre akkor, amikor az információk bizalmassága, sértetlensége és/vagy rendelkezésre állása sérül, esetleg amikor a kritikus információs infrastruktúrák sértetlensége és rendelkezésre állása tekintetében következik be negatív esemény, a nemzetközi kapcsolatok nézőpontjából a támadás ennél mélyebb meghatározást igényel. Először is, a már idézett ENSZ Alapokmány 51. cikke a „fegyveres támadás" kifejezést használja, azonban ez a fogalom nincsen részletesen meghatározva. Értelmezési segítséget jelent az ENSZ 3314. (XXIX) közgyűlési határozata, amely az „agresszió" fogalmát definiálja. Kajtár az alábbiak szerint foglalja össze az agresszió és a fegyveres támadás közötti kapcsolatot:

„*A 3314. sz. határozat előkészítő munkálataiból egyértelmű, hogy az államok különbséget tettek az agresszió és a fegyveres támadás között, és a határozatban az előbbit kívánták meghatározni. Számos okból azonban a határozat mégis nagy jelentőségű. Egyrészt a fegyveres erőszak legtipikusabb formáit sorolja fel, ha csak példálózva is. Másrészt jelzi, hogy a fegyveres erőszak különböző formái és különösen intenzitása jogilag is relevánsak. Az agresszió definíciójából egyértelműen kiderül, hogy minden agresszió egyben fegyveres erőszak, de ez fordítva már nem igaz (vagyis az agresszió a fegyveres erőszak teljes részhalmaza). Ez már a határozat preambulumából is világosan kiderül, amely a következőképpen fogalmaz: »az agresszió az erő jogtalan alkalmazásának legkomolyabb és legveszélyesebb formája«. Harmadrészt egyértelművé teszi, hogy fegyveres erőszakot közvetett módon is el lehet követni, azaz nem csupán a fegyveres erőszak közvetlen formái sértik a 2. cikk (4) bekezdését. Negyedrészt világossá teszi a határozat, hogy – mint minden más, a 2. cikk (4) bekezdéséhez kapcsolódó erőszakfogalomnál – itt is államközi erőszakfogalomról van szó. Illeszkedve a 2. cikk (4) bekezdésének logikájához, a határozat 1. cikkében lévő fogalom meghatározás szerint agresszió* »fegyveres erő alkalmazása valamely állam részéről…« Az agresszió államközi jellegét a 2. cikk ismét megerősíti: »Fegyveres erőnek az Alapokmány megsértésével elsőként való alkalmazása valamely állam részéről – első megítélésre – agresszió bizonyítékának tekintendő…«" (Kajtár 2010)

Kovács[3] könyvében idézi a közgyűlési határozat pontos szövegét is, amely segít megérteni azokat a példákat, amelyek agressziónak minősülnek:

„*Az agresszió fegyveres erő alkalmazása egy állam által más állam szuverenitása, területi integritása vagy politikai függetlensége ellen, illetve az Egyesült Nemzetek Alapokmányával össze nem férő bármely más módon.*"

[3] https://jak.ppke.hu/uploads/collection/205/file/Kovacs_Peter_A-nemzetkozi-jog-fejlesztesenek-lehetosegei_Pazmany_Press_2010.pdf

Ezt követi a tényállások listája. Agresszió tehát, függetlenül attól, hogy volt-e hadüzenet,

i) ha egy állam fegyveres erői inváziót vagy támadást hajtanak végre más állam területe ellen, vagy mindenfajta katonai megszállás, bármilyen ideiglenes is, amely ilyen invázió vagy támadás következménye, vagy más állam területének erő alkalmazásával történt annektálása;
ii) ha egy állam fegyveres erői bombázzák más állam területét, vagy ha egy állam bármiféle fegyvert használ más állam területe ellen;
iii) ha egy állam kikötőit vagy partvidékét más állam fegyveres erői blokád alá veszik;
iv) ha egy állam fegyveres erői megtámadják más állam szárazföldi, tengeri vagy légierőit, tengeri és légiflottáját;
v) ha egy állam fegyveres erőit, amelyek más állam területén tartózkodnak a fogadó állammal történt megegyezés alapján, az egyezményben foglalt feltételek megszegésével használja fel, vagy ha azok az egyezmény lejárta után tovább tartózkodnak az illető területen;
vi) ha egy állam megengedi, hogy területét, amelyet egy másik állam rendelkezésére bocsátott, a másik állam agressziós cselekmény elkövetésére használja fel harmadik állam ellen;
vii) ha egy állam fegyveres bandákat, csoportokat, önkénteseket vagy zsoldosokat küld – vagy a nevében ilyeneket küldenek – más állam ellen fegyveres cselekmények végrehajtására, amelyek oly súlyosak, hogy kimerítik a fent felsorolt cselekményeket, illetve ha egy államnak komoly része van ebben. (Kovács 2010)

A Tallinni Kézikönyv a fenti jogforrások alapján javaslatot tesz a „kibertámadás” meghatározására, amely merőben eltér attól a fogalomtól, ami a fenti, mérnöki terminus technicusból vezethető le. A Kézikönyv 92. Szabálya ekképpen fogalmaz:

„Egy kibertámadás olyan kiberművelet, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható.”

Ezen forrás 103. Szabálya szerint a kiberhadviselés eszközei a kiberfegyverek és a hozzájuk tartozó kiberrendszerek, módszerei pedig azok a kibertaktikák, technikák és eljárások, melyekkel az ellenséges tevékenységet végrehajtják. (Schmitt 2017)

A kiberháború, kibertámadás és kiberfegyver szavak a nemzetközi jog mélyebb megismerése után tehát inkább az újságírók, semmint a nemzetközi jogászok szótárába tartozik. Ez azért is megnyugtató, mert ha egy tisztán informatikai úton megvalósuló támadást a szó jogi értelmében is támadásnak minősítenének, az jogalapot adna a NATO Észak-atlanti Szerződés V. cikkelyének alkalmazására. A Szerződés szövege ugyanis ezt írja:

„A Felek megegyeznek abban, hogy az egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Felekkel egyetértésben, azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és az ennek következtében foganatosított minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezen intézkedések akkor zárulnak le, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat.” (NATO 1949)

Az V. cikkely alkalmazásának lehetősége már a 2007-es, Észtország elleni művelet idején felmerült, akkor azonban nem éltek vele a felek. Elkezdődött azonban egy komoly gondolkodás arról, mik lehetnek azok a kiváltó okok, amelyek mellett a kollektív védelmet alkalmazni kell és lehet akkor is, ha a támadás tisztán a kibertérből érkezik, a fizikai térben azonban semmilyen más művelet nem kíséri azt. Az Észak-atlanti Szerződés Szervezete folyamatosan elemzi ezt a kérdést, de megnyugtatóan csak a saját információs rendszerek védelméről intézkedett a 2010-es években, a kollektív védelem gyakorlata nem alakult ki. Veenendaal és szerzőtársai 2016-ban foglalták össze, milyen lépéseket kell tennie a NATO-nak annak érdekében, hogy erre a kérdésre választ kapjon. A szerzők az alábbi javaslatokat tették:

- A NATO ismerje el a kiberteret mint a katonai műveletek lehetséges doménjét. Ezt a katonai szövetség a 2016-os varsói csúcson megtette. Tálas összefoglalója szerint „*Az állam- és kormányfők azzal, hogy a kibervédelmet a NATO kollektív védelmi feladatai közé sorolták, az operatív hadviselés területét pedig kiterjesztették a kibertérre is, lehetővé tették, hogy egy tagállama elleni koordinált kibertámadást a NATO a szövetség egésze elleni támadásnak tekintsen. Deklarálták azt is, hogy a NATO támogatni fogja a kiberhadviselés fenyegetéseinek elhárításával és a kibervédelemmel összefüggő kutatásokat, illetve a tagállamok védelmi iparának együttműködését e téren.*”
- Különböztesse meg a békeidőre szóló, hálózati védelemre vonatkozó mandátumot a katonai műveletekre és a kollektív védelemre szóló mandátumtól, és vizsgálja meg egy olyan szabályozás létrehozását, amely lehetővé teszi a szövetségeseknek a képességek teljes spektrumának felhasználását az elrettentés és védelem céljából, bármilyen kibertérből érkező fenyegetésre.
- Hozzon létre olyan doktrínát és eljárásrendet, mely a kiberképességek használatát katonai műveletekben teszi lehetővé. (Veenendaal–Kaska–Brangetto 2016) (Tálas 2016)

Jelen tanulmány írásának idején annak a küszöbértéknek a meghatározása történik, amit már a nemzetközi jog alapján is fegyveres támadásnak lehet minősíteni, de továbbra sem világos, hogyan reagálna a NATO egy komoly hatással rendelkező, kibertérből érkező incidensre. Ez különösen aggasztó az Ukrajnában végrehajtott kiberműveletek sorozatának fényében, amelyek erősen feszegetik az agresszió fentiek szerint leírt megfogalmazását. Az ukrán kibervédelemmel foglalkozó szervezetek gyakorlatilag havonta szembesülnek, vagy legalábbis hoznak nyilvánosságra olyan incidenseket, amelyek jogi elemzésének eredményeképp a műveletet fegyveres támadásnak lehetne minősíteni. 2018 júliusában például arról adtak tájékoztatást, hogy gyaníthatóan oroszországi támadók az ivóvízellátást veszélyeztették a tisztítórendszerek informatikai rendszereinek támadásával. (Martin 2018)

A NATO mindenesetre legalább a kibervédelmi gyakorlatai során teszteli az V. cikkely alkalmazhatóságát. A rendszeresen megrendezésre kerülő Locked Shields gyakorlat, mely az egyes NATO-tagországok kiberbiztonsági együttműködését teszteli egy szimulált kibertámadás során, minden évben olyan helyzetbe próbálja hozni a csapatokat, hogy felvessék a kollektív védelem lehetőségét. A már idézett Veenendaal egy interjúban arról számolt be, hogy míg a 2016-os gyakorlaton nem került sor az V. cikkely alkalmazására, a 2017-es gyakorlaton az egyik résztvevő csoport olyan módon tudta a forgatókönyv határait kifeszíteni, hogy a gyakorlat végeredményeként kérelmezni tudták a NATO beavatkozását. (Calatayud 2017)

A fokozódó kibertéri kihívások és a gyakorlatok eredményei teszik lehetővé, hogy a katonai-szakmai felkészüléssel párhuzamosan a politikai támogatás is megjelenjen a NATO tagországainak részéről. Kis lépésekkel ugyan, de évről évre tovább merészkedik az a politikai állásfoglalás, melyet az aktuális csúcstalálkozó után tesznek közzé. A 2018-as brüsszeli csúcs zárónyilatkozata például reagál mindazokra a változásokra, melyek a 2016-os varsói csúcs óta történtek, amikor is a kiberteret műveleti területté nyilvánították. Így különösen érdekes megvizsgálni az alábbi pontokat:

- „*Képesnek kell lennünk olyan hatékonyan működni a kibertérben, ahogy tesszük azt a levegőben, a vízen és a tengeren, így megerősítve és támogatva a Szövetség általános elrettentési és védelmi szempontjait.*" Ez a rész utal arra, hogy a kibertérben NATO-szinten is szükséges az offenzív képességeket fejleszteni, egyben a védelmi szemszögű megközelítés mellé az elrettentés is felzárkózik. Kiemeli továbbá azt a tényt, hogy a katonai műveleteket a kibertérben is végre lehet hajtani, megerősítve ezzel a 2016-os állásfoglalást.
- „*Egyetértettünk abban, hogyan integráljuk a szuverén kiberképességeket a Szövetség műveleteibe és misszióiba, melyet önkéntesen ajánlanak fel a Szövetségesek, erős politikai felügyelet keretében.*" Ez egyben azt is jelenti, hogy továbbra sincsen egyértelmű politikai állásfoglalás arról, mikor lépi át egy kibertámadás a közös védelem kezdeményezésének határát, de a tagországok készek magas politikai szinten megvizsgálni a válaszadás lehetőségét, amennyiben ez szükséges.
- „*A NATO védelmi mandátumának megerősítése mellett eltökélt szándékunk képességeink teljes körének felhasználása, beleértve ebbe a kiberképességeket is, a kiberfenyegetések teljes spektrumának elrettentésére, kivédésére és válaszadásra, beleértve ebbe azokat is, melyeket hibrid kampányok részeként hajtanak végre.*" Ez fontos üzenet Oroszország felé, hiszen a NATO jelzi, nem hagyja annyiban a kibertámadásokat, még azokat sem, melyek a hibrid hadviselés részeként nem érték el a fegyveres beavatkozás szintjét. A teljes képességek emlegetésével a hagyományos, kinetikus válaszadást is elvileg lehetővé teszik.
- „*Az egyes szövetséges tagállamok szükség esetén megfontolhatják a kártékony kibertevékenységek attribúcióját és a koordinált válaszadást, az attribúciót szuverén nemzeti előjogként elismerve.*" Miután az Egyesült Államok, majd több ország is hivatalosan élt az attribúció lehetőségével, azaz egy bizonyos országot nevesített egy kibertámadás elkövetésével kapcsolatosan, a katonai szövetség állást foglalt arról, hogy elismeri az attribúciót mint szuverén jogot, de ezzel egyelőre nem kíván szövetségi szinten élni.
- „*Megerősítjük elkötelezettségünket abban, hogy mindenkor a nemzetközi jog, így az ENSZ Alapokmány, a nemzetközi humanitárius jog és az emberi jogok keretében cselekszünk, amennyiben ezek alkalmazhatók.*" A NATO ezzel kijelöli azt a nemzetközi joganyagot, melyet érvényesnek tart a kibertérben, ahogy tette azt 2014-ben is, de meghagyja azt a kiskaput, hogy bizonyos esetekben ezek a keretrendszerek nem lesznek alkalmazhatók a virtuális térben. (NATO 2018)

1.5. Kiberkémkedés

Míg a kiberhadviselés, azaz a kibertérben történő katonai műveletek nemzetközi joggal összefüggő elemzése meglehetősen előrehaladott, miközben a gyakorlatban ritkán találkozunk vele, a kiberkémkedés, azaz az elektronikus információs rendszerekben tárolt információk hírszerzési célú támadása napi gyakorlatnak számít az államok eszköztárában, nemzetközi jogi szabályozása viszont minimális. A Tallinni Kézikönyv 32. szabálya is ezt emeli ki:

„Bár a békeidőben történő állami kiberkémkedés önmagában nem sérti a nemzetközi jogot, a módszer, amivel kivitelezik, már lehet, hogy az előírásokba ütközik." (Schmitt 2017)

Nem meglepő tehát, hogy a szakmai közvélemény először a kibertérben történő hírszerzéssel találkozhatott a kibertéri konfliktusok sorából. Ilyen tevékenységekről már az 1990-es évek második felében lehetett hallani, például a gyaníthatóan Oroszország által végrehajtott Moonlight Maze akciót 1999-ben tárta fel a sajtó. Emlékezzünk vissza az ENSZ kiberbiztonsági tevékenységéről szóló korábbi fejezetre, melyben azt írtuk, először 1998-ban Oroszország kezdett el a kibertéri tevékenységekkel foglalkozni a nemzetközi szervezetben. A jelek tehát arra utalnak, hogy a nagyhatalmak, kiemelten az Egyesült Államok és Oroszország már az 1990-es évek végén aktívan használták a kiberteret titkos műveletek végrehajtására. A valószínűleg Kína által végrehajtott Titan Rain művelet pedig 2003-ban indult, így a képességfejlesztés valószínűleg ott is a 90-es évek végén vette kezdetét. A nemzetközi kapcsolatokat befolyásoló kiberműveletek tehát már jóval azelőtt részesei voltak az állami gyakorlatoknak, mielőtt a közvélemény erről tudomást szerzett volna.

Ez nem meglepő annak tudatában, hogy az informatika széles körű elterjedésével a hírszerzés sosem volt olyan könnyű, mint a 21. században. A hírszerzés célja Izsa szerint

„a (politikai és katonai) döntéshozók támogatása információkkal. A politikai jelentőséggel bíró döntéseket bonyolult helyzetben, hiányos informáltság mellett, a várható következmények részleges ismeretében, kockázatokat vállalva hozzák meg az illetékesek. Az informáltság növeli a döntések megalapozottságát és esélyeit a kedvezőbb eredmény bekövetkezésének elősegítésére. Ám ennek alapvető feltételeként az információknak összhangban kell lenniük a tényekkel." (Izsa 2009)

Tekintettel arra, hogy az információk napjainkban szinte kizárólagosan digitális formában keletkeznek, tárolódnak, továbbítódnak és kerülnek feldolgozásra, a hírszerzéssel foglalkozó szakemberek elsődleges feladata azoknak a számítástechnikai eszközöknek a fellelése, melyek a döntéshozatalhoz releváns információkat kezelik. Ehhez pedig nem feltétlenül kell elhagyni a saját országot, hiszen a határtalan internet lehetőséget biztosít a biztonságos körülmények között végrehajtott információszerzésre is, a határok átlépése nélkül.

Tovább könnyíti a helyzetet, hogy az információk jelentős része eleve nyilvánosan jelenik meg. A nyílt forrású hírszerzés integráns része a hírszerzési eljárásoknak, de az olyan szolgáltatók, mint a Google vagy a Facebook lehetővé tették a személyekről, intézményekről, történésekről szóló információk szinte korlátlan begyűjtését. Ferenczy megfogalmazásában a nyílt forrású hírszerzés

„*olyan információgyűjtő eljárás, amely során a nyilvánosan (a publikum számára) elérhető forrásokból az információkat felkutatják, elemzik, értékelik és felhasználják egy adott cél elérése érdekében, általában a parancsnok és annak közvetlen törzse által feltett kérdés megválaszolására. Más szavakkal az információszerzés kipróbált eljárásainak alkalmazása a széles körben hozzáférhető nyílt adatforrásokra. A nyílt forrású információszerzés nem kizárólag katonai felderítései vagy információszerzési kategória, mivel ezt a tevékenységet a civil szférában is folytatják.*" (Ferenczy 2007)

A társadalom digitalizálódásával ráadásul olyan különleges metaadatokhoz is hozzá lehet férni, amelyek kontextuális információt is tudnak szolgáltatni a nyílt forrásból megszerzett információkhoz. Bányász a közösségi médiába beleérti az okoseszközök használatát is, így egy olyan kiterjesztett teret határoz meg, mely a metaadatok széles körét kínálja a felkészült hírszerzők számára a következőképp:

„*Nem csak az esetleges, akár már a gyártósoron feltelepített kémprogramok jelentenek veszélyeket, hanem az egyes feltelepített alkalmazások is, hiszen használatuk érdekében különböző hozzáféréseket biztosítunk személyes adatainkhoz. A Facebook például az alábbi adatokhoz kér hozzáférést: személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet-hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardvervezérlők (fénykép- és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). Természetesen eldönthetjük, hogy feltelepítjük-e az alkalmazást a telefonunkra, de hasonló engedélyeket kér a Google is a szolgáltatásai használataiért cserébe, már pedig egy androidos telefon esetében nincs döntési lehetőségünk, nem távolíthatjuk el a telefonról a Google alkalmazásait.*” (Bányász 2015)

A döntéshez szükséges információk tehát gyaníthatóan elérhetők az interneten vagy az internetről elérhető elektronikus információs rendszerekben. Nyilvánvalóan kiberkémkedési tevékenységről az utóbbi esetben beszélünk, azaz a nem nyilvános információk nem jogosult megszerzése tartozik ebbe a fogalomkörbe.

Buchan az államilag támogatott kiberkémkedés és a nemzetközi jog kapcsolatában kiemeli, hogy nincsen egyetlen nemzetközi egyezmény sem, amely a kiberkémkedést szabályozná, egyben olyan egyezmény sincsen, amely a kémkedést szabályozza, és egyértelműen adaptálható lehetne a kiberkémkedésre, legalábbis békeidő esetén. Mivel azonban a nemzetközi jogrend az államok szuverén egyenlőségére épít, ezen cselekmény szembekerülhet a nemzetközi jog általános elveivel, egyben kijelenthető, hogy a nemzetközi kapcsolatokban a kibertéri hírszerző tevékenységek elsősorban a szuverenitás szempontjából vizsgálhatók. Fegyveres konfliktus során a Genfi Egyezmény I. Kiegészítő Jegyzőkönyvének 46. cikkelye vonatkozik a hírszerzési tevékenységekre, történjenek azok akár a fizikai, akár a virtuális világban. (Buchan 2016)

A területi szuverenitás a kibertérben kétféleképp értelmezhető. Egyrészt a kibertér egy olyan környezet, mely egyetlen ország területéhez sem tartozik, hasonlóan például a világűrhöz. Ebben az esetben azokat a joggyakorlatokat kéne alkalmazni, amelyeket a semleges területekre már korábban megalkottak. Az egyes államok azonban határozottan kinyilvánították igényüket arra, hogy szuverenitást gyakoroljanak a saját kiberterük felett, ezért napjainkban ezt a virtuális, emberek által létrehozott képződményt is hasonlóan kezelik, mint a saját fizikai területüket. Így történt ez Magyarországon is, a 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégia kinyilvánítja azt az igényt, hogy a nemzeti kibertér felett Magyarország szuverenitást kíván gyakorolni. Suba ezt ekképp fogalmazta meg:

„*A kibertér nincs tekintettel az állami határokra, eszközeit és infrastruktúráját meghatározó mértékben az üzleti szektor szereplői tulajdonolják, működtetik és ellenőrzik. […] A fentiek figyelembevételével került meghatározásra a kibertér fogalma, miszerint a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a Magyarországon található, a globális kibertér részét képező elektronikus információs rendszerekből és ezen elektronikus információs rendszereken keresztül adatok és információk formájában Magyarországra irányuló és hazánkban megjelenő társadalmi és gazdasági folyamatok összességéből áll.*” (Suba 2014)

A nemzeti kibertér feletti szuverenitás alapját az adja, hogy a kibertér nem lenne elképzelhető fizikai infrastruktúrák, azaz hálózatok, szerverek, végpontok és hasonló informatikai alkotóelemek nélkül. Amennyiben tehát ezek az alkotóelemek az ország területén helyezkednek el, az ezeken tárolt információk ellen végrehajtott hírszerzési tevékenység sérti az adott ország szuverenitását. Nem véletlen tehát, hogy egyre több kormányzat igyekszik az érzékeny információkat kezelő rendszereit minden tekintetben a belső határok között tartani. Magyarország sem kivétel ez alól, a 2013. évi L. törvény az állami és önkormányzati szervezetek elektronikus információbiztonságáról elvárja, hogy a jogszabály alá tartozó intézmények az országhatáron belül kezeljék a magyar közigazgatás adatvagyonát, illetve azt csak kockázatelemzés és hatósági engedély beszerzése után tehessék külföldi szerverre, ekkor is csak az Európai Unió határain belül.

Vannak azonban olyan esetek, amikor az információ nemzeti határon belül tartása nem egyszerű. Már említettük a felhőszolgáltatók jelentette kihívásokat, amikor egyáltalán nem lehet biztosan megmondani, hogy az információ pontosan melyik ország területén található, köszönhetően a szolgáltatók adatközpontjai közötti folyamatos adatszinkronizálásnak. De még nehezebb megoldást találni az adatátvitelt érintő támadásokra. Az internet működését az úgynevezett routing, azaz útválasztó protokollok segítik, ezek teszik lehetővé a kliens és a szerver közötti megbízható adatkapcsolat létrejöttét és fenntartását. Az egyik ilyen alapvető protokoll a Border Gateway Protocol, röviden BGP. Ennek manipulálása elvileg lehetővé teszi, hogy a teljes internetforgalmat „eltérítsék", azaz a legkézenfekvőbb útvonal helyett egy bizonyos ország felé irányítsák. Ez történt 2017 decemberének közepén, amikor a Google, a Facebook, az Apple és Microsoft szerverei felé irányuló forgalom 3 percig minden műszaki logika nélkül Oroszország területén található infrastruktúra elemeken keresztül folyt át. A feltételezések szerint ebben a 3 percben az orosz hírszerző szervezetek hozzájutottak az amerikai informatikai mamutvállalatok felé haladó teljes globális forgalomhoz, amely nagyon értékes információforrás lehetett, még akkor is, ha a tartalom maga titkosított volt, és valószínűleg jelenleg nincsen meg a képesség annak dekódolásához. De a metaadatok elemzése, illetve a robbanásszerűen fejlődő informatika mellett a kriptográfiai lehetőségek előrehaladása elvileg lehetővé teszi értékes információk megszerzését ebből a hatalmas adathalomból, akár rövid távon is. (Goodin 2017)

Az ilyen esetekben a területi szuverenitás nyilvánvalóan nem értelmezhető. Figyelembe lehet azonban venni a be nem avatkozás elvét, amely a nemzetközi jog azon próbálkozása, hogy az állami szuverenitást megvédje bármilyen külső hatástól. Ez az elv két pilléren nyugszik. Egyrészt egy ország megsérti a be nem avatkozás elvét akkor, ha olyan cselekményt hajt végre, amely hatással van egy másik állam szuverén cselekedeteire, másrészt ha a cselekmény természeténél fogva kényszerítő erejű. Buchan az első pillért a kibertér vonatkozásában úgy magyarázza, hogy például amennyiben egy ország a minősített adatait egy külföldi ország kiberinfrastruktúráján tárolja vagy továbbítja, akkor ezt az információt tiszteletben kell tartani a nemzeti szuverenitás részeként abban az esetben, ha ez az információ hozzájárul az állam közfeladatainak ellátásához. Üzleti titkoknál ez az érvelés már nem áll fenn. Ha például egy ország külképviseleti szerveinek elektronikus információs rendszereit támadják információszerzési céllal, az megalapozza a be nem avatkozás elvének megsértését az első pillér szerint. (Buchan 2016) Ilyen támadások pedig gyakran előfordulnak. A kelet-európai régió kitettsége ebből a szempontból kiemelkedő, a 2010-es években számos kártékony kód támadta meg az itt működő nagykövetségeket. A WhiteBear, más néven Turla csoport tevékenysége például kifejezetten ezekre az intézményekre fókuszál, és a célpontok kiválasztása Oroszország információéhségét hivatott kielégíteni. Meg lehet említeni továbbá a Ke3chang csoportot is, amelyet az elemzések szerint Kínában kell keresni, és szintén a diplomáciai célpontok állnak érdeklődése középpontjában. De Edward Snowden szivárogtatásai szerint az amerikai National Security Agency, az NSA is rutinszerűen figyelte meg más országok, így közeli szövetségeseinek diplomáciával kapcsolatos informatikai forgalmát is.

A másik feltétel a kényszerítő erő alkalmazása. Ez azt jelenti, hogy egy ország olyan tevékenységet hajt végre, mely komolyan befolyásol egy másik országot jogszabályalkotásában vagy állami gyakorlatában, olyan tevékenységekre kényszeríti, amelyeket szabad akaratából az nem tett volna

meg. Erre sokkal nehezebb példát hozni a nyilvánosságra került kiberbiztonsági incidensek sorából, jellegénél fogva ugyanis az ilyen kényszerítések csak jóval később kerülnek a nyilvánosság elé. Kiindulva viszont abból, hogy az információk szinte kizárólagosan digitális formában léteznek napjainkban, nem zárható ki, hogy már a 2010-es évtizedben is képesek voltak egyes országok más országok döntéseit befolyásolni a területükön kívül megszerzett, minősített információk felhasználásával. Amíg azonban ilyen esetek nem kerülnek napvilágra, és nincsen róla a hágai Nemzetközi Bíróság által hozott ítélet, csak elméletben állapíthatjuk meg, hogy a kiberkémkedés bizonyos esetekben a nemzetközi jogba ütközhet. A gyakorlat azt mutatja, hogy ez a megfelelő képességekkel rendelkező országok napi rutinja, amelynek egyelőre még a nemzetközi normák rendszere sem szab határt.

A fedett információszerzés tehát elfogadott gyakorlat az államok kapcsolatában. A hírszerzés legtöbbször a biztonságos saját országból történik. Előfordul viszont, hogy a hírszerzők „terepen" dolgoznak, azaz a célország területéről hajtják végre az elektronikus információs rendszerek elleni támadásokat. Ez érthető, hiszen számos esetben a megcélzott rendszer zárt hálózaton működik, internetről nem elérhető, így fizikailag kell hozzáférni a rendszerhez, ahogy történt ez a Stuxnet kártékony kód bejuttatása esetén is a szigorúan védett bushehri nukleáris telepre is. Az ilyen cselekményeket a szokásjog alapján minden állam igyekszik kivédeni, esetleg észlelése után számára kedvező módon befolyásolni, például hamis információk átadásával. Ritkán azonban, de előfordul, hogy a közvélemény számára is látható módon szakítanak meg egy hírszerzési műveletet. Amennyiben saját állampolgár vagy nem diplomáciai fedésben dolgozó hírszerző vesz részt a felszámolt műveletben, az adott ország büntető törvénykönyve alapján történik a számonkérés, diplomáciai akkreditációval rendelkező személyek esetén pedig jellemzően kiutasítják az országból az illetőt. A 2016-os amerikai elnökválasztásra tett befolyásolási kísérlet miatt Barack Obama leköszönő elnök 35 orosz diplomatát utasított ki az Egyesült Államok területéről és bezáratott két orosz diplomáciai létesítményt. Tekintettel arra, hogy ez röviddel a befolyásolási kísérlet nyilvánosságra kerülése után történt, bizonyosak lehetünk abban, hogy az amerikai elhárító szervezetek hosszabb ideje tudatában voltak azon személyeknek, akik amerikai földről vettek részt a műveletben.

Fegyveres konfliktus idején a kémek jogállása megváltozik. Ahogy a Tallinni Kézikönyv 89. pontja fogalmaz: „A fegyveres erők azon tagja, aki kiberkémkedési tevékenységben vesz részt az ellenséges területen, elveszíti a hadifoglyoknak járó jogokat, és kémnek tekinthető, mielőtt csatlakozna azon fegyveres erőhöz, melyhez tartozik." Így bár a kiberkémkedés fegyveres konfliktus esetén sem tiltott tevékenység, az ebben résztvevők nagyobb kockázatot vállalnak, mintha azt békeidőben tennék. Libicki így foglalja össze a kiberkémkedés dilemmáját, amelyet akár békeidőben, akár fegyveres konfliktus idején érdemes megfontolni:

„*A lecke, amit meg kell fontolni az, hogy milyen üzenetet hordozzon a kiberkémkedési tevékenységed, ha és amennyiben azt felfedezik. Amennyiben nem akarod, hogy feszültséget szüljön, duplázd meg a műveleti biztonságot, de ne számíts sikerre. Emellett kerüld el a katonai célpontok elleni hírszerzést krízis esetén, vagy legalábbis olyan technikákkal közelítsd meg ezeket, hogy azok biztosan elkülöníthetők legyenek egy kibertámadás előkészítésétől. Amennyiben viszont a képességeidet szeretnéd megvillantani vagy jelzésértékű szándékaid vannak, olyan narratívát készíts elő, amely számít a felfedezésre. De mindezt gondold végig alaposan a művelet előtt.*" (Libicki 2018)

1.6. Kiberdiplomácia

A kibertér, ahogy láthattuk, roppant komoly értelmezési kihívást jelent a kialakult nemzetközi biztonságpolitikai környezetben. Évtizedek óta folynak állami hátterű műveletek, melyekre valamilyen módon reagálni kell. A válaszadás természetesen csak végső esetben lehet katonai jellegű, a feszültségeket lehetőség szerint bilaterális és multilaterális keretek között, diplomáciai eszközökkel kell csökkenteni. Rácz megfogalmazása szerint

„*[a] diplomácia az államközi (külpolitikai) kapcsolatok nemzetközi jog által szabályozott, intézményes formája. Elsődleges tartalma az államok, mint a nemzetközi jog alanyai, azaz egyenjogú és szuverén entitások (önálló és cselekvőképes egységek) érdekeinek képviselete azok összehangolt, békés és civilizált módon történő érvényesítése céljából, az együttműködés és a kapcsolatfejlesztés útján. Az érdekképviselet gyakorlati módja az államok külpolitikai céljainak, szándékainak, törekvéseinek az érintettek részére történő – két- és többoldalú keretben megvalósított – világos, érthető, pontos, artikulált kifejtése az előírt speciális (diplomáciai) udvariassági szabályok betartásával úgy, hogy az még az esetleges nézeteltérések, potenciális konfliktusok fennállása mellett is biztosítsa a felek közötti folyamatos konzultációt, tárgyalást, megoldáskeresést, kompromisszumos (kölcsönösen elfogadható) végkifejlethez vezető együttműködést. Mindezt egy sajátos intézményi keretben, a külképviseleti munkát végző személyek és szervezetek működési és tevékenységi feltételeinek meghatározott módon történő – kölcsönösségen alapuló – biztosítása mellett.*” (Rácz 2010)

Ennek megfelelően a diplomácia területén kialakult egy új szakterület, amelyet kiberdiplomáciának neveznek. Barrinha és Renard meghatározása szerint

„*a kiberdiplomácia a kibertérben megjelenő diplomácia, más szavakkal a diplomáciai erőforrások használata, valamint a diplomáciai funkciók kiaknázása a nemzeti érdekek kibertérben történő érvényesítése céljából. Ezeket az érdekeket általánosságban a nemzeti kibertér vagy kiberbiztonsági stratégia fogalmazza meg, mely jellemzően hivatkozik a diplomáciai agendára. A kiberdiplomácia legfontosabb témái között megtalálhatók a kiberbiztonság, a kiberbűnözés, a bizalomerősítés, az internetszabadság és az internetirányítás kérdései.*” (Barrinha-Renard 2017)

A kibertér legfontosabb multilaterális intézményei diplomáciai szempontból az ENSZ, az EBESZ és az ITU, de például a Délkelet-ázsiai Nemzetek Szövetsége (ASEAN – Association of Southeast Asian Nations) is egy kiemelkedően fontos regionális szervezet, ahol a kiberbiztonság regionális kérdéseiről születnek többoldalú megállapodások, vagy a Visegrádi Négyek (Csehország, Lengyelország, Szlovákia, Magyarország) közötti regionális együttműködést is érdemes megemlíteni.

Magyarország kiberdiplomáciai tevékenysége során az ország a Nemzeti Kiberbiztonsági Stratégiájában foglalt értékeket képviseli:

„Magyarország a globális kibertér minden Magyarországgal hasonló értékrendet valló állami és nem állami szereplőjével kölcsönös bizalmon alapuló együttműködés kialakítását és fenntartását célozza meg, továbbá szövetségi és nemzetközi kapcsolati rendszerén, különösen az EU és a NATO, továbbá az Európai Biztonsági és Együttműködési Szervezet (EBESZ), az ENSZ, az Európa Tanács és más nemzetközi szervezeti tagságán keresztül törekszik a globális kibertér szabad és biztonságos használatának szavatolására. Magyarország tudatában van annak, hogy a kibertérben megjelenő fenyegetések és támadások elérhetnek egy olyan szintet, ami szövetségesi együttműködést tehet szükségessé, ezért kiemelten fontosnak tartja, hogy a kiberbiztonság kérdése bekerült a NATO Alapító

Okmányának 5. cikkelye alá tartozó kollektív védelem körébe. E szövetségesi nemzetközi együttműködésben Magyarország saját biztonsága miatt is érdekelt. Magyarország különös figyelemmel tekint a közép- és kelet-európai régióra, melynek kiberbiztonságát regionális együttműködések keretében tovább erősíthetőnek látja." [1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról]

Bilaterálisan, azaz két állam között jellemzően akkor történik kiberdiplomáciai együttműködés, ha az adott országok érdekei kölcsönösen sérülnek az egymással szembeni kibertevékenységek miatt. A legismertebb példa erre az Amerikai Egyesült Államok és Kína közötti 2015-ös megállapodás. Ekkor Barack Obama és Hszi Csin-ping állapodott meg a kiberbűnözés elleni kölcsönös fellépésben, valamint a kibertérben történő, gazdasági célú hírszerzés korlátozásában. Egy forródrót létrehozásáról is döntöttek, mely segít a kérdéses esetek gyors tisztázását, elkerülve ezzel egy incidens eszkalálódását. Történt mindez azután, hogy az amerikai államot és vállalatokat súlyosan érintette a kibertérben történő kínai hírszerzés, amely során kínai vállalatokhoz jutott az amerikai iparban keletkezett szellemi tulajdon, ezzel tisztességtelen előnyhöz juttatva a kínai felet. A találkozó eredményeképp drasztikusan visszaestek a Kínának tulajdonított kibertámadások az Egyesült Államokban.

A kiberdiplomácia fogalma gyakran keveredik a digitális diplomácia fogalmával, holott ez utóbbi a digitális eszközök és szolgáltatások használatát jelenti a diplomáciai kapcsolatok fenntartása során. A Twitter szolgáltatás például igen gyakran jelent hivatkozási alapot napjainkban, elég csak Donald Trump amerikai elnök online tevékenységére gondolni. Fontosságát jelzi, hogy a diplomáciai szakzsargonban elterjedt a „Twiplomacy" kifejezés, utalva a néhány száz karakterben nyilvánosságra hozott állami üzenetek fontosságára. A kommunikáció felgyorsulásával ezek a digitális eszközök is fontosak, azonban a kommunikáció stílusa miatt a hagyományos diplomáciai kapcsolattartás szabályai gyakran sérülnek, amiatt pedig újszerűen kell hozzáállni az évszázadok óta létező diplomáciai protokollhoz. Mivel aránylag új jelenségről van szó, ezek a szabályok kialakulóban vannak, még a fogalmi rendszer sem egyértelmű. Manor cikkében áttekintette a digitális diplomácia szakirodalomban elterjedt definícióit, majd arra jutott, hogy ezek közül egyik sem fedi le teljesen a gyakorlati jelenséget, így ő a „diplomáciai digitalizálódását" javasolja fogalomként használni, mely bővebb a Facebook, a Twitter, az okostelefon és egyéb, a hétköznapokban elterjedt eszközök használatánál az állami kommunikációban. Ez megfogalmazása szerint

„*olyan kifejezés, mely a digitális technológiák normatív és időleges hatását helyezi a középpontba. Ebben benne van az a hosszú távú folyamat is, melynek hatása messze túllépi az innovatív technológiák hatását.*" (Manor 2017)

Több, mint pusztán imázsépítés a közösségi médiában, mint a Twitter használata a kommunikációban, hiszen egyes tudósok már arról cikkeznek, vajon kitörhet-e egy fegyveres konfliktus egy rosszul sikerült Twitter-bejegyzés miatt.

A kiberdiplomácia tehát az állami kapcsolatokról szól a kibertérben, mégis van egy speciális eleme, amely megkülönbözteti minden más diplomáciai ágazattól. A kibertérben ugyanis vannak olyan vállalati szereplők, melyek helyet követelnek maguknak az államközi együttműködésekben, hiszen az általuk működtetett infrastruktúrák globálisan meghatározóak. Az olyan több milliárd felhasználóval rendelkező szereplők, mint a már sokszor emlegetett Facebook, Microsoft vagy Google meghatározó résztvevői a multilaterális kapcsolatoknak, és bár nem szuverén szereplők, hiszen alapvetően amerikai joghatóság alatt állnak, együttműködésük nélkül a kibertér békéje nem megvalósítható. Az együttműködés természetesen a vállalatok érdeke is, hiszen nem egyszer előfordult már, hogy akaratukon kívül részeseivé váltak a geopolitikai folyamatoknak.

A Microsoft a 2017-es WannaCry kártékony kód kampány idején került a figyelem középpontjába, tekintettel arra, hogy az automatikusan terjedő zsarolóvírus, úgynevezett féreg típusú kód a Microsoft Windows rendszerekben megtalálható, EternalBlue nevű sérülékenységet használta ki, amely

legalább 20 éve része volt ezeknek az operációs rendszereknek. Habár a 2017 május végén elindult fertőzést meg lehetett volna előzni a cég által márciusban kiadott javítással, az ezt a hibát kihasználó támadás nem került volna nyilvánosságra, ha az amerikai titkosszolgálat, az NSA azt nem fedezi fel évekkel korábban, nem használja fedett műveletekben és nem kezeli olyan hanyagul, hogy utána a Shadow Broker hackercsoport azt meg tudja szerezni. Mivel a Microsoft már annak az évnek az elején tisztában volt azzal, hogy ez a sebezhetőség komoly károkat okozhat a későbbiekben, és úgy általában komoly üzleti kockázatot látott abban, hogy állami szereplők az általuk készített szoftverek sebezhetőségeire építik műveleteiket anélkül, hogy ezekre a hibákra figyelmeztetnék a gyártókat, előálltak a Digitális Genfi Egyezmény (Digital Geneva Convention) című javaslatukkal, ezzel aktív részesei lettek a kiberdiplomáciai tevékenységnek, javaslatuk gyakran hivatkozott kiadvány lett a nemzetközi diplomáciai körökben.

A Digitális Genfi Egyezmény az alábbiakat javasolja az államok felé, kifejezve a digitális ipar szereplőinek elvárásait a termékeikkel és szolgáltatásaikkal kapcsolatos felelős viselkedéssel kapcsolatban.

- Ne támadjanak olyan rendszerek ellen, amelyek megsemmisítése hátrányosan befolyásolná a biztonságot (azaz a létfontosságú infrastruktúrákat, például a kórházakat, energiaszolgáltató vállalatokat).
- Ne támadjanak olyan rendszerek ellen, amelyek megsemmisítése károsíthatja a globális gazdaságot (például a pénzügyi tranzakciók sértetlensége), vagy egyéb jelentős globális zavarokat okozhatnak (például felhőalapú szolgáltatások támadása esetén).
- Tartsák távol magukat az újságírók és a választási folyamatokban részt vevő magánszemélyek személyes fiókjainak vagy személyes adatainak meghackelésétől.
- Ne használjanak információs és kommunikációs technológiát a magánvállalkozások szellemi tulajdonának ellopásához, ideértve a kereskedelmi titkokat vagy más bizalmas üzleti információkat azért, hogy más vállalatoknak vagy kereskedelmi szektoroknak versenyelőnyt szerezzenek.
- Ne illesszenek be vagy ne követeljenek meg „backdoorokat”, azaz hátsó kapukat tömegpiaci kereskedelmi technológiai termékekben.
- Értsenek egyet a sérülékenységek megszerzésével, megtartásával, biztosításával, használatával és jelentésével kapcsolatos egyértelmű szabályozással, ami tükrözi azt az erőteljes követelményt, hogy a megtalált sebezhetőségeket jelenteniük kell a gyártók felé – a tömegpiaci termékek és szolgáltatások terén.
- Tanúsítsanak önmérsékletet a kiberfegyverek kifejlesztésének terén, biztosítsák azt, hogy ezek korlátozottak, pontosak és nem újrahasználhatók legyenek. Az államoknak azt is biztosítaniuk kell, hogy a fegyvereiket biztonságos környezetben, megfelelő kontrollok mellett kezelik.
- Elfogadják a kiberfegyverek elterjedésének korlátozását. A kormányok nem terjeszthetnek, és nem engedélyezhetik mások számára sem a számítógépes fegyverek terjesztését, egyben hírszerzési, bűnüldözési eszközöket és pénzügyi szankciókat alkalmaznak azok ellen, akik ennek a követelménynek nem tesznek eleget.
- A kibertámadó műveletekben való részvételt korlátozzák, a civil infrastruktúrák és létesítmények tömeges károsodásának elkerülése érdekében.
- Részt vesznek a magánszektor azon erőfeszítéseiben, melyek a kibertámadások észleléshez, korlátozásához, a reagáláshoz és helyreállításhoz szükségesek. Kifejezetten rendelkezésre bocsájtják a válaszadáshoz és helyreállításhoz szükséges alapvető képességeiket vagy eljárásaikat, beleértve az eseménykezelő központokkal (Computer Emergency Response Team, CERT) való együttműködést. A magánszektor válaszába és a helyreállításban való részvételbe való beavatkozás hasonló lenne a katonai kórházak orvosi személyzetének támadásához. (Microsoft 2018)

A kiberdiplomáciai szakértelem jellemzően az egyes országok külügyminisztériumában található. Nincs ez másképp Magyarországon sem, a tanulmány írása idején hatályos 19/2016. (VIII. 31.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról szerint a minisztérium Erőforrás-diplomácia és Új Típusú Biztonsági Kihívások Főosztályon működő Kibertér Koordinátor feladata ennek a szerepkörnek a betöltése. Tiirmaa-Klaar hangsúlyozza, hogy ez a szerep jelentősen különbözik más külügyi pozícióktól, hiszen

„*az infokommunikációs technológiák átfogó ismerete szükséges hozzá, így át kell látni a fejlesztési folyamatokat, a számítógép- és hálózati biztonságot, az internetirányítást, a nemzetközi biztonságpolitikát, a kiberbűnözést, a kibertérben történő hírszerzést stb. Ezen tárgyak jó részét nem tanítják a diplomáciai akadémiákon vagy a külkapcsolati iskolákban. Eközben viszont a diplomatáknak gyorsan meg kell tanulniuk kibernyelven beszélni, mivel a téma gyorsan fejlődik.*" (Tiirmaa-Klaar 2013)

2014-ben kelt cikkében a kiberdiplomácia főbb kihívásai között a nemzetközi biztonság és bizalomerősítést a kibertérben, a kiberbűnözés elleni küzdelmet, az emberi jogok védelmét a kibertérben és az internetirányítás kérdését említi meg. Bár ezek a prioritások folyamatosan fejlődnek, az elfogadásra váró amerikai kiberdiplomáciai törvény (Cyber Diplomacy Act of 2017) is hasonló fókuszterületeket fogalmaz meg az USA kiberkapcsolataival összefüggésben.

1.7. Esettanulmány: a NotPetya kampány

A kiberteret érintő kártékony cselekmények sora végtelen hosszú, de vannak olyan események, amelyek fordulópontot, egyben hivatkozási alapot jelentenek a kutatóknak. A 2007-es Észtország elleni támadás, a Stuxnet kártékony kód bevetése, Edward Snowden információszivárogtatása mind olyan történések voltak, amikor át kellett értékelni a kibertérről alkotott véleményünket. Jelen tanulmány szempontjából a NotPetya kártékony kód kampány az a fordulópont, mely megmagyarázza a nemzetközi jog és a nemzetközi kapcsolatok fontosságát a kibertéri események kapcsán. Ez az incidens ugyanis olyan kritikus pontokra mutatott rá a külkapcsolatok területén, amelyek a gyakorlatban is megmutatták, hogy a Tallinni Kézikönyv létrehozása vagy a Digitális Genfi Egyezmény megalkotására tett javaslat valóban szükséges volt egyes országok nemzetközi normákat szabadon értelmező gyakorlata miatt.

A *Wired* magazin összefoglalója alapján a NotPetya kampány 2017. június 27-én, késő délután tört ki, az ukrán alkotmány ünnepe előtti munkanap utolsó munkaóráiban. Már az első fertőzések időpontjai találgatásra adtak okot, ugyanis az ukrán köztársaság jeles ünnepét megválasztani a támadás kezdetének jelzésértékű üzenet. Igaz, ekkor még valószínűsíthető volt, hogy az időzítésnél szempont volt az is, hogy az informatikai üzemeltetők nagy része szabadságon lesz, tehát a védelem alacsonyabb erőforrásokkal fog működni. Bár a fertőzések más országokban is hamar megjelentek, a legtöbb fertőzött gépet Ukrajnából jelentették, így gyaníthatóan a célpont Ukrajna mint állam volt, nem pedig egyes vállalatok. A többi országban, így többek között Németországban, Franciaországban, Olaszországban, Lengyelországban és az Egyesült Államokban csak járulékos áldozatok voltak. Tovább erősíti ezt a teóriát az is, hogy ugyanaznap egy gépjárműbe rejtett robbanóeszköz ölt meg egy különleges erőknél szolgáló munkatársat Kijevben. (Greenberg 2017)

A kártékony kód a zsarolóvírusok jellegzetességeit viselte magán, így a fertőzés után titkosította a merevlemezt, a gép elindulása után pedig 300 dollárnyi bitcoint kért a feloldásért cserébe. Hamar kiderült azonban, hogy a kapcsolattartásra megadott e-mail cím nem él, tehát esély sincsen az elvesztett adatok visszaszerzésére. Amennyiben anyagi motivációjú lett volna a támadás, mint a NotPetyát egy hónappal megelőző WannaCry esetén, akkor a támadó elérhető maradt volna, és biztosította

volna a váltságdíjért cserébe az adatok visszaszolgáltatását, hiszen a hasonló bűncselekmények tanulsága alapján az áldozat csak akkor fizet, ha van esélye a dekódoló kulcs megszerzésére, tehát a bűnelkövetőnek érdeke az áldozat megfelelő kiszolgálása. A zsarolóvírus jelleget erősített az első órákban az is, hogy a kód hasonlóságot mutatott a jól ismert Petya zsarolóvírussal, de hamar kiderítették, hogy ez szándékos maszkírozás volt, így terjedt el a NotPetya, azaz a Nem Petya elnevezés a szakmában.

Hatásmechanizmusát tekintve a kártékony kód a számítógép master boot record-ját, tehát az operációs rendszer betöltéséért felelős merevlemez-szegmenst fertőzte meg, a gép indítását követően pedig elkezdte titkosítani a fájlrendszert. Ha ez sikerült neki, a képernyőn feltüntette a zsarolóvírusok által használatos szöveget, jelezte, hogy mennyi pénzt kér, és mi a kommunikáció módja. Mielőtt a gépet használhatatlanná tette volna, megpróbált elterjedni azon a hálózaton, amin a fertőzött gép volt. Ehhez egyrészt használta az EternalBlue sebezhetőséget, azaz a WannaCry-nál megismert módon féregjelleggel terjedt a korábban nem frissített gépekre, de a fertőzött gép memóriájából is összegyűjtötte az ott levő adminisztrátori jelszavakat, amelyek szintén hozzáférést adhattak neki más hálózati gépekhez. Az első fertőzések a feltételezések szerint az M.E. Doc nevű szoftver frissítési mechanizmusán keresztül érkeztek. Ez a szoftver az egyik hivatalosan jóváhagyott adóbevallási program, így az ukrán vállalatok jelentős részénél fut. Ez a program jelezte, hogy frissíteni kell, majd miután a felhasználó engedélyezte a javítások telepítését, elkezdődött a fertőzés. Arról nincsen információ, hogyan tudták a M.E. Doc frissítési eljárását befolyásolni, a távoli feltöréstől kezdve a frissítőszerverhez való közvetlen, fizikai hozzáférésig számos lehetséges megoldás szóba kerülhet. Az biztosnak tűnik, hogy a támadó adminisztrátori jogosultságot szervezett a M.E. Doc vállalat egyik szerverén, ez tette lehetővé számára azt, hogy a frissítési mechanizmusba is beavatkozzon. A Talos kiberbiztonsági cég nyomozása szerint már 2017 április 24-én olyan frissítés ment a felhasználókhoz, ami hátsó kaput tartalmazott, tehát elvileg lehetővé tette a támadás kivitelezését. A támadók tehát hónapokkal korábban elkezdtek felkészülni az akcióra. Szemben a WannaCry-jal, itt nem találtak olyan kapcsolót, úgynevezett „kill switch”-et, amely lehetővé tette volna a fertőzés gyors leállítását. A támadó célja egyértelműen a minél nagyobb, földrajzilag a leginkább lokalizált pusztítás volt. (Maynor–Nikolic–Olney–Younan 2017)

Végül több ezer ukrán vállalatot ért el az incidens. Az áldozatok között megtalálhatók bizonyos ukrán kritikus infrastruktúrák, így többek között ukrán bankok, a kijevi Borispol repülőtér, az energetikai cégek közül pedig a Kyivenergo és az Ukrenergo. De több külföldi cég is jelentett fertőzést, így az amerikai gyógyászati vállalat, a Merck, az orosz Rosznyeft, illetve a magyar OTP Bank ukrajnai pénzkiadó automatáiról is elterjedtek olyan képek a világhálón, amelyek NotPetya fertőzést mutatnak. A legnagyobb publicitást az A.P. Moller – Maersk cégnél történt pusztítás kapta. A cég a világ egyik legnagyobb logisztikai vállalata, a Forbes Global 2000 céglistája szerint a világ 558. legnagyobb konglomerátuma. A NotPetya fertőzés a beszámolók szerint két napra ellehetetlenített a cég működését, a teherszállító hajók berakodását világszerte manuálisan kellett irányítani, számítógép helyett a papírra és a ceruzára hagyatkozva. Ez meg is látszódott a dán vállalat bevételén, negyedéves beszámolójukban azt becsülték, hogy 200-300 millió dollár közötti kárt okozott nekik ez a kétnapos leállás. (A.P. Moller – Maersk 2017)

A NotPetya kártékony kód az első olyan kibertéri incidens, amely békeidőben történő koordinált támadásnak tűnik egy szuverén állam ellen, támadva annak kritikus infrastruktúráit, civil létesítményeit, járulékos kárt okozva más országokban működő civil vállalatoknak is. Célja egyértelműen a pusztítás volt. A kártékony kód által felhasznált eszközök korábban ismertek voltak, hiszen sem a hálózaton belüli terjedéshez kihasznált sebezhetőség, sem a kiemelt jogosultságú felhasználók hitelesítési adataihoz való hozzáférést megvalósító szoftver nem okozott meglepetést a szakembereknek. A támadási taktika azonban merőben új volt, érezhetően alapos műveleti tervezés előzte meg, hiszen a terjesztéshez választott M.E. Doc szoftver Ukrajna határain túl ismeretlen, csak megfelelő hírszerzési háttérrel lehetett biztosan tudni, hogy ez a terjedési vektor ennyire hatékony lehet egy földrajzilag fókuszált kibercsapás végrehajtására. Külön ki kell emelni azt a lélektani csavart a támadásban, amivel az áldozatokkal elhitették, hogy a kártékony kód számára hátsó kaput nyitó M.E. Doc verziót fel kell

telepíteni. Mind a végfelhasználók, mind az informatikai üzemeltetők számára ugyanis évtizedek óta tudatosítják a kiberbiztonsági szakemberek, hogy a szoftverekből a legfrissebb változatot kell használni, tehát ha egy szoftverfrissítés rendelkezésre áll, akkor azt a lehető leghamarabb telepíteni kell. A támadó tehát erre az alapvetésre építette fel a terjesztést, bízva abban, hogy a felhasználók külön kérdés nélkül, a lehető leghamarabb telepítenek bármit, ami frissítésnek tűnik, így a frissítőszerver megtámadása és terjesztési pontnak való használata briliáns választás.

Az államok szempontjából az eldöntendő kérdés az, hogy ha adott egy kiberbiztonsági incidens, ami szakmai szempontból egy kiberháborús cselekménynek látszódik, melynek során egy fejlett kiberfegyvert vetettek be egy olyan országban, mely már korábban is szenvedett ilyen célzott támadásoktól, tehát egy másik ország fegyverkísérleteinek rendszeres célpontja, akkor vajon ki lehet-e mondani, hogy ez az incidens ténylegesen támadásnak minősíthető-e a szó nemzetközi jogi értelmében, illetve élhetnek-e az attribúció eszközével, megnevezhetnek-e egy országot támadóként. Másrészt kérdés az is, hogy a nemzetközi diplomácia felkészült-e arra, hogy egy ilyen nyilatkozat után a hagyományos diplomáciai eszközökkel kezelni tudják a megnevezett ország ellenintézkedéseit. Végül kérdés az is, hogy a megnevezett támadó országra lehet-e olyan nyomást gyakorolni, melynek eredményeképp az csökkenti vagy beszünteti a kibertérben történő ellenséges cselekményeit.

Schmitt és Biller a NotPetya támadás után pár héttel megvizsgálta, hogy az incidens hogyan viszonyul a nemzetközi jog előírásaihoz. Első megjegyzésük az volt, hogy a kártékony kód nem okozott sérülést vagy halált a beszámolók szerint. Jelen tanulmány szerzői ehhez annyit tesznek hozzá, hogy bár közvetlen halálesetekről sem a NotPetya, sem a WannaCry esetén nem olvashattunk, nem kizárt, hogy egyes egészségügyi létesítmények nem működő elektronikus információs rendszerei, különösen a WannaCry esetén a brit egészségügyi rendszert érő befolyás miatt, közvetve hozzájárulhattak olyan halálesetekhez, amelyek megelőzhetők lehettek volna, ha a beteget időben tudják a megfelelő ellátáshoz juttatni. Schmitt és Biller a számonkérhetőséget az attribúcióhoz köti, azaz a fő kérdés az, hogy a támadás mögött egy ország fegyveres erői, hírszerző ügynökségei álltak, vagy nem állami szereplő esetén az utasításokat állami szereplő adta-e. Feltételezve, hogy ez történt, három állami kötelezettség megsértését lehet feltételezni. Ezek a szuverenitás tiszteletben tartása, a be nem avatkozás elve és az erő alkalmazásának tilalma.

A szuverenitás a szakértők szerint sérült a NotPetya támadás alatt, ennek ugyanis két feltétele van. Egyrészt a területi integritás megsértése, amely a kibertérben úgy képzelhető el, hogy egy támadás fizikai károkat vagy személyi sérülést, esetleg halálesetet okoz. Kiterjesztő értelmezésben, amennyiben egy kiberinfrastruktúra hosszabb időre elérhetetlenné válik, a szerzők véleménye szerint szintén megfogalmazható a területi integritás megsértése. Mivel a NotPetya túlmutatott egy átlagos elosztott túlterheléses támadás hatásain, konkrétan kulcsfontosságú adatok elvesztésével járt, illetve kritikus számítógépes rendszerek helyett kellett új gépeket üzembe állítani, ez felfogható a fizikai létesítmények sérüléseként. A másik feltétel az alapvető kormányzati tevékenységek megzavarása lenne, ez azonban a NotPetya esetében nem történt meg. Habár a pénzintézeti tevékenységeket lehetővé tevő informatikai rendszerek sérültek, ezek nem alapvető kormányzati funkcionalitást támogatnak, tehát a szuverenitás megsértésének ez a feltétele nem állt fenn.

A be nem avatkozás elvének megsértéséhez kényszerítő erejű tevékenységek társulnak, melyeket egy állam fejt ki egy másik állammal szemben a politikai, gazdasági, társadalmi és kulturális berendezkedés megváltoztatása, illetve a külpolitika befolyásolása céljából. Schmitt és Biller nem látta bizonyítottnak, hogy a NotPetya kártékony kód alkalmas lett volna ezen célok megvalósítására, tekintettel arra, hogy célja a pusztítás és nem a befolyásolás volt. Amennyiben a kiberfegyver valóban zsarolóvírus lett volna, aminek az első pillantásra látszódott, elvileg lehetőség lett volna a kényszerítésre, hiszen a zsarolás lényege valamilyen döntés kicsikarása a másik féltől.

Az erők használatának elve békeidőben azt jelenti, hogy egy állam ENSZ-felhatalmazás vagy mandátum nélkül hajt végre olyan erőszakos tevékenységet, amely nem minősül önvédelemnek vagy kollektív védelemnek. A kibertevékenységek jellemzően kis hatással vannak a fizikai környezetre,

így nehéz olyan támadást elképzelni, mely eléri az erő használatának nem jogosult szintjét. A kiberinfrastruktúra hosszú távú kiesése azért, mert az azt alkotó számítógépek vagy hálózati eszközök elérhetetlenné váltak egy NotPetyához hasonló kártékony kód miatt, viszont már minősíthető lenne jogosulatlan erőhasználatként. A szerzők véleménye szerint a gazdasági destabilizáció is ebbe a körbe tartozhat. Az ukrán kormány véleménye szerint a kibertámadás elérte ezt a szintet, a nemzetközi gyakorlat azonban 2017 közepén még nem adott egyértelmű választ arra, hol a határ.

A nemzetközi humanitárius jog akkor lenne érvényes ebben az esetben, ha két állam, azaz Ukrajna és tegyük fel, Oroszország között nemzetközi fegyveres konfliktus állna fenn. Ennek feltétele, hogy egy ország megszállás alatt tartja egy másik ország területét vagy egy nem állami csoportot támogat, mely ellenséges tevékenységet fejt ki a másik ország ellen. Mivel a Krím-félsziget és a kelet-ukrajnai felkelőcsoportok támogatása miatt a szerzők meglátása szerint joggal feltételezhető, hogy a két állam között fegyveres konfliktus áll fenn, a NotPetya használatát a nemzetközi humanitárius jog alapján is vizsgálni kell, dacára annak, hogy az ENSZ GGE-ben erről nincsen teljeskörű egyetértés. Ennek a kártékony kódnak a minősítését a Tallinni Kézikönyv alapján érdemes megvizsgálni, mely alapján támadásnak minősül az ilyen kiberfegyverek használata még akkor is, ha közvetlen kárt nem okoznak a kiberinfrastruktúrában, csak közvetve fejtik ki hatásukat, illetve egyes szakértők szerint az infrastruktúra elérhetetlenségének elérése is a támadás körébe tartozik.

A NotPetya célpontjai között szerepelt a kijevi repülőtér, a csernobili erőmű és az ukrán egészségügyi rendszer is. Amennyiben feltételezhető, hogy ez a támadó szándékával megegyezően történt, nem a kártékony kód koordinálhatatlan terjedése miatt valósult meg a fertőzés, ez támadásnak minősíthető a szerzők álláspontja szerint. Habár egyes megtámadott létesítmények minősíthetők lennének kettős felhasználásúnak, például a repülőtér, a legtöbb kiberinfrastruktúra elem egyértelműen civil, nem szolgál katonai célokat, így akár a háborús bűncselekmény kategóriájába is tartozhatna a cselekmény. Ráadásul a kiberfegyver hatása túlmutatott Ukrajnán, harmadik országokban is éreztette hatását, így azok semlegességét is megsértette a támadó. (Schmitt–Biller 2017)

Mindez természetesen csak a kutatók tudományos gondolatmenete, egy kibertámadás kapcsán háborús bűncselekményeket emlegetni komoly diplomáciai hatásokkal járhat, ha azt egy hivatalban levő politikus teszi. A NotPetya viszont különleges abban a tekintetben, hogy a kutatói álláspontok mellett megjelentek az olyan kommentárok, majd politikai állásfoglalások, amelyeket az elméleti gondolatmenetnél komolyabban kellett venni. Először a NATO Kooperatív Kibervédelmi Kiválósági Központjának kutatói elemezték a kialakult helyzetet. Az idézett Michael Schmitt is ehhez a tudományos körhöz tartozik, a korábban idézett elemzése azonban nem a szervezet honlapján jelent meg, így Blumbergs, Minárik, van der Meij és Lindström cikkét a világsajtó már mint a NATO álláspontját tette közzé. Így különös súly van annak, amit Minárik mondott: „Amennyiben a művelet összefügg egy nemzetközi fegyveres konfliktussal, akkor a fegyveres konfliktusokra vonatkozó jogszabályok vonatkoznak rá.” Korábban a NATO CCD COE kommentárjai nem járták be a világsajtót ilyen kényes ügyben, így érzékelni lehetett, hogy a NotPetya súlya lényegesen nagyobb, mint bármilyen másik korábbi esetnek. (Blumbergs–Minárik–van der Meij–Lindström 2017)

Az igazán nagy áttörést 2018 februárjában érte el az ügy, amikor 7 ország, az Egyesült Államok, Nagy-Britannia, Dánia, Litvánia, Észtország, Kanada és Ausztrália közösen ítélték el Oroszországot a NotPetya-támadás miatt, ezt pedig hivatalosan is támogatta Új-Zéland, Norvégia, Lettország, Svédország és Finnország. Korábban soha nem történt meg, hogy több ország közösen élt volna az attribúció eszközével, azaz egyöntetűen mutattak volna rá a támadóra. Az attribúció mindig politikai döntés, amelyet támogathat műszaki vagy hírszerzési bizonyíték, de politikai akarat nélkül ezek nem sokat érnek. Tobias Feakin, Ausztrália kiberügyekben felelős nagykövete foglalta össze kiválóan, miért volt fontos lépés ez a közös kiállás, és mit jelent ez a támadókra nézve: „Amit teszünk, az az, hogy tovább érleljük hozzáállásunkat annak érdekében, hogy a következmények még jobban érezhetők legyenek a jövőben. Tehát az elrettentés egyik kulcsfontosságú jele más országok számára az, hogy tiszta, egyértelmű és hiteles üzenetet küldünk a támadóknak arról, hogy következményei lesznek viselkedésüknek.” (Stilgherrian 2018)

1.8. Irodalomjegyzék

- 1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- A.P. MOLLER – MAERSK (2017): *A.P. Moller - Maersk improves underlying profit and grows revenue in first half of the year*. Forrás: https://www.marineinsight.com/shipping-news/maersk-improves-underlying-profit-grows-revenue-first-half-year/. (Letöltés ideje: 2020. 07. 15.)
- BARRINHA, André – RENARD Thomas (2017) Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, 3:4–5. 353–36.
- BÁNYÁSZ Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* III. évfolyam II. szám. 21–36.
- BLUMBERGS, Bernhards – MINÁRIK, Tomáš – VAN DER MEIJ, Kris – LINDSTRÖM, Lauri (2017): *NotPetya and WannaCry Call for a Joint Response from International Community*. Forrás: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ (Letöltés ideje: 2018. 07. 17.)
- BÓDI Stefánia – KÁDÁR Pál – PETRUSKA Ferenc (2014): *Jogi alapismeretek honvéd tisztjelölteknek.* Nemzeti Közszolgálati Egyetem
- BUCHAN, Russell (2016): *The International Legal Regulation of State-Sponsored Cyber Espionage.* In: Anna-Maria Osula, Henry Rõigas (Eds.) International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn. 65–86.
- CALATAYUD, Jose Miguel (2017): *Locked Shields: The world's largest cyber-war game*. Forrás: https://www.aljazeera.com/indepth/features/2017/05/locked-shields-world-largest-cyber-war-game-170527102554714.html (Letöltés ideje: 2018. 07. 12.)
- CSERNY Ákos – TÉGLÁSI András (2014): *Jogforrástan: nemzetközi és uniós jog.* Nemzeti Közszolgálati Egyetem
- DÁN Károly (2018): *Promoting confidence in Cyberspace: The workings of the OSCE*. Elhangzott: Nemzeti Közszolgálati Egyetem, 2018. 03. 12.
- ENSZ (1945): *Az Egyesült Nemzetek Alapokmánya*. Forrás: http://www.grotius.hu/doc/pub/HBJFWJ/az%20ensz%20alapokm%C3%A1nya.pdf. (Letöltés ideje: 2018. 07. 11.)
- FERENCZY Gábor Zoltán (2007): *Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása*. Zrínyi Miklós Nemzetvédelmi Egyetem.
- GOODIN, Dan (2017): *"Suspicious" event routes traffic for big-name sites through Russia.* Forrás: https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/ (Letöltve: 2018. 07. 14.)
- GREENBERG, Andy (2017): *Petya Ransomware Epidemic May Be Spillover From Cyberwar*. Forrás: https://www.wired.com/story/petya-ransomware-ukraine/ (Letöltés ideje: 2018. 07. 16.)
- ITU (2005): *Report of the Working Group on Internet Governance*. Forrás: http://www.wgig.org/docs/WGIGREPORT.pdf. (Letöltés ideje: 2018. 07. 05.)
- ITU (2014): *On the road to implement the Connect 2020 Agenda*. Forrás: https://www.itu.int/en/connect2020/Documents/pp14-connect2020-commitments.pdf. (Letöltés ideje: 2018. 07. 05.)
- ITU (2018): *ITU Cybersecurity Activities*. Forrás: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx. (Letöltés ideje: 2018. 07. 05.)
- IZSA Jenő (2009): A hírszerzés céljáról és rendszeréről. *Hadtudomány,* 2009 1–2. szám. 72–83.
- KAJTÁR Gábor (2010): *Az önvédelem jogával kapcsolatos dilemmák a terrorizmus elleni háború korában*. In: Nagy Marianna (szerk.) Ünnepi konferencia az ELTE megalakulásának 375. évfordulója alkalmából Jogi Tanulmányok, 2010. II. kötet. pp. 293-308.
- KORZAK, Elaine (2017): *UN GGE on Cybersecurity: The End of an Era*? Forrás: https://

thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (Letöltés ideje: 2018. 07. 11.)

- KOVÁCS Péter (2010): *A nemzetközi jog fejlesztésének lehetőségei és korlátai a nemzetközi bíróságok joggyakorlatában*. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar.
- LATTMANN Tamás (2013): *A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén*. In Csapó Zsuzsanna (szerk.) Emlékkötet Herczegh Géza születésének 85. évfordulójára: A ius in bello fejlődése és mai problémái. Pécsi Tudományegyetem Állam- és Jogtudományi Kar. 209–220.
- LATTMANN Tamás (2018): *Nemzetközi jogi szabályozás célzott kibertámadások esetén*. Nemzeti Közszolgálati Egyetem (megjelenés alatt).
- LIBICKI, Martin C. (2018): *Drawing Inferences from Cyber Espionage.* In T. Minárik, – R. Jakschis – L. Lindström (Eds.): 2018 10th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn. 109–122.
- MARTIN, Alexander J. (2018): *Russian hackers targeted Ukraine's water supply, security service claims*. Forrás: https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826. (Letöltés ideje: 2018. 07. 12.)
- MANOR, Ilan (2017): *The Digitalization of Diplomacy: Toward Clarification of a Fractured Terminology*. Forrás: https://digdipblog.files.wordpress.com/2017/08/the-digitalization-of-diplomacy-working-paper-number-1.pdf (Letöltés ideje: 2018. 07. 15.)
- MAYNOR, David – NIKOLIC, Aleksandar – OLNEY, Matt – YOUNAN, Yves (2017): *The MeDoc Connection*. Forrás: https://blog.talosintelligence.com/2017/07/the-medoc-connection.html. (Letöltés időpontja: 2018. 07. 16.)
- MAURER, Tim (2011): *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security*. Belfer Center for Science and International Affairs.
- Microsoft (2018): *A Digital Geneva Convention to protect cyberspace*. Forrás: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH. (Letöltés ideje: 2018. 07. 15.)
- Munich Security Conference (2011): *MSC 2011 Summary.* Forrás: https://www.securityconference.de/en/activities/munich-security-conference/munich-security-conference/msc-2011/ (Letöltés ideje: 2018. 07. 10.)
- MUNK Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány*, 2018/1 szám. 113–131.
- NATO (1949): *Az Észak-Atlanti Szerződés*. Forrás: https://www.nato.int/cps/ic/natohq/official_texts_17120.htm?selectedLocale=hu. (Letöltés ideje: 2018. 07. 12.)
- NATO (2014): *Wales Summit Declaration*. Forrás: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (Letöltés ideje: 2018. 07. 10.)
- NATO (2018): *Brussels Summit Declaration*. Forrás: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en (Letöltés ideje: 2018. 07. 13.)
- Nuclear Threat Initiative (2018): *The UN Groups of Governmental Experts (GGE)*. Forrás: http://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/ (Letöltés ideje: 2018. 07. 11.)
- OSULA, Anna-Maria – RÕIGAS, Henry (2016): *Introduction.* In Anna-Maria Osula– Henry Rõigas (Eds.): International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn. 11–22.
- RÁCZ Lajos (2010): *Diplomácia – Katonadiplomácia.* Zrínyi Miklós Nemzetvédelmi Egyetem
- SCHMITT, Michael N. – BILLER, Jeffrey (2017): *The NotPetya Cyber Operation as a Case Study of International Law*. Forrás: https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ (Letöltés ideje: 2018. 07. 16.)

- SCHMITT, Michael N. – VIHUL, Liis (2016): *The Nature of International Law Cyber Norms*. In: Anna-Maria Osula, Henry Rõigas (Eds.) International Cyber Norms, Legal: Policy & Industry Perspectives. NATO CCD COE Publications, Tallinn. 23–48.
- SCHMITT, Michael N. (Szerk) (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
- STILGHERRIAN (2018): *Blaming Russia for NotPetya was coordinated diplomatic action*. Forrás: https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/ (Letöltés ideje: 2018. 07. 17.)
- SUBA Ferenc (2014): *Nemzeti Kiberbiztonsági Stratégia.* In Dobák Imre (szerk.) A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem. 110–115.
- TÁLAS Péter (2016): Avarsói NATO-csúcs legfontosabb döntéseiről. *Nemzet és Biztonság,* 2016/2. szám, pp. 97-101.
- TIIRMAA-KLAAR, Heli (2013): *Cyber Diplomacy: Agenda, Challenges and Mission*. In Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn. 509–532.
- VEENENDAAL, Matthijs – KASKA, Kadri – BRANGETTO, Pascal (2016): *Is NATO Ready to Cross the Rubicon on Cyber Defence?* Forrás: https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf. (Letöltés ideje: 2018. 07. 12.)

2. BÓDI ANTAL – INFORMÁCIÓBIZTONSÁG A KÖZLEKEDÉS MINT LÉTFONTOSSÁGÚ RENDSZERELEM ESETÉN

2.1. Bevezetés

A közlekedés áthatja mindennapjainkat, a közlekedési rendszerek szinte észrevétlenül, magától értetődő módon szolgálják ki a napi helyváltoztatási igényeinket. Természetesnek vesszük, hogy a jelzőlámpák működnek, még ha olykor dugóban is kell állnunk, és egyre természetesebb igényünk, hogy egy közlekedési vagy a közlekedést érintő zavar esetén információt kapjunk a rádión, az autónk navigációs készülékén, az okostelefonon vagy tableten futó alkalmazáson keresztül.

A hagyományos megközelítés szerint a közlekedés egészének mindezekhez a hátteret a forgalomirányítási, forgalmi menedzsment rendszerekhez köthető tevékenység biztosítja, jellegéből adódó hatalmas felelősséget és kockázatot viselve. Ezért is van kiemelkedő jelentősége a tevékenységet támogató rendszereknek, amelyek az igények növekvő szintjéből fakadóan, illetve a rendelkezésre álló fejlett infokommunikációs technológiának köszönhetően a gyakorlatban egyre inkább az intelligens közlekedési alkalmazásokat, ökoszisztémába integrálódó intelligens szenzorrendszerek kialakulását segítik elő. A közlekedés minden szereplője által mérhető adatok együttesen teszik majd lehetővé az optimalizált és biztonságosabb közlekedési rendszerek létrejöttét.

A jelenlegi gyakorlatban nem szükséges részletesen fejtegetni, hogy a közúti forgalomirányítás milyen mértékben hat egy-egy nagyváros mindennapi életére, vagy akár az egész országra kiterjedő hatással bír. A jelenlegi rendszer működési logikájából adódóan kis mértékű, helyi beavatkozások vagy események is képesek globálisan kiterjedő hálózati szintű hatásokat kiváltani, tehát a városi közlekedési rendszerek rendkívül zavarérzékenyek. Nemzetközi tanulmányok szerint a városokban a forgalmi torlódások az éves GDP 3%-ának megfelelő nemzetgazdasági károkat okoznak, ideértve a munkaképes közlekedők kieső produktív idejét, a minden szereplő által elszenvedett stresszhatást, a fölöslegesen elégetett üzemanyagot és az ennek során keletkező káros anyagok környezetterhelését, az infrastruktúra túlzott amortizációját, és még sok egyéb nehezen számszerűsíthető, de nyilvánvalóan további jelentős negatív externália hatást lehetne még felsorolni. Nem véletlen az sem, hogy magára a forgalomirányítási rendszerre nyugodtan tekinthetjük, mint „kritikus infrastruktúrára", mint a közlekedés jelentette létfontosságú rendszerelem meghatározó részére.

2.2. A közlekedés helyzete az európai adattérben

Az Európai Parlament és a Tanács épp ezért olyan hosszú távú irányelveket határozott meg, amelyek célja, hogy a tagállamok összehangolt, innovatív közlekedési technológiák bevezetésével optimalizálják az egész EU közútforgalmát. Ma már ez kiterjed a közlekedés egészére. A legújabb kihívásokat is figyelembe

véve például most folyik a pilóta nélküli rendszerekkel (UAV,[4] drónok) végzett műveletekre vonatkozó szabályokról és eljárásokról szóló (EU) 2019/947 végrehajtási rendelet nemzeti szintű hatályba léptetése, amely új alapokra helyezi majd az ezekkel az eszközökkel való tevékenységek végzését.[5] Ebből is látszik, hogy ami eddig a tudományos-fantasztikus irodalom területén volt csak tapasztalható, arra egyre inkább valós igény és megoldás jelentkezik. Ilyenek lehet a drónok felhasználása pl. az egészségügyben, a mezőgazdaságban vagy akár az ipari és biztonsági megoldásoknál. Elemi erővel megjelenik egy szélesebb kör, elsősorban a hobbi- és rekreációs felhasználók, továbbá a kereskedelmi célú felhasználás, amely EU szabályozási keretek között kerül majd megvalósulásra. Figyelembe kell venni, hogy az UAV-k kontrollálhatatlan felhasználása akár nemzetbiztonsági kockázatot is jelent, így az UAV-k esetében cél kialakítani egy olyan rendszert, hogy a mozgásuk és a felhasználási tevékenységük „látható", kontrollálható legyen a digitális térben, és minden eszközhöz felhasználása során egyértelműen felelős személy legyen rendelhető letagadhatatlan módon. Szükségképpen cél, hogy ez a megoldás, a felelősség megállapításán kívül, növelje a jogkövető magatartást az üzembentartóktól és a távpilóták részéről.

A hagyományos közlekedés megreformálására már szigetszerűen elterjedtek intelligens közlekedési rendszerek, ezek elterjedtebb alkalmazásával – óvatos becslések szerint – legkevesebb 10 százalékkal csökkenthetők lennének a fővárosi/nagyvárosi torlódások, vagyis pl. az autós közlekedés hatékonyságának javításával jelentős megtérüléssel és externália-hatásokkal lehet számolni. Amennyiben a közlekedés egészére kiterjedt, összefüggő ökoszisztémát lehetne ezen intelligens rendszerekből és további rendszerelemekből létrehozni, még ettől is jelentősebb javulást lehetne elérni.

Az elmúlt néhány évben a digitális technológiák jelentősen átalakították gazdaságunkat és társadalmunkat. A Covid-19 pandémia helyzet kezelésénél már teljes természetességgel vettük igénybe az online tér nyújtotta lehetőségeket. A digitalizáció hatása érzékelhető minden ágazatban és az európai polgárok mindennapi életében. Az átalakulás középpontjában az adatok állnak, és ez még csak a kezdet. Az adatvezérelt innováció óriási előnyökkel fog járni a polgárok számára, például a még inkább személyre szabott orvoslás, az újfajta mobilitás, valamint az európai zöld megállapodáshoz való hozzájárulása által.

Egy olyan társadalomban, ahol az egyének egyre növekvő mennyiségű adatot állítanak elő, az adatgyűjtés és az adatfelhasználás módjának elsősorban az egyén érdekeit kell előtérbe helyeznie, összhangban az európai értékekkel, az alapvető jogokkal és a szabályokkal. A polgárok csak akkor fognak megbízni az adatvezérelt innovációban, és csak akkor fogadják el azt, ha meggyőződnek arról, hogy az EU-ban az adatok megosztása során maradéktalanul érvényesülnek a szigorú uniós adatvédelmi szabályok. Ugyanakkor a nem személyes ipari adatok és nyilvános közadatok mennyisége folyamatosan nő Európában, ez pedig az adatok tárolásának és feldolgozásának technológiai változásával együtt a növekedés és az innováció potenciális forrása lesz, amelyet ki kell tudnunk aknázni.

A polgárok számára lehetővé kell tenni, hogy a nem személyes adatokból nyert információk alapján jobb döntéseket hozzanak. Továbbá az adatoknak és az adatokból kinyerhető információknak mindenki számára hozzáférhetőknek kell lenniük. Ez segíteni fogja a társadalmat abban, hogy a lehető legtöbbet hozza ki az innovációból és a versenyből, és biztosítja, hogy mindenki részesüljön a digitális hozadékból, a digitalizáció által elérhető előnyökből. Ennek a digitális Európának a kontinens legjobb tulajdonságait kell tükröznie az egyik oldalról: nyitottságot, tisztességességet, sokszínűséget, demokratikusságot és magabiztosságot. Ahhoz, hogy az ehhez szükséges társadalmi bizalom is kialakuljon, garantálni kell a digitális adatvagyon megvédhetőségét, információbiztonságát és a visszaélések kiszűrését. E törekvés megvalósítása érdekében az EU építhet az adatvédelem, az alapvető jogok és a biztonság terén meglévő szilárd jogi keretére, belső piacára és változatos ipari háttérrel rendelkező, versenyképes vállalkozásaira. Ahhoz, hogy az EU átvegye a vezető és kezdeményező szerepet az adatgazdaságban, most kell cselekednie, számos kérdést EU-szinten összehangoltabb mó-

[4] UAV a szakmai sajtóban Unmanned Aerial Vehicles, ember nélküli légi járművek

[5] Az Országgyűlés 2020. december 16-i ülésnapján fogadta el a 2020. évi CLXXIX. törvényt a pilóta nélküli légijárművek üzemelésével összefüggő egyes törvények módosításáról

don kell kezelnie, a hálózati összekapcsoltságtól az adatok feldolgozásán és tárolásán át a számítási teljesítményig és kifejezetten a kiberbiztonságig. Emellett javítania kell az adatkezelésre vonatkozó irányítási struktúráit, és növelnie kell a felhasználásra és a további felhasználásra rendelkezésre álló minőségi adatok állományait.

Az EU-adatstratégia[6] egyidejűleg került előterjesztésre az *Európa digitális jövőjének megtervezése* című bizottsági közleménnyel és a mesterséges intelligenciáról szóló fehér könyvvel, amely bemutatja, hogyan fogja támogatni és előmozdítania a Bizottság a mesterséges intelligencia fejlesztését és elterjedését EU-szerte. E stratégia alapján a Bizottság átfogó konzultációt indított azokkal a jövőbeli konkrét intézkedésekkel kapcsolatban, amelyek azt a célt szolgálják, hogy az EU az adatagilis gazdaság élvonalában maradjon, miközben tiszteletben tartja és előmozdítja azokat az alapvető értékeket, amelyekre az európai társadalmak épülnek.

Növekvő adatmennyiség és technológiai változás következtében a világon előállított adatok mennyisége gyorsan nő, a 2018. évi 33 zettabájtról[7] 2025-re várhatóan 175 zettabájtra fog nőni. Minden új adathullám óriási potenciális lehetőséget jelent az EU számára, hogy világelsővé váljon ezen a területen. Az elkövetkező 5 év során az adatok tárolásának és feldolgozásának módja drámaian meg fog változni. Napjainkban az adatfeldolgozások és adatelemzések 80%-a az adatközpontokban és központi informatikai berendezésekben történik, és csak a 20%-a az intelligens összekapcsolt objektumokban, például autókban, háztartási készülékekben vagy robotokban, valamint a felhasználóhoz közeli informatikai berendezésekben („edge computing”, azaz pereminformatikai alkalmazások). 2025-re ezek az arányok valószínűleg meg fognak fordulni. A gazdasági, a fenntarthatósági előnyökön és a pandémiahelyzeten túl ez a fejlődés további lehetőségeket biztosít a vállalkozásoknak, hogy olyan eszközöket fejlesszenek ki az adatelőállítók számára, amelyekkel növelhetik a saját adataik feletti ellenőrzést.

Az adatok jelentősége a gazdaság és a társadalom szempontjából jelentős átalakulást fog indítani a társadalmunkban. Meg fognak változni a termelési és fogyasztási szokásaink, és általában az életmódunk. Az előnyök életünk minden területén érezhetők lesznek, a tudatosabb energiafogyasztástól a termékek, anyagok és élelmiszerek nyomonkövethetőségén át az egészségesebb életig és a jobb egészségügyi ellátásig. Ebből a sorból nem maradhat ki a közlekedés nyomonkövethetősége sem.

Az adatok a gazdaságfejlesztés éltető elemét jelentik: számos új termék és szolgáltatás alapját képezik, mivel a gazdaság valamennyi ágazatában növelik a termelékenységet és az erőforrás-hatékonyságot, továbbá személyre szabottabb termékeket és szolgáltatásokat, valamint jobb szakpolitikai döntéshozatalt és korszerűsített kormányzati szolgáltatásokat tesznek majd lehetővé. Az adatok rendelkezésre állása elengedhetetlen a mesterségesintelligencia-rendszerek tanításához és felhasználásához. A termékek és szolgáltatások a mintafelismerésről és a tudásgenerálásról gyors ütemben térnek át egyre kifinomultabb előrejelzési technikákra, és így jobb, hatékonyabb és gyorsabb döntések születnek.

Az adatok az olyan nagy átalakító hatású gyakorlatok széles körű alkalmazását is elő fogják segíteni, mint pl. a digitális ikrek használata a gyártás vagy akár a kiberbiztonsági vizsgálatok során. Digitális ikrek létrehozása során fizikai termék, folyamat vagy rendszer virtuális mását hozzák létre. A digitális másolat például adatelemzés alapján előre jelezheti, hogy egy gép mikor fog meghibásodni, ami megelőző karbantartás révén lehetővé teszi a termelékenység növelését, a közlekedésben lehetővé fogja tenni a baleseti kockázatok időbeli kiszűrhetőségét.

Ezenkívül a társadalmi, az éghajlattal és a környezettel kapcsolatos kihívások kezeléséhez, az egészségesebb, virágzóbb és fenntarthatóbb társadalmak létrehozásához is elengedhetetlen, hogy több adat álljon rendelkezésre és javuljon az adatok felhasználásának módja.

Ugyanakkor az IKT-ágazat jelenlegi környezeti lábnyoma a becslések szerint a világ teljes villamosenergia-felhasználásának 5–9%-át és az összes kibocsátás több mint 2%-át teszi ki, ami nagyrészt

6 Európai adatstratégia COM(2020) 66

7 1 zettabyte (ZB) 10^{21}byte.

az adatközpontok működésének, a *felhőszolgáltatás*ok nyújtásának és az összekapcsoltságnak tudható be. Az „Európa digitális jövőjének megtervezése" című uniós digitális stratégia zöld átalakítási intézkedéseket javasol az IKT-ágazat számára. Az adathasznosítás kiterjesztésében és a másodlagos adathasznosításban éppen ezért óriási tartalékok és lehetőségek vannak.

Jelenleg a világ adatainak nagy részét néhány technológiai nagyvállalat birtokolja, és kiszolgáltatott helyzeteket eredményezhet, amikor egy-egy adat elérését a létrejövő természetes monopóliumok akadályozzák. Ez visszafoghatja az adatvezérelt vállalkozások megjelenését, növekedését és innovációját az EU-ban, ugyanakkor számos lehetőség adott ezek kiküszöbölésére. A jövő adatainak nagy része ipari és szakmai alkalmazásokból, közérdekű szakterületekről vagy a dolgok internetével kapcsolatos alkalmazásokból fog származni a mindennapi életben, amely területeken az EU erős. Lehetőségeket teremt továbbá a technológiai változás is: új perspektívák nyílnak az európai vállalkozások számára például a peremhálózati felhő, a biztonság szempontjából kritikus alkalmazások digitális megoldásai, valamint a kvantuminformatika terén. Ezek a tendenciák rámutatnak, hogy a ma győztesei nem feltétlenül lesznek a holnap győztesei. Az adatgazdaságban azonban most dől el, hogy mi jelenti majd a következő évtizedek versenyképességének forrását. Az EU-nak – és benne Magyarországnak – ezért most kell cselekednie. Az EU-nak megvan a lehetősége arra, hogy sikeres legyen az adatagilis gazdaságban. Rendelkezünk számos technológiával, know-how-val és magasan képzett munkaerővel. Az olyan versenytársak azonban, mint Kína és az Egyesült Államok, már most gyors innovációt folytatnak ezen a területen, és az adathozzáféréssel és adatfelhasználással kapcsolatos elképzeléseiket az egész világra kivetítik és hasznosítják. Az Egyesült Államokban az adattér megszervezése a magánszektorra van bízva, és jelentős koncentrációs hatás érvényesül. Kínában a kormányzati felügyelet mellett technológiai nagyvállalatok gyakorolnak erős ellenőrzést óriási mennyiségű adat felett, anélkül, hogy az egyének számára megfelelő biztosítékokat nyújtanának a személyes adataik kezeléséről. Annak érdekében, hogy felszabadítsuk és kiaknázzuk az európai potenciált, meg kell találnunk az európai utat, egyensúlyt teremtve az adatok áramlása és széleskörű felhasználása, illetve a magánéletre, a védelemre, a biztonságra és az etikai kérdésekre vonatkozó magas szintű normák megőrzése között.

A Bizottság 2014 óta már számos lépést tett. Az általános adatvédelmi rendelettel[8] az EU szilárd keretet hozott létre a digitális bizalom megteremtéséhez. Az általános adatvédelmi rendelet közelgő felülvizsgálata további hasznos elemekkel szolgálhat e tekintetben. Az adatgazdaság fejlődését előmozdító egyéb kezdeményezések közé tartozik a nem személyes adatok szabad áramlásáról szóló rendelet,[9] a kiberbiztonsági jogszabály[10], és a nyílt hozzáférésű adatokról szóló irányelv.[11]

Egyes területeken, például az autóiparban,[12] a pénzforgalmi szolgáltatások,[13] az intelligens fogyasztásmérés,[14] a villamosenergia-hálózati adatok[15] vagy az intelligens közlekedési rendszerek[16] területén adathozzáférésre vonatkozó ágazatspecifikus jogszabályokat is elfogadtak az azonosított piaci hiányosságok kezelése érdekében. A digitális tartalomról szóló irányelv[17] hozzájárult az egyének jogainak erősítéséhez azáltal, hogy szerződéses jogokat vezetett be azokra az esetekre, amikor a fogyasztók a digitális szolgáltatók számára hozzáférést biztosítanak adataikhoz. Nagyon nagy előrelépést jelent az elektronikus azonosítási és bizalmi szolgáltatásokról szóló eIDAS,[18] amely egy ren-

8 Az (EU) 2016/679 rendelet.
9 Az (EU) 2018/1807 rendelet.
10 Az (EU) 2019/881 rendelet.
11 Az (EU) 2019/1024 irányelv.
12 Az 595/2009/EK rendelettel módosított 715/2007/EK rendelet.
13 A pénzforgalmi szolgáltatásokról szóló (EU) 2015/2366 irányelv.
14 A villamos energia esetében az (EU) 2019/944 irányelv, a gázmérők esetében a 2009/73/EK irányelv.
15 Az (EU) 2017/1485 bizottsági rendelet, az (EU) 2015/703 bizottsági rendelet.
16 A 2010/40/EU irányelv.
17 Az (EU) 2019/770 irányelv.
18 Az 910/2014/EU. rendelet.

deletbe foglalt szabványosítási előírás, amely minden EU tagországra vonatkozik – konzisztens jogi kereteket biztosít az elektronikus azonosítók és aláírások elfogadására. Digitális pecséteket is bevezet a szervezetek számára. Az eIDAS megérkezésével az európai szervezetek és kormányzatok egymással versengve folytatják folyamataik teljes digitalizálását.

Közös európai mobilitási adattér kialakítása a legújabb törekvés, amelynek a kialakítása körül nagyon komoly fejlesztési, stratégiaalkotási törekvések húzódnak meg. A közlekedés és a mobilitás nagy hangsúlyt kap az adatmegosztásról szóló vitában a jelenlegi pandémiahelyzet kezelhetőségében is, és ezeken a területeken az EU számos eszközzel rendelkezik. Ez érinti a gépjárműipart, ahol a hálózatba kapcsolt autók működéséhez elengedhetetlenek az adatok, valamint más közlekedési módokat is. A digitalizálás, valamint az összes közlekedési móddal és a logisztikával kapcsolatos adatok alapvető fontosságúak lesznek az európai közlekedési rendszerrel kapcsolatos további munka, és különösen a hamarosan elkészülő intelligens és fenntartható közlekedési stratégia szempontjából (2020. 4. negyedéve). Ennek keretében intézkedésekre kerül majd sor az összes közlekedési ágazatban, valamint a több közlekedési módra kiterjedő adatmegosztással kapcsolatos logisztikára és az utasközpontú ökoszisztémákra vonatkozóan is.

2.2.1. A gépjárművek legújabb fejlesztései

Napjainkban a korszerű járművek óránként mintegy 25 gigabájtnyi adatot generálnak, az önvezető autók pedig több terabájtnyi adatot fognak előállítani, amelyeket a mobilitással kapcsolatos innovatív szolgáltatásokhoz, valamint a javítási és karbantartási szolgáltatásokhoz lehet majd használni. Ezen a területen az innovációhoz szükség van az autók adatainak biztonságosan, jól szervezetten és a versenyszabályokkal összhangban történő megosztására számos különböző gazdasági szereplő között. A járművek fedélzeti adataihoz való hozzáférést az uniós jármű-jóváhagyási jogszabályok 2007 óta szabályozzák, hogy a független javítóműhelyek számára méltányos hozzáférést biztosítsanak bizonyos gépjárműadatokhoz. Jelenleg folyamatban van ennek a jogszabálynak a frissítése annak érdekében, hogy figyelembe vegye az összekapcsolt rendszerek terjedését (3G-4G-5G, az úgynevezett távdiagnosztikai rendszerek), valamint biztosítsa az adatokat generáló autótulajdonosok jogainak és érdekeinek tiszteletben tartását és az adatvédelmi szabályok betartását.

Az autonóm intelligens járművek esetében az autonómiát biztosító többféle intelligens járműrendszer pl.: adatbiztonsági szoftver, HMI, beágyazott modem, V2X, beavatkozók, beágyazott vezérlők, ultrahangos érzékelők, odometriai érzékelők, LIDAR, radar, kamerák működésének kiberbiztonsággal kapcsolatos kérdései még nem váltak általánosan kezelt iparági kérdéssé. Számos tanulmány foglalkozik az autonóm járművek szenzorjainak és vezérlésének a megzavarásával. Az elektromos, elektronikus és programozható elektronikus biztonsági rendszerek járműipari kiberbiztonsági integritási szintjét az ACSIL (Automotive Cybersecurity Integrity Level) értékekkel határozhatjuk meg. A fejlesztések egyik igen erős iránya arra törekszik, hogy olyan autonóm járművek jöjjenek létre, amelyek intelligens módon önállóan képesek lesznek majd közlekedni. Egyre többet tudnak az utakon a hálózatba kapcsolt autók, az okosautók ökoszisztémája egyre komplexebbé válik, aminek számtalan előnye is lehet az autósok számára. A koncepció lényege, hogy az autók kétirányú kommunikációt képesek folytatni a rajtuk „kívül eső" egyéb rendszerekkel is. A kapcsolat általában vezeték nélküli helyi hálózaton (wireless local area network, WLAN) keresztül valósul meg. Ez lehetővé teszi az adatok megosztását más eszközökkel – az autón belül és kívül egyaránt. A connected car mögött álló koncepció pedig egyre kifinomultabbá válik. Elég csak a celluláris kapcsolatra, a felhőmenedzsmentre, az adatokhoz való hozzáférésre és elemzésére gondolni. A fő mozgatórugó várhatóan egyre inkább az 5G és a V2X (vehicle-to-everything), vagyis az autó és minden más közötti kommunikáció lesz majd. A legújabb prognózisok szerint az okosautós piac nagysága 2030-ra eléri majd a 12,7 milliárd dollárt, a kapcsolódó ökoszisztéma pedig egyre összetettebbé fog válni. Az alábbi példákkal szemléltethetjük a fejlődést.

Szórakoztató alkalmazások
A különféle médiatartalom-szolgáltatók – például a Spotify és a Pandora – sok esetben már a világhálóra csatlakoztatott gépjárművek alaptartozékainak számítanak. Az Android Auto és az Apple CarPlay applikációk mellett ezek egyre inkább alapvető extrák lehetnek.

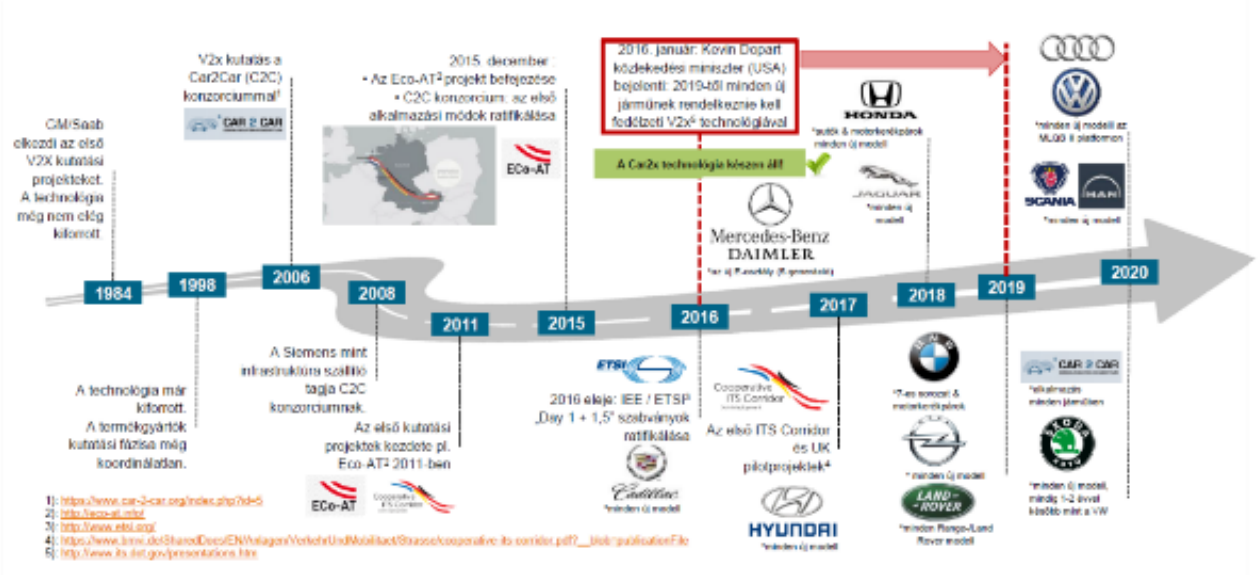
Diagnosztikai és prediktív karbantartási szolgáltatások
A fedélzeti szenzorok és kamerák, az autódiagnosztikai kódok, a rezgés-, zajszint és sérülékenység elemzése révén az autó tulajdonosa és adott esetben a szervizek is könnyebben azonosíthatják a jármű esetleges mechanikai problémáit.

Használatalapú biztosítás
A kapcsolódó, gépkocsiba vagy okostelefonba integrált szenzoros technológia segítségével elemezhető a vezető viselkedése, vezetési stílusa is. A biztosítási díjak mértékét pedig az ezek alapján kalkulált pontszám is befolyásolhatja.

Autonóm járművek „oktatása”
A technológia kidolgozásának folyamatához kapcsolódóan az önvezető autók képesek lesznek feltölteni a szenzoroktól és a precíziós térképektől származó adatokat a megfelelő helyre. A jövőben pedig a frissített térképeket és gépi tanulási modelleket más flottához tartozó járművek is letölthetik majd.

Helyalapú szolgáltatások
A GPS és a térképadatok alapján az autó javaslatot tehet az utasoknak, hogy hol érdemes például enniük vagy tankolniuk. A navigáció pedig valós idejű forgalmi frissítések révén történik.

OTA (Over-the-Air) frissítések
A jármű automatikus szoftverfrissítéseinek köszönhetően az alapvető biztonsági funkciók vagy a fejlett járművezető-támogatási rendszerek (ADAS) is folyamatosan naprakészek lehetnek.



1. ábra: Autonóm intelligens járművek fejlesztései

2.2.2. Átfogó közlekedési rendszer

A személyszállítási tevékenység az előrejelzések szerint 35%-kal nő majd 2015 és 2050 között. A belvízi áruszállítás növekedésének üteme 2050-ig 53%-os lesz, és várhatóan meghaladja majd az utasforgalomét. A digitalizáció és az adatok egyre nagyobb szerepet játszanak a közlekedés fenntarthatóságának támogatásában. Számos jogszabályi keret már tartalmaz adatmegosztási kötelezettségeket, amelyek révén egy lista készül az adatkészletekről (így a tömegközlekedésre vonatkozó adatkészletekről is). Emellett a Digitális Szállítási és Logisztikai Fórum egy „egyesített platformokon" alapuló koncepción dolgozik, melynek célja annak meghatározása, hogy milyen uniós szintű lépésekre van szükség ahhoz, hogy könnyebbé váljon az adatoknak a különböző köz- és magánplatformok biztonságos összekapcsolása révén történő adatok megosztása/további felhasználása. Továbbá, azokban a tagállamokban, ahol az adatokat a közúti közlekedésbiztonsággal, a forgalommal és a multimodális utazásra vonatkozó információkkal kapcsolatos szolgáltatások számára elérhetővé teszik, a nemzeti hozzáférési pontok már meglévő hálózatai biztosítják a köz- és a magánszektor által generált adatok hozzáférhetőségét. Azáltal, hogy az adatok széles körben rendelkezésre állnak és felhasználhatók a tömegközlekedési rendszerekben, az ilyen rendszerek hatékonyabbá, környezetbarátabbá és felhasználóbarátabbá válhatnak. A közlekedési rendszerek javítását célzó adatfelhasználás emellett az intelligens városoknak is kulcsfontosságú jellemzője.

A Bizottság a következőket vállalja:

- Felülvizsgálja a gépjárművekre vonatkozó hatályos uniós típusjóváhagyási jogszabályokat (amelyek jelenleg a javítási és karbantartási célú vezeték nélküli adatmegosztásra összpontosítanak) azzal a céllal, hogy azok hatálya több, a gépjárműadatokon alapuló szolgáltatásra is kiterjedjen (2021 1. negyedéve). A felülvizsgálat keretében többek között arra keresi a választ, hogy a gépjárműgyártók miként teszik hozzáférhetővé az adatokat, valamint milyen eljárások szükségesek ahhoz, hogy az ilyen adatok lehívása az adatvédelmi szabályok, valamint a gépjármű-tulajdonosok szerepének és jogainak maradéktalan tiszteletben tartása mellett történjen.
- Felülvizsgálja a harmonizált folyami információs szolgáltatásokról szóló irányelvet, valamint az intelligens közlekedési rendszerekről szóló irányelvet és az ahhoz kapcsolódó felhatalmazáson alapuló rendeleteket az adatok rendelkezésre állásának, újra felhasználásának és interoperabilitásának további elősegítése érdekében (mindkettő 2021-ben), és erősebb koordinációs mechanizmust hoz létre azzal a céllal, hogy az egész EU-ra kiterjedő CEF-program támogatási cselekvése keretében egyesítse az ITS-irányelv alapján létrehozott nemzeti hozzáférési pontokat (2020).
- Módosítja az egységes európai égboltról szóló rendeletre irányuló javaslatot, új rendelkezésekkel bővítve azt az adatok rendelkezésre állására és az adatszolgáltatók piaci hozzáférésére vonatkozóan, hogy ezáltal előmozdítsa a légiforgalmi szolgáltatás digitalizálását és automatizálását (2020). Ennek köszönhetően javulni fog a légi közlekedés biztonsága, hatékonysága és kapacitása.
- Felülvizsgálja a vasúti közlekedés területén alkalmazott interoperábilis adatmegosztásra vonatkozó szabályozási keretet (2022).

2.3. Az ITS helyzete Magyarországon

Hazánkban is az ITS városi alkalmazásai eddig jellemzően elsősorban a nagyvárosokhoz köthetők, ahol a népesség és ehhez kapcsolódóan a mobilitás mértéke nagy vagy az összetett városi infrastruktúra-, illetve közúthálózat mobilitásra gyakorolt hatása, a forgalmi jellemzők, az úthálózat szerkezete olyan közlekedéssel kapcsolatos problémákat indukálnak, melyek kezelésében az építési jellegű beavatkozások mellett vagy helyett hatékony segítséget nyújthatna az ITS működése.

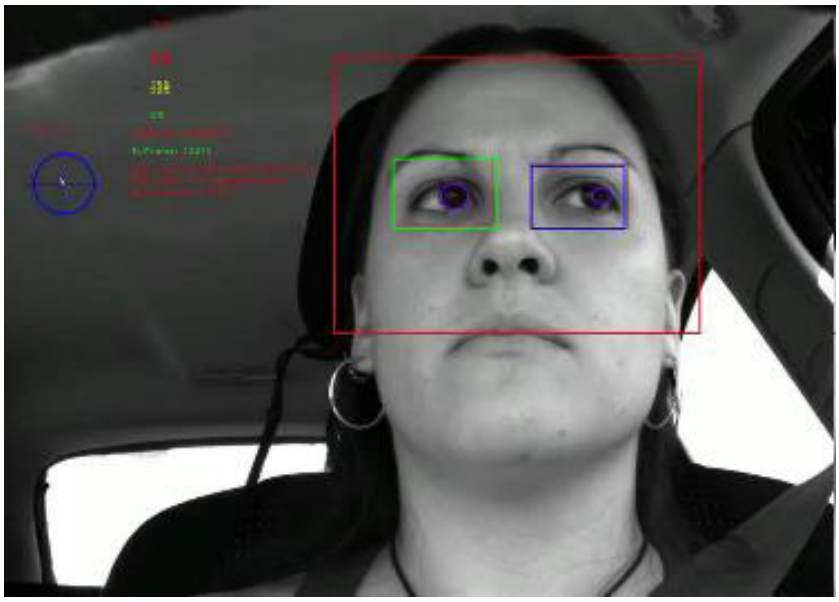
Az intelligens közlekedési rendszerek nagyvárosi alkalmazásának operatív célja a várost érintő hazai, adott esetben nemzetközi tranzitforgalom, a nagyvárosi agglomerációs forgalom és a városon belüli forgalom egyenletesebb, kevesebb zavarral járó és kontrollált, ezáltal biztonságosabb és kevesebb környezeti terheléssel járó lebonyolítása. Ezzel párhuzamos távlati, stratégiai célja pedig a közlekedők környezetkímélőbb közlekedési módok használatára való ösztönzése, az új közlekedési formákra való váltás kedvező feltételeinek megteremtésével, illetve, ezen közlekedési módok szolgáltatási színvonalának emelésével.

A városi közlekedési ITS-megoldások túlnyomó többsége az integrált közlekedésszervezési és szabályozási rendszer keretein belül, abba integrálva jelenik meg, azonban több olyan lehetőség is lenne, ahol a mérési adatok jobb felhasználásával vagy megosztásával jelentős haladást lehetne elérni, amennyiben mind az adatgyűjtő, mind az adattovábbító, mind a szabályozó-információt nyújtó eszközök több célt szolgálhatnának egyszerre.

Módszertani szempontunk, hogy elsősorban olyan rendszereket vizsgálatunk, amelyek felhőalapú ITS Ökoszisztéma esetén jelentős mértékben javíthatnának a közlekedésbiztonság egészén. Minden egyes vizsgálandó lehetőség kapcsán értékeljük az adott rendszert az adatgyűjtés, adatfeldolgozás és információbiztonság szempontjából, és ennek a rendszernek az értékelésében kifejtjük, hogy az így előálló adatok mennyiben hasznosíthatók a komplex ITS-szempontok szerint.

2.3.1. Fáradtságfigyelő rendszer

A járművezető fáradtságát figyelő rendszer (2. ábra) automatikusan elemzi a vezetési jellemzőket, és amennyiben annak bizonyos jelei a sofőr fáradtságára utalnak, pihenésre tesz javaslatot a járművezető felé. A rendszer bizonyos km/h sebesség felett folyamatosan figyeli a kormánykerék mozgását és egyéb járműbeli jeleket, amelyek alapján fáradtsági szintet becsül. Meghatározott szint felett a sofőrt vizuális és akusztikus úton figyelmezteti. Ha a vezető mégsem tesz pihenőt, a jelzés adott percenként megismétlődik.



2. ábra: Szemmozgást figyelő rendszer
Forrás: https://www.youtube.com/watch?v=rHAkyynLGeA
Letöltve: 2020. 04. 23.

Adatgyűjtés, adatfeldolgozás
A különböző rendszerek eltérő adatok alapján figyelik a vezető fáradtságát, például a sávtartás, kormánymozdulatok, gyorsulások érzékelése által). Fejlesztés alatt állnak a vezető szívverését és légzését figyelő biztonsági övek és ülésborítások, illetve szem- és fejmozgásfigyelők is.

A rendszer értékelése
Általában önállóan működő járműrendszerekben a járművön belüli szenzorok adatait alkalmazhatják (pl. kormánykerékelfordítás-jeladó, mely az ESP része). A különböző tudatmódosító szerek általi befolyásoltságot ellenőrző rendszerek hazai alkalmazása még nem jellemző.

Amennyiben ezeknek a szenzorrendszereknek az adatai egy felhőalkalmazásba összegyűjthetőek lennének a GPS/GNSS koordinátákkal együtt, akkor ki lehetne olyan szakértőirendszer-alkalmazást alakítani, amely szükség esetén riasztást vagy figyelmeztetést küld a környezetben mozgó járműveknek, vagy kritikus esetben a közlekedésbiztonsági felügyelet számára, mivel ezek a megoldások manapság önmagukban, járművenként autonóm rendszerként viselkednek. A riasztást fel lehetne használni, hogy az arra jogosult szereplők megelőző beavatkozással pihenésre kötelezhetik a vezetőt.

A felmerülő kérdésre, hogy meddig tartozik a GDPR szempontból személyes adatnak, vagy hol kezdődik a beavatkozási szükséglet határa, kik, milyen jogosultsággal avatkozhatnak be, választ ad a rendelkezésre álló GPS/GNSS[19] információ, illetve egy integrált felhőalapú rendszer integrációjában megvalósítható jogosultság/érvényességi területkezelés, amely által területileg is kijelölhetők a riasztásban érintettek, amelyben implementálandó a fizikai területhatárok átlépésével járó folyamatok is. Ennek bevezethetősége csak hosszú távon képzelhető el, mivel kötelező bevezetése várhatóan nagy ellenállásba ütközne a gépjárművezetők részéről.

[19] GNSS - Global Navigation Satellite System.

2.3.2. KRESZ-szabályok betartását segítő rendszerek

2.3.2.1. Sebesség túllépésére figyelmeztető rendszerek

Hangjelzéssel, látható jelzéssel és/vagy mechanikus jelekkel figyelmeztetik a járművezetőt, ha a jármű sebessége túllépi a vezető által szándékolt mértéket (3. ábra), vagy éppen az úton engedélyezett legnagyobb sebességet. A rendszerek egy része képes felismerni és kijelezni az útszéli sebességhatárt jelző táblákat, emellett a gépkocsi más rendszerei (pl. navigációs GPS/GNSS) által kapott információkat is felhasználja. A navigációs rendszerek leggyakrabban érzékelt funkcionalitása a megfelelő sebességhatár betartása.

3. ábra: Sebesség túllépésére figyelmeztető rendszer:
Forrás: https://www.renault.hu/autok/modellek/kadjar/jellemzok.html
Letöltve: 2020. 03. 18.

Adatgyűjtés, adatfeldolgozás
A sebességhatárról szóló információt/megengedett sebességet a jelzésbe épített adó, a gépjárműben lévő kamera, digitális térkép és a jármű egyéb rendszerei vagy ezek kombinációja közvetíti megbízható helymeghatározással. Az adatok gyűjtése ily módon a járművön belül történik.

A rendszer értékelése
A rendszer jelenleg általában elszigetelten működik, funkciója a vezetés támogatása, az adatokat nem küldi tovább, szankcionálási rendszerekkel nem integrált, külső ellenőrzést nem tesz lehetővé. Már az új középkategóriás járművekben is szériaalkalmazásként alkalmazzák, navigációs rendszerekkel vagy navigációs mobiltelefon-alkalmazásokkal egyre jobban elterjedt a használata.

Az alapmegoldás ebben a formában nem integrálható felhőalapú informatikai rendszerbe, azonban pl. a Waze[20] rendszer megközelítése az okostelefonokra telepített applikáción keresztül képes ezt a feladatot hálózati szinten ellátni, és az itt gyűjtött adatokkal már Big Data- és MI-elemzéseket lehet végezni. Ennek azonban a GDPR megfelelősségével a jelenlegi formájában az EU-ban probléma lehet. A rendszer továbbfejleszthető lenne, ha egységes ITS Ökoszisztéma lenne kialakítva, amelyben akár az utak menti jelzőtáblák is teljes körű digitális kontroll alatt lennének. Egy olyan chip lehetne rajtuk például, amely rendelkezik gyorsulásmérővel, és egy jelzőtábla kidőlése vagy kiütése azonnal észlelhető lenne a rendszerben. A jövőben az ITS Ökoszisztémának, ha a szabályozás megköveteli, preventív vagy szankcionálás céllal integrálhatónak kell lennie, mert enélkül az önvezető járművek, amelyek teljes kontroll alatt működnek, és a nem önvezető járművek nem fognak tudni biztonságosan együtt közlekedni. Nyilván ennek megvan az auditálási követelménye is, különös tekintettel az IT-biztonsági megfelelőségre, a rendszerek bizalmasságára, sérthetetlenségére és rendelkezésre állására.

2.3.2.2. Sebességkijelző, -mérő táblák

A rendszer feladata a járművezetők számára a megengedett sebesség túllépése esetén figyelmeztető jelzést adni, vagy számukra jelezni a haladási sebességüket. A radaros sebességmérő és sebességkijelző táblák a jármű sebességét folyamatosan frissítve jelzik a járművezetőknek, illetve a „LASSÍTS” LED-felirat figyelmeztethet, hogy túl nagy sebességgel közelítenek.

Adatgyűjtés, adatfeldolgozás
A rendszer (4. ábra) radaros sebességméréssel működik, az adatok gyűjtése és feldolgozása az eszközben történik a helyszínen.

4. ábra: Sebességmérő és -kijelző tábla
Forrás: http://www.sebessegmerotabla.hu/ Letöltve: 2020. 04. 23.

[20] KSII The 14th Asia Pacific International Conference on Information Science and Technology (APIC-IST) 2019. This study was supported by Isaac Engineering and Oracle Cloud Innovation Accelerator. Oracle Big Data Cloud Service was used in the data analysis. Traffic Data Analysis and Prediction using Big Data Dalyapraz Dauletbak and Jongwook Woo Department of Information Systems, California State University Los Angeles: http://www.calstatela.edu/sites/default/files/groups/High%20Performance%20Information%20Computing%20Center%20%28HiPIC%29/papers/trafficapic-ist2019.pdf

A rendszer értékelése
A rendszerek alapvetően önálló működésre képesek, rendszámfelismerést, adatgyűjtést és ezáltal szankcionálást nem tesznek lehetővé. Ugyanakkor kiegészíthetők térfigyelő kamerával és videórögzítővel, illetve rendszámfelismerő rendszerekkel. Több hazai és nyugati tanulmány bizonyítja, hogy a sebességmérő előjelző berendezések csökkentik a balesetek számát és súlyosságát. A rendszernél mért értékes adatok a forgalomirányításban felhasználhatók lennének, és a felhőalapú ökoszisztémában növelni lehetne vele a közlekedés biztonságát vagy akár a lopott járművek felderítési hatékonyságát is a GDPR-elvárások figyelembevételével.

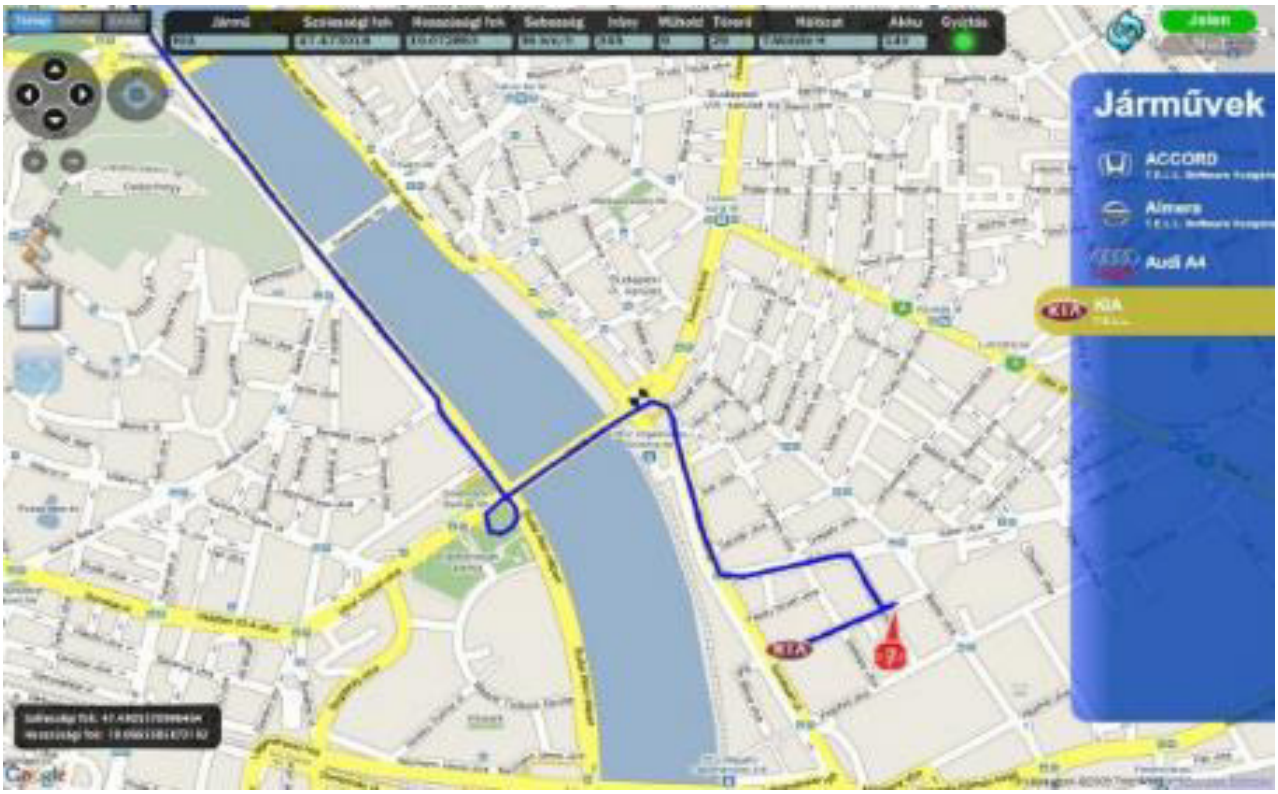
2.3.3. Közlekedői viselkedés egyénre szabott valós idejű követését támogató rendszerek

2.3.3.1. EasyTrack[21] applikáció

GPS-nyomkövető, -járműkövető és -flottamenedzsment rendszer. Képes a vezetési stílus rögzítésére, kimutatások készítésére (sebességeloszlás, motorfordulatszám-eloszlás, gázpedálállás-eloszlás).

A rendszer kétféle adatrögzítést végez, egyrészt az integrált fedélzeti egység monitorozza a gépjármű különböző működési mutatóit és helyzetét, másrészt a vezetőnek lehetősége nyílik különböző adatok rögzítésére (pl. szállítmányra vonatkozó adatok). A rendszer hálózati működését, a fedélzeti egység és a központi szerver közötti adatkapcsolatot mobilhálózat biztosítja. A rendszer kétirányú kommunikációja biztosított, vagyis szükség esetén a központban feldolgozott adatok alapján a rendszer képes figyelmeztetést vagy riasztást küldeni a gépjármű vezetőjének.
Adatgyűjtés, adatfeldolgozás
Az adatok gyűjtése a járművekben történik, fedélzeti egységek segítségével (mért és tárolt adatok). Az adatokat a fedélzeti rendszer továbbítja a központnak, ahol centralizált szervereken történik meg az adatfeldolgozás és az adattárolás. Az adatok nagy megbízhatósággal és integritással jutnak a járműről a központi adatbázisba. Az adatátvitel kiindulópontja a járműfedélzeti egység, amely egy kommunikációs egység segítségével GSM-hálózaton keresztül kapcsolódik a kommunikációs szerverhez. A szerver fogadja az adatokat, majd a megfelelő ellenőrzések és konverziók után, egy adatbázisba írja az információkat. Az adatfeldolgozó rendszer fő részei a térképes, illetve táblázatos és grafikonos megjelenítők (5. ábra).

[21] Bővebben: https://info.easytrack.hu/



5. ábra: EasyTrack applikáció
Forrás: https://www.ldsz.hu/files/attachments/product_image-/1057/large/TELL_EASYTRACK_terkep.jpg
Letöltve: 2020. 03. 18.

A járműkövető rendszerek jelenleg a nyilvános GSM-hálózatot használják adatátviteli célokra (SMS-alapú/adatkapcsolt/csomagkapcsolt GPRS, EGPRS, UMTS, HSDPA). A felhasználók az adatokhoz az adatszolgáltatón keresztül férnek hozzá.

A rendszer értékelése
A rendszer a nemzeti útdíjfizetési rendszerrel együttműködik, integrált. A fedélzeti egységek segítségével az útdíjfizetés automatikusan megvalósítható. A rendszer egyelőre más városirányítási rendszerekkel nem képes együttműködni (pl. parkolási rendszerek, forgalomirányító rendszerek, behajtásidíj-kezelő rendszerek stb.). A jövőbeli együttműködés funkcióbeli fejlesztéseket is megkövetel, tudni kell például elkülöníteni a hosszú távú megállást (5-15 percen túl) és a rövid távú megállást (piros lámpa, forgalmi dugó, kiszállás stb.).

A fent részletezett követőrendszer azért került feldolgozásra, hogy bemutatható legyen, hogy már vannak ilyen jellegű rendszerek, amelyek sajnos alapvetően továbbra is szigetszerűen vagy cég szinten működnek. Az egységes felhőalapú rendszernek ezeket a rendszereket kellene adatszinten integrálnia.

2.3.3.2. WebEye applikáció[22]

Az előzővel azonos funkciójú alkalmazás a WebEye, alapja a korszerű, megbízhatóan működő GPS-alapú járműkövetés. Korszerű telematikai eszközökkel támogatja a járműfelügyelet és a fuvarirányítás komplex működését. A járművek valós idejű felügyeletével és a gépkocsivezetőkkel való gyors és hatékony kommunikáció biztosításával segíti a fuvarszervezési feladatok ellátását, növeli a megbízhatóságot, biztonságot.

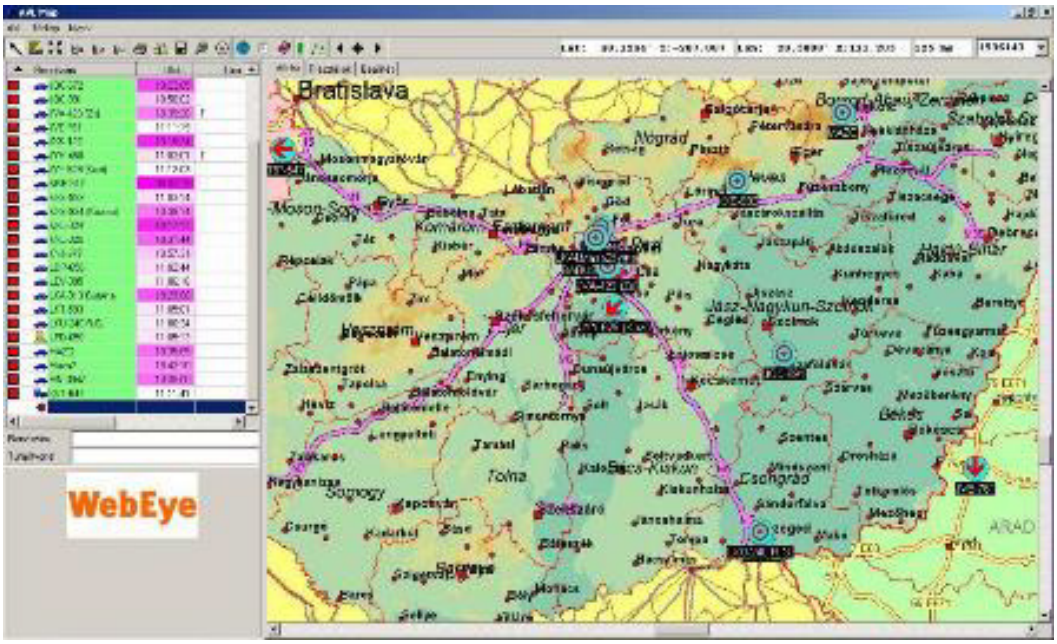
[22] Bővebben: https://hu.webeye.eu/

A rendszer képes az alábbi funkciók elvégzésére:

- Vezetési idő figyelése
- Vezetési stílus elemzése
- Üzemanyagmérés
- Veszélyes áruszállítás támogatása
- Nagy értékű áruszállítás támogatása
- Hűtött áruszállítás támogatása

Adatgyűjtés, adatfeldolgozás

Az adatok gyűjtése a járművekben történik, fedélzeti egységek segítségével (mért és tárolt adatok). Az adatokat előre definiált események bekövetkezésekor vagy időközönként elküldik egy központi szervernek, amely az adatfeldolgozásért és a tárolásért felelős. Az adatok nagy megbízhatósággal és integritással jutnak a járműről a központi adatbázisba. Az adatátvitel kiindulópontja a járműfedélzeti egység, amely egy kommunikációs egység segítségével GSM (Global System for Mobile communications) hálózaton keresztül kapcsolódik a kommunikációs szerverhez. A szerver fogadja az adatokat, majd a megfelelő ellenőrzések és konverziók után egy adatbázisba írja az információkat. Az adatfeldolgozó rendszer fő részei a térképes, illetve táblázatos és grafikonos megjelenítők (6. ábra).



6. ábra: WebEye alkalmazás
Forrás: http://docplayer.hu/docs-images/40/767618/images/page_6.jpg
Letöltve: 2020. 04. 23.

A járműkövető rendszerek jelenleg a nyilvános GSM-hálózatot használják adatátviteli célokra (SMS-alapú/adatkapcsolt/csomagkapcsolt GPRS, EGPRS, UMTS, HSDPA). A felhasználók az adatokhoz az adatszolgáltatón keresztül férnek hozzá.

A rendszer értékelése

A rendszer a nemzeti útdíjfizetési rendszerrel együttműködik, integrált. A fedélzeti egységek segítségével az útdíjfizetés automatikusan megvalósítható. A fent részletezett követő rendszer szigetszerűen működik, egy felhőalapú szenzorhálózati rendszerbe való integrálhatósága a jelen fejlettségi szinten számos további fejlesztési feladatot követel meg.

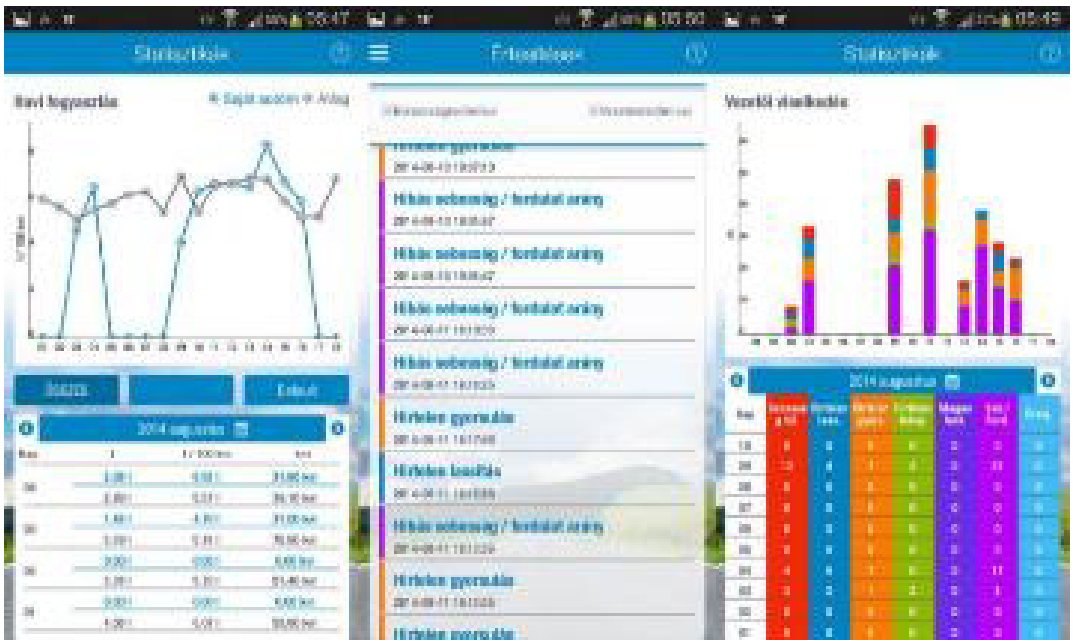
2.3.3.3. VEMOCO rendszer[23]

Magyar fejlesztésű, komplex autóbiztonsági szolgáltatás. Alapjául a gépjárművek fedélzeti számítógépe által biztosított autódiagnosztikai adatok szolgálnak, a rendszer fő alkotóelemei az autó OBD[24] portjára csatlakozó modul, a kinyert adatokat feldolgozó és megjelenítő mobil alkalmazás, illetve webes felület, valamint a 24 órás ügyfélszolgálat és a biztosítói partnerekkel köthető, legújabb trendeknek megfelelő viselkedés alapú biztosítás.

Európai uniós előírások szerint a 2001 után gyártott járműveknek már mind rendelkezniük kell az OBD-csatlakozóval, erre csatlakozik a VEMOCO modulja is. A VEMOCO rendszer által alkalmazott olvasó modul önálló GPS-chippel rendelkezik, illetve saját zárt, egész Európára kiterjedő rendszerén keresztül kommunikál a VEMOCO adatbázisával. Az OBD-csatlakozók harmadik fél részéről történő felhasználását a gyártók szeretnék tiltani, így ez a fejlesztési irány a későbbiekben be fog záródni.

Adatgyűjtés, adatfeldolgozás

A rendszer alapját a gépjárművek fedélzeti számítógépe által biztosított autódiagnosztikai adatok szolgáltatják. A kinyert adatok feldolgozása és megjelenítése mobil alkalmazással, illetve webes felületen lehetséges (7. ábra).



7. ábra: VEMOCO rendszer felhasználói felülete
Forrás: https://vemoco.com/bundles/connectedcarsite/images/content_images-/hu/news/androidblog3.jpg
Letöltve: 2020. 03. 18.

A VEMOCO 24 órás ügyfélszolgálata folyamatosan rendelkezik a rendszerhez csatlakoztatott járművek műszaki állapotára vonatkozó információkkal, valamint GPS-koordinátáikkal.

A rendszer értékelése

A rendszer autonóm működésű, szigorúan bizalmasan kezeli az adatokat, azonban az autó pozíciójára és járműdinamikai adataira vonatkozóan adatokhoz folyamatosan hozzáfér. A rendszer szempontjából kockázati tényezőként kell nyilvántartani, hogy az autógyártók egyre inkább szorgalmazzák az OBD interface lezárását, ezzel megakadályozandó a gépjármű adatbuszának a „megcsapolását”.

[23] Bővebben: https://vemoco.com/hu/
[24] OBD On-Board Diagnostic.

2.3.4. Veszélyes közlekedési helyzetek előrejelzését támogató rendszerek

2.3.4.1. Változtatható jelzésképű táblák (VJT)

Az autópályák egyes keresztmetszeteiben változtatható jelzésképű szöveges és grafikus információs és jelzőtáblák állnak rendelkezésre az utazóközönség tájékoztatása céljából. A dinamikus forgalmi-menedzsment-rendszerek harmonizálják a forgalmi folyamot, és a forgalmi helyzetnek megfelelően befolyásolják a járművek sebességét. A változtatható jelzésképű táblák működtetésének célja a közlekedésbiztonság növelése, valamint a forgalom harmonizálása – váratlan események, forgalmi torlódások és kedvezőtlen időjárási viszonyok miatt kialakuló – forgalmi zavarok esetében. Eseménymentes (esemény alatt balesetet, torlódást, munkavégzést, időjárási vagy egyéb veszélyhelyzetet értünk) állapotban közlekedésbiztonsági információk kijelzése történhet rajtuk (biztonsági öv viselésére, követési távolság betartására figyelmeztetnek stb.).

Adatgyűjtés, adatfeldolgozás
A rendszer adatok gyűjtésére nem, csak megjelenítésére, tájékoztatásra alkalmas. Vezérlésüket, folyamatos frissítésüket központilag végzik (8. ábra).

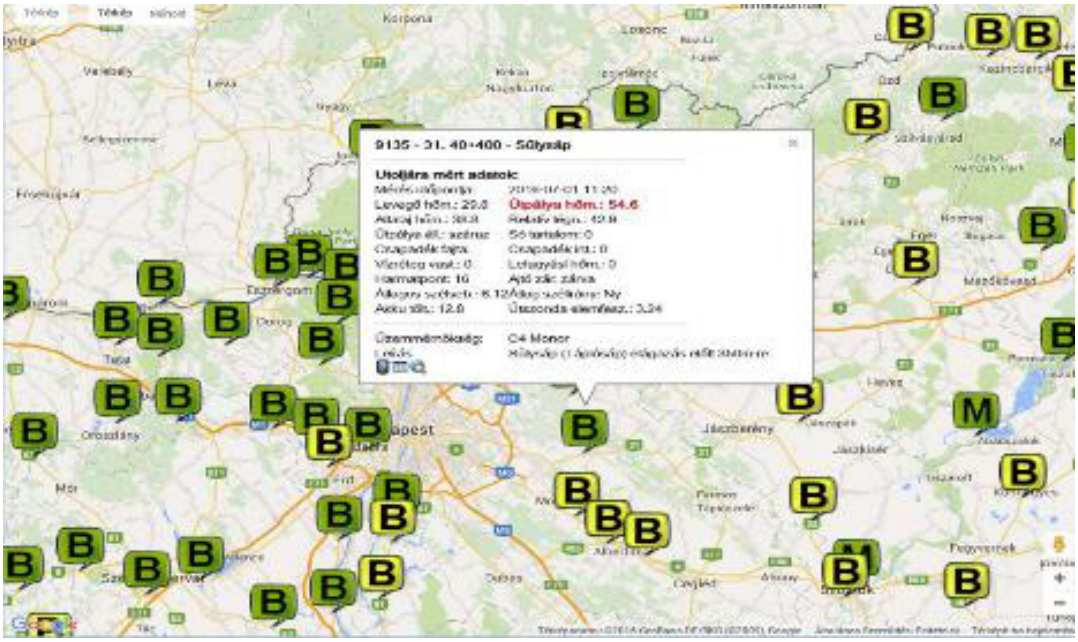
8. ábra: Változtatható jelzésképű tábla
Forrás: https://www.swarco.com/var/em_plain_site/storage/images/media/images/swarco-traffic-hungaria/vjt/p1040132/72082-1-eng-US/P1040132_795x530px.jpg
Letöltve: 2020. 04. 15.

A rendszer értékelése
Változtatható jelzésképű táblák segítségével dinamikus forgalommenedzsment valósítható meg. A kijelzők tartalmának összehangolása központilag valósul meg úgy, hogy a nagy elemszám és a földrajzi függetlenség biztosítható centralizált informatikai szolgáltatás segítségével. Ez mint kiterjedt tájékoztató rendszerelem kerülhet bevonásra és megvalósításra. Továbbá a bemutatott rendszer alkalmas lehet más rendszerelmekből érkező riasztások alapján előrejelzésre, így több szolgáltatás összekapcsolására. Példaként említhetjük, hogy az ÚtMet rendszer beküldi az adatokat a központba, a feldolgozó logika pedig eldönti, hogy hol és mit kell előre jelezni (pl. csúszós út), vagy helyalapú információkból torlódás várható. A kategóriában bemutatott rendszereket érdemes lenne összekapcsolni az egyéni navigációs lehetőségekkel is.

2.3.4.2. ÚtMet rendszer

Országos kiterjedésű útmeteorológiai információs rendszer a korszerű útüzemeltetés támogatására. Célja objektív útállapot- és időjárási adatok gyűjtése. A mérési adatok alapján a rendszer riaszt, ha például 1 órán belül az úttest lefagyása várható.

Adatgyűjtés, adatfeldolgozás
A végfelhasználó útkezelő, illetve diszpécser számára az adatok/információk kezelőfelületen jelennek meg térképes, grafikonos, táblázatos formában (9. ábra).



9. ábra: Útmet rendszer információs felülete
Forrás: http://docplayer.hu/44293987-A-klimavaltozas-hatasai-a-kozuti-infrastrukturara.html
Letöltve: 2020. 04. 15.

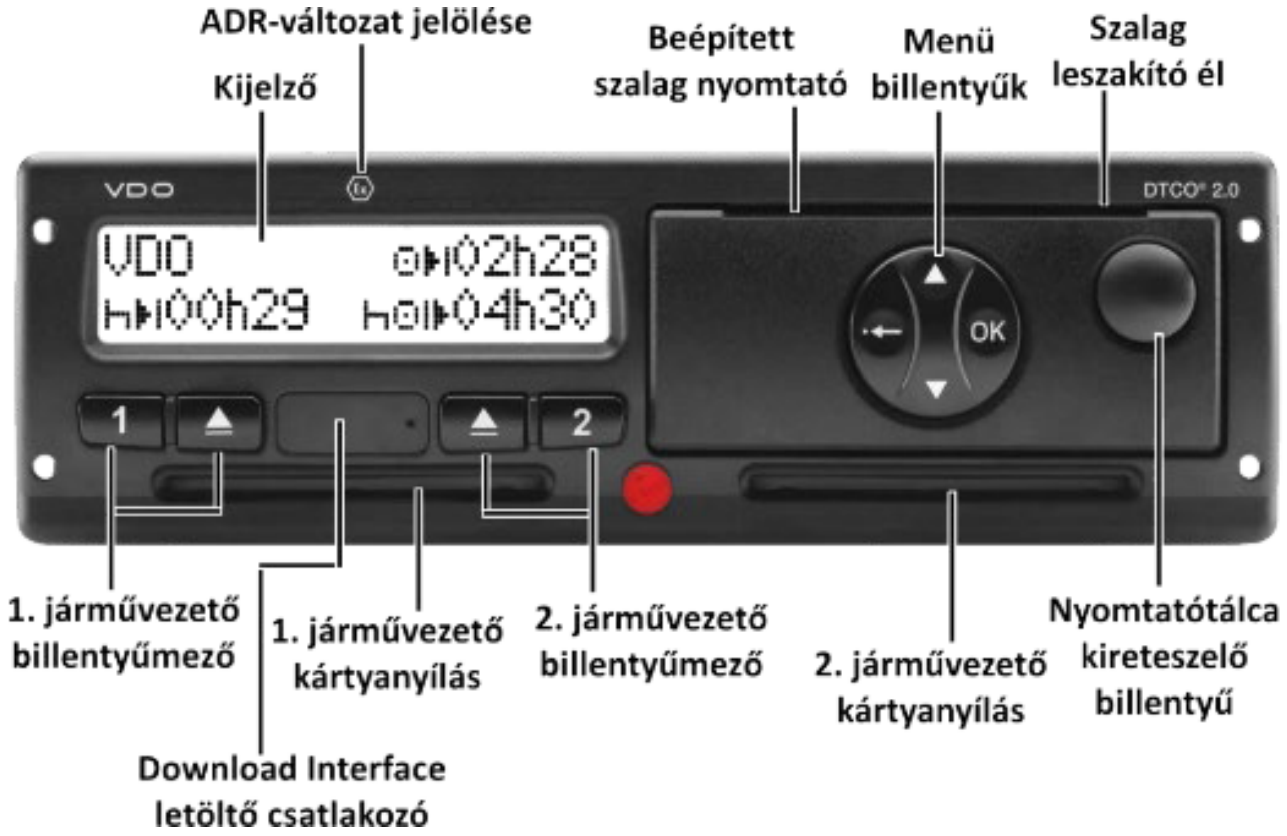
A rendszer értékelése
A szolgáltatott adatok meteorológiai adatokkal integráltak. A rendszer használói: közútkezelők üzemmérnökségei. Későbbi fázisban más központok, illetve közvetlenül az úthasználók is felhasználók lehetnek.

A dinamikus adatokat a központi rendszeren keresztül lehet disztributálni a törzsadatok és idősori adatok alapján történő feldolgozással. A cél, hogy szükség esetén lehessen riasztást generálni, a megfelelő jogosultság alapján több város/közútkezelői terület legyen megcímezhető, legyen riasztható a szükséges beavatkozásra, illetve az adatok alapján vészhelyzet-előrejelzés legyen generálható automatikusan az utakon elhelyezett kijelzőkre vagy navigációs rendszerekre.

2.3.5. Járművön belüli közlekedésbiztonságot támogató rendszerek

2.3.5.1. Digitális tachográf

A digitális tachográf (10. ábra) elektronikus úton rögzíti a gépjárművezető által vezetéssel, pihenéssel és egyéb munkavégzéssel eltöltött idejét. Ezeket az adatokat mind a fedélzeti egység, mind pedig a kártya tartalmazza; az előbbi kb. 365 nap adatainak tárolására képes, az utóbbi pedig kb. 28 napot tud tárolni. A kártyán található adatokat rendszeres időközönként – kb. 3 hetente –, illetve minden egyéb indokolt esetben javasolt letölteni az adatvesztés elkerülése érdekében. Alkalmazásának célja a vezetési és pihenőidők fokozottabb betartatása, továbbá a közutak biztonságosabbá tétele – közlekedésbiztonság növelése –, illetve a tisztességes versenyhelyzet megteremtése Európa országaiban.



10. ábra: Digitális tachográf
Forrás: http://onlinetachograf.eu/wp-content/uploads/2015/09/digi-tacho-reszei-2-1024x652.png
Letöltve: 2020. 04. 15.

Adatgyűjtés, adatfeldolgozás
Az adatokat a fedélzeti egység (azaz maga a digitális tachográf) gyűjti és elektronikus úton rögzíti. A tachográfok elektronikus érzékelők, rögzítik a jármű sebességét, a megtett út hosszát, külön az egyes utak hosszát, a buszok és teherautók indulási és megállási időpontját.

A rendszer értékelése

Az Európai Unió rendeletben (2135/98/EK rendelete) határozta meg a tachográfok bevezetését. A digitális tachográfok kötelező alkalmazása a 3,5 tonna feletti megengedett legnagyobb össztömegű tehergépjárművekre, valamint a 9 főnél több ülőhellyel rendelkező személyszállító járművekre terjed ki. A digitális tachográfkártyák kiadásának támogatására, nyilvántartására, valamint a gépjárművezetők vezetési- és pihenőidejének közúti és telephelyi ellenőrzésére integrált informatikai rendszer került kialakításra. A rendszer az EU jogszabályokban meghatározott adatokat a TACHOnet hálózaton közvetíti az EU adatbázisába. Ez a „fekete doboz" funkciót jelenti alapvetően, az online térben és a navigációs rendszerekkel nincs adatkapcsolatuk.

2.3.5.2. e-Call és a 112 Segélyhívó Rendszer

Az Európai Parlament „A fedélzeti e-segélyhívó rendszer kiépítésével összefüggő típus-jóváhagyási követelményekről és a 2007/46/EK irányelv módosításáról szóló európai parlamenti és tanácsi rendelet" előterjesztést, a Tanács által első olvasatban elfogadott szöveggel, 2015-ben jóváhagyta. A rendelet alapján 2018. március 31-től az összes, Európában engedélyezett új gépjárművet fel kell fedélzeti e-segélyhívó eCall (11. ábra) rendszerrel szerelni. A korábban elfogadott 585/2014/EU európai parlamenti és tanácsi határozat 2017. október 1-ig adott határidőt a tagállamoknak, hogy kiépítsék az e-segélyhívások fogadásához és kezeléséhez szükséges infrastruktúrát. Ennek az utóbbinak az a célja, hogy közlekedési baleset bekövetkeztekor a járművekbe épített, intelligens egység a segélyhívó központot azonnal értesítse.

11. ábra: Az eCall – OnStar szolgáltatás
Forrás: http://www.autoszektor.hu/sites/default/files/u1640/a7on_star_opel.jpg Letöltve: 2020. 04. 15.

Az eCall a helyszín pontos koordinátáit is automatikusan továbbítja, így a gyors segítségnyújtás abban az esetben is biztosított, ha az autóvezető pillanatnyi állapota a segélykérés általa való kezdeményezését nem teszi lehetővé. A 112-es segélyhívó központból a diszpécser a riasztást a mentőkhöz, a tűzoltókhoz és a rendőrséghez egyaránt továbbíthatja. Szakértői becslések szerint ezzel a módszerrel a későn érkező segítség miatt bekövetkező közúti baleseti halálesetek száma 50%-kal csökkenthető lesz.

Az e-Call rendszer úgynevezett intelligens telekommunikációs eszközként a beépített szenzorok visszajelzései alapján képes a baleset bekövetkezésének tényét megállapítani, és azonnal, emberi beavatkozás nélkül értesíti a segélyhívó központot, a baleset legfontosabb paramétereit is elküldve, mint például:

- a baleset pontos időpontja, helyszíne,
- a jármű egyedi azonosítója,
- GPS-koordináták.
- feltételezett sérültek száma.

A segélyhívó központ a beérkező adatok rögzítése után azonnal értesíti az érintett mentőegységeket, így a baleset helyszínelése, a sérültek ellátása a lehető leghamarabb elkezdődhet, ami sok esetben életeket menthet. Az e-Call rendszer úgy lett kialakítva, hogy szükség esetén maga a gépjárműben utazó személy is képes legyen vele segélyhívást kezdeményezni.

Az eCall 2015-ös bevezetésével párhuzamosan az EP arra kötelezte az egyes tagországokat (a 305/2013/EU előírásoknak megfelelően), hogy építsék ki a 112-es segélyhívószámhoz tartozó központok egységes hálózatát (12. ábra).

12. ábra: 112 SOS – Egységes Segélyhívó Rendszer
Forrás: http://sos112.info/ Letöltve: 2020. 04. 15.

13. ábra: 112.hu

Az ESR (Egységes Segélyhívó Rendszer) ugyanúgy a 112-es telefonszámon hívható, azonban a hálózat működése azonos minden EU-s országban, és a hatóságokkal való kapcsolatfelvétel azonos feltételek mellett elérhető minden uniós polgár számára. Magyarországon a két hívásfogadó központ Szombathelyen és Miskolcon található, és 7 x 24-ben működik.

Adatgyűjtés, adatfeldolgozás

Az adatgyűjtés automatikus, a járműbe épített szenzorok által. A továbbított adatokat a segélyhívó központ rögzíti és dolgozza fel, a mentést ezek alapján azonnal meg lehet kezdeni. Balesetkor küldött adatok: a baleset legfontosabb adatai, például: a gépjármű azonosítója, a baleset pontos ideje, a helyszín GPS-koordináták, illetve az utasok száma. A hívásfogadó központok az eCall-készülékek által elküldött adatokat a nemzeti szabályozás és az adatvédelmi törvény értelmében meghatározott ideig őrzik (14. ábra) eCall séma szerint.

14. ábra: eCALL séma

A rendszer értékelése

A baleset bekövetkezése és annak bejelentése közt eltelt idő kb. 10-15 perccel csökkenthető. Traumatológiai elemzések, forgalmi vizsgálatok szerint a közlekedési balesetekben elhunytak száma 2-2,5%-kal csökkenthető. Az elvégzett vizsgálatok alapján az eCall szolgáltatással 17-18%-os csökkenés érhető el az összes baleseti torlódást tekintve. Különböző becslések alapján az eCall segélyhívó szolgáltatással a teljes, hazai úthálózaton akár 3,5%-os csökkenés is elérhető lehet az összes torlódásos órák számában.

A 2018. március 31-et követően forgalomba helyezett új gépjárművek és kisteherautók esetén az Európai Parlament kötelezően előírja a gyári beépítésű e-Call segélyhívó rendszerek meglétét, ezeket minden autógyártónak az összes új modellbe gyárilag implementálni kellett.

Az eCall rendszer integrálása még kialakítás alatt van, és kapcsolódni fog az ESR 112 rendszerhez. Magyarországon kormányzati támogatású projekt van folyamatban a meglévő járművekbe történő beszereléshez egy olcsóbb rendszer kialakítására.[25]

Nagyon kellemetlen és nem megoldott probléma, hogy a 112-re érkező hívások 53% hideghívás (felesleges, intézkedést nem igényel) (15. ábra). E hívások kezelése sok esetben akadályozhatja a valódi hívások kezelését. Pl. a mobiltelefonokról ingyenes hívásokat lehet indítani még SIM-kártya nélkül is, így több kereskedőnél a telefonkészülék kipróbálását a 112 hívásával mutatják be.

[25] GINOP-2.2.1-15-2016-00011.

Hívásfogadó központok tevékenységének alakulása a 2015-2019. évben

	2018. IV.	2019. IV.	Változás Eset	Dinamika % -ban	Országos % a 2019.	2015. I IV.	2016. I IV.	2017. I IV.	2018. I IV.	2019. I IV.	Változás 2018 2019.	Dinamika 2018 2019.	Országos % a 2019.
Valós segélyhívások száma	135 899	126 382	-9 517	-7,0%	25%	291 112	296 993	304 812	509 630	507 446	-2 184	-0,4%	35%
Információt kérő hívások száma	46 426	42 517	-3 909	-8,4%	12%	169 839	157 318	157 883	173 830	164 372	-9 458	-5,4%	11%
Intézkedést nem igénylő hívások száma	225 340	189 049	-36 291	-16,1%	53%	1 139 966	1 037 710	919 985	903 727	767 553	-136 174	-15,1%	53%
Összesen	407 665	357 948	-49 717	-12,2%	100%	1 600 917	1 492 021	1 382 680	1 587 187	1 439 371	-147 816	-9,3%	100%

15. ábra: 112 hívásfogadó központok statisztikája[26]

2.4. Az ITS Ökoszisztéma kialakítása

A közlekedés önmagában is jelentős veszélyeket hordoz, és frusztrációt vált ki mindenkiből, aki részt vesz benne. A tapasztalataink a közlekedéssel ambivalensek. Az a cél, hogy elérjük, hogy tudatosabban nézzünk szembe a tényekkel és a lehetőségekkel. Magyarország számára nyitott a lehetőség, hogy ezen a területen példaértékű megoldások kialakításában vegyen részt.

A KTI Közlekedéstudományi Intézet hivatott arra, hogy a felsőoktatással és más tudományos műhelyekkel együttműködve olyan modelleket dolgozzon ki, amelyek jelentősen képesek lesznek javítani azt a közlekedési modellt, amelyben most élünk, és megtalálja azokat a lehetőségeket és módszereket, amelyeket a társadalommal el is lehet fogadtatni.

Azt szeretnénk fölvázolni, hogyan lehet átvinni a mai világunkat, amiben most élünk, abba a világba, amit mindenki tud vagy sejteni vél, hogy milyen lesz pl. 30 év múlva. Ma már mindenki letenné a nagy esküt, hogy csak önvezető elektromos autók vagy akár drónok lesznek az egész Földön. Valóban nagyon komoly erőfeszítéseket tesznek kutatóintézetek, illetve cégek, államok is arra, hogy az önvezető autó mint lehetőség minél előbb előálljon, de van egy nagyon komoly balansz, a jelenlegi elterjedt járműpark és a kialakult szokások, amit át kell vinni, át kell tudni alakítani az idealizált jövőbeli világunkhoz, és a két világnak valahogy együtt kell tudni élnie az átmeneti időszakban.

Az átmenet kérdései

Ma még többségben vannak azok, akik megélték, hogy a lovas kocsik, amelyek a faluhelyen és kisebb városokban is elég gyakori közlekedési eszközök voltak, hirtelen eltűntek, és helyettük gépjárművek lettek. Ekkor magában a közlekedésben egy nagyon komoly drasztikus átalakulás következett be. Az tény, hogy a második világháborúban a logisztikának a 70%-a még lóvontatású volt. Abban a korban a kerékgyártó mesterek által a társadalmilag magas presztízsen lévő szakmunkára hirtelen nem volt igény. Tulajdonképpen ez a fajta nagyon durva átalakulás most megint be fog következni. A közlekedést teljesen másképp kell majd kezelnünk. Rengeteg olyan videót láthatunk a YouTube-csatornákon, ahol bizonyos szinten önvezető járművek közlekednek. Azonban nem lehet látni olyan felvételeket, ahol valós forgalmi környezetben láthatnánk előzést kétirányú útszakaszon. Nagyon komoly feladvány ma még egy valós forgalomban az önvezető járműveknek a körforgalmakat bevenniük. Valós forgalomban az önvezető autóknak még az egyik legnagyobb hibájuk, hogy az ember számára nem bonyolult dolgokat nem tudnak teljesíteni. Ezzel szemben egy másik megközelítéssel is találkozhatunk, főleg az ázsiai országokban terjedtek el a totális megfigyelésen alapuló közlekedésirányítási rendszerek, így pl. a 8,5 millió lakosú Csingtaoban, Kínában, ahol a forgalmat 900 ezer okoskamera figyeli meg, és a képek feldolgozásával komplex városirányítási rendszer jött létre.

[26] Statisztikai adatok a hívásfogadó központok tevékenységéről http://www.police.hu/sites/default/files/%C3%9Cgyelet%20SK%202019.%2004.pdf

16. ábra: A csingtaoi városirányítási rendszer modellkörnyezete

Tagadhatatlan tény, hogy ez a „nagy testvér” megközelítés nem tűnik az európaiak számára elfogadhatónak, ennek ellenére Európában is találunk hasonló rendszereket, pl. Londonban.[27] Forgalomfigyelő, térfigyelő kamerák: bár a dedikált, pici szenzorokhoz képest egy kamera jóval komplexebb eszköz, alapvetően a kamerák is érzékelőegységek, és ezáltal az érzékelési infrastruktúra részei. Az okos városokban elhelyezett kamerákat számos különböző célra használhatjuk: érzékelhetik a forgalmi viszonyokat az útkereszteződésekben, végezhetnek forgalomszámlálást, számolhatják a szabad parkolóhelyeket, és persze nyilvánvalóan biztonsági célt is szolgálhatnak.

Az első megközelítés alapja, hogy maguk a járművek lesznek nagyon okosak, egyre inkább képesek lesznek a helyi mesterséges intelligencia segítségével, helyi és az úthálózati szenzorokra, helyben meghozott döntésekre támaszkodva egész jól elboldogulni a világban. A másik oldalon pedig egy teljesen kontrollált környezettel láttunk, a megfigyelési adatok alapján központi mesterséges intelligencia felügyel mindent, és ez gondoskodik arról, hogy a közlekedés mindenkinek harmonikusan és lehetőleg folyamatosan optimalizáltan tudjon menni. Ahhoz, hogy a közlekedés egészének az átalakulása mindenki számára elfogadható legyen, valahol a megoldás e kettő véglet között lesz. Célunk, hogy ezt a lehetőséget megmutassuk.

Az ITS Ökoszisztéma kialakítás fő hajtóereje a közlekedésbiztonság javítása

Bemutatjuk, hogy mit kell tennünk, hogy kialakuljon, és kiberbiztonsági szempontból is kellően ellenálló rendszert sikerüljön létrehozni. Egy olyan közlekedési modellt kell felhasználni, ahol az alapvető személyes adatvédelmi szempontjaink is egy időben teljesülhetnek. Ez a kérdés több országban nagyon élénken foglalkoztatja az embereket. Látszik, hogy hamarosan meg kell ezt a kérdést

[27] https://infostart.hu/eletmod/2019/09/20/europa-legjobb-bekamerazott-varosai-budapest-az-elmezonyben

oldani, mert a közlekedés eddig is veszélyes üzem volt, de az újabb kihívások jelentősen növelték a már meglévő kockázatot. A biztosítási szektor felől is komoly elvárás, hogy szülessenek olyan megoldások, amelyek akár új alapokra is tudják helyezni a közlekedésbiztonságot.[28]

A legnagyobb változás lehetőségét igazából a távközlés, illetve az infokommunikáció fejlődése teremtheti meg, mert nagyon sok új lehetőséget hozhat majd az 5G hálózat kialakulása, amely megváltoztathatja a közlekedést is, ezen kívül az ipart, az egészségügyet és szinte az egész életünket átformálhatja.

A közlekedés globális átalakulását el tudjuk képzelni úgy is, ahogy „connected car" módon egymással fognak kommunikálni majd a járművek. Ez nagyon sok problémát vet fel. Például, ha sorozatban egymással kommunikáló járműveken megy keresztül az információ, és ebben a kommunikációs láncolatban valamelyik hibázik, akkor a végén ki lesz a felelős? Lehetséges felelős lehet az autó fejlesztője, gyártója, az autó szoftverének az előállítója, forgalmazója, a tanúsító szervezetek, a kommunikációs hálózat üzemeltetői stb. Ebből is látszik, hogy a felelősség kérdése önmagában nagyon problémás, és nagyon komoly fejlesztések zajlanak ennek érdekében. Nagyon fontos, hogy ne csak a jövőbeli technológiai szempontból vizsgáljuk meg ezt a kérdést, hanem a jelenlegi helyzettel és annak a társadalmi vetületével is foglalkozni kell, végig kell gondolni a változtatás humán oldalát is. Ezt a kérdést jobban fogjuk érinteni, mert az emberi tényező az, ami igazából fontos. Ismert mondás, hogy a mérnök bármit képes megcsinálni, hogyha megbízást kap. Nyilvánvaló, hogy előbb találjuk ki azt, hogy milyen legyen az az üzleti modell, mi legyen az az üzleti elvárás, az a hasznosság, ami alapján létre fogjuk tudni hozni az új, biztonságos átmenetet garantáló modellt. Nagyon fontos, hogy ez találkozzon a felhasználók (szinte minden embert ide lehet sorolni) várakozásával, illetve legyen számukra elfogadható.

Az első fő kérdés a bizalom. Mikor fogunk megbízni egy olyan járműben, amelyet algoritmusok, vagyis számítógépek vezetnek? Megbízhatunk-e egyáltalán ezekben?

A másik kérdés maga az átmenet kérdése. A mai tapasztalataink alapján nagyon nehéz elképzelnünk, hogy ez a két világ, ez a két nagyon különböző világ, ahol az egyik járművet ember, a másik járművet számítógép vezeti, egyszerre, egy úton tudjon közlekedni, egymástól fizikailag nem elkülönített pályán.

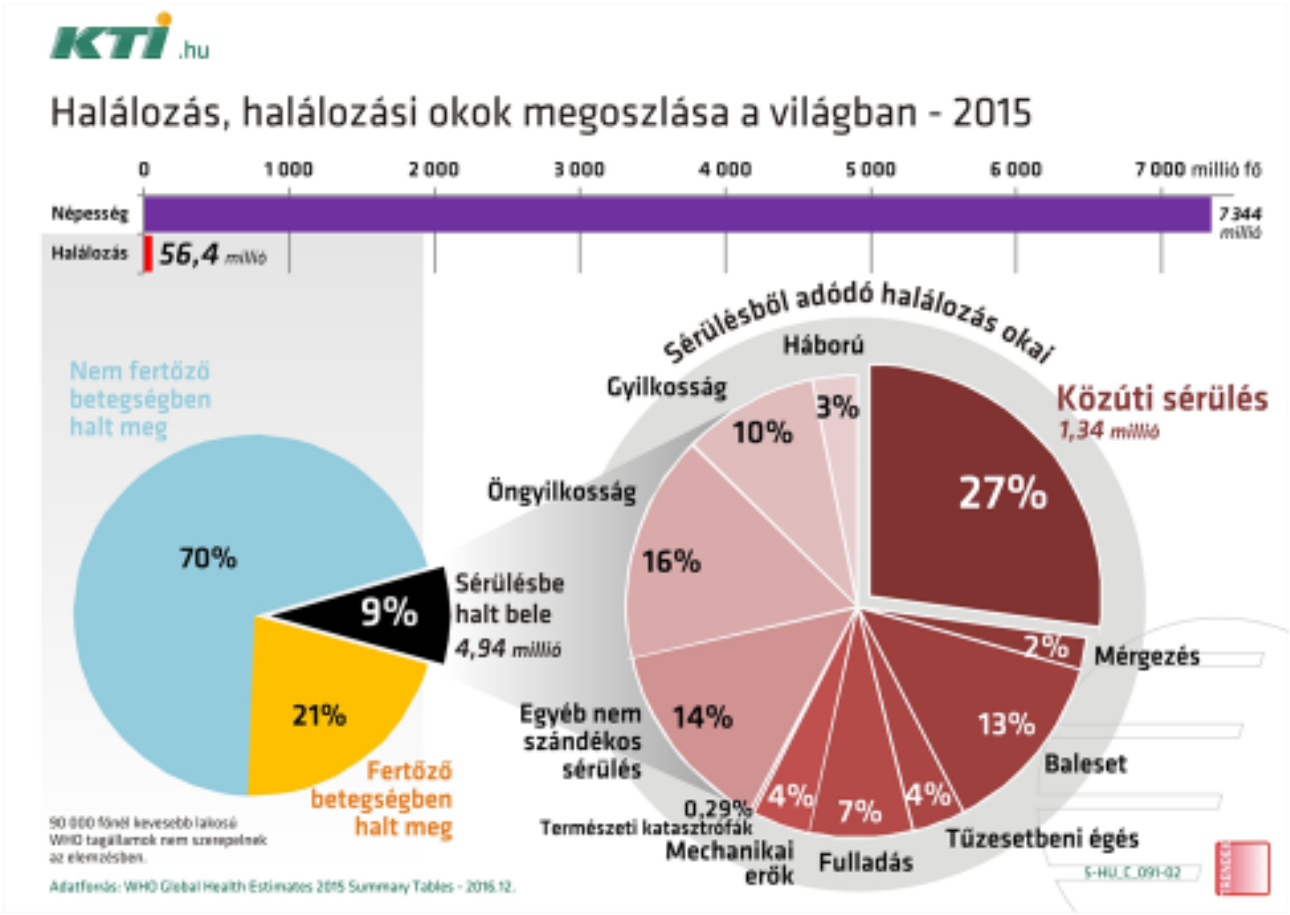
Belátható, hogy itt nagyon komoly kihívással állunk szemben, mi magunk, az egész emberiség. Természetesen nagyon komoly fejlesztések vannak, és komoly víziókat, illetve fejlesztési modelleket lehet látni, a világkiállítások során meg lehet ezeket csodálni. Felvetődik a kérdés, hogy ez mennyire a ma kérdése, és a jövőbeli ideális világ, az idealisztikus világ kialakítása-e a legnagyobb probléma, amivel szembe kell manapság néznünk. A valóság még nem ez. A mai valóságunkra az jellemző, hogy emberek halnak meg, sérülnek meg az utakon a balesetek következtében, és az egyik ember a másik embernek nagyon komoly sérülést vagy kárt tud okozni. Mindenki fel tud idézni olyan esetet, amelyben autók vagy más járművek ütköztek, és akár több ember is meghalt ott helyben. Sajnos ilyen eset nagyon sok van. A balesetek velünk vannak, és mindannyian ki vagyunk téve ennek ebből a szempontból. Tegyük fel a kérdést! Miért kell ennek így lennie? Egyszerűen elfogadhatatlan az a helyzet, az a társadalmi és egyéni veszteség, ami Európában és az egész világon van. Éves szinten átlagosan 25 ezer ember hal meg Európában nagyon sok év óta a közlekedési balesetek folyományaképpen. Magyarországon évente 5-600 fő hal meg az utakon, átlagosan 5 ezer ember szenved súlyos sérülést szenved, illetve kb. 15 ezer a könnyebb személyi sérülések száma. A KSH hivatalos baleseti adatai és a KTI becslési módszertana[29] alapján évente meghaladja a 600 milliárd forintot a személyi sérüléssel járó karambolokban elhunyt, illetve súlyosan vagy könnyen megsérült személyekkel kapcsolatos társadalmi kár. Éves szinten nagyságrendileg 200 ezer olyan közlekedési esemény történik, amely a biztosítókra tartozik valamilyen szinten. Ezekből a számokból is látszik, hogy a közlekedés

[28] Ki felel, ha a fejedre esik egy drón, vagy elüt egy önvezető autó? https://www.napi.hu/nemzetkozi_gazdasag/onvezeto-auto-dron-szabalyozas.700924.html

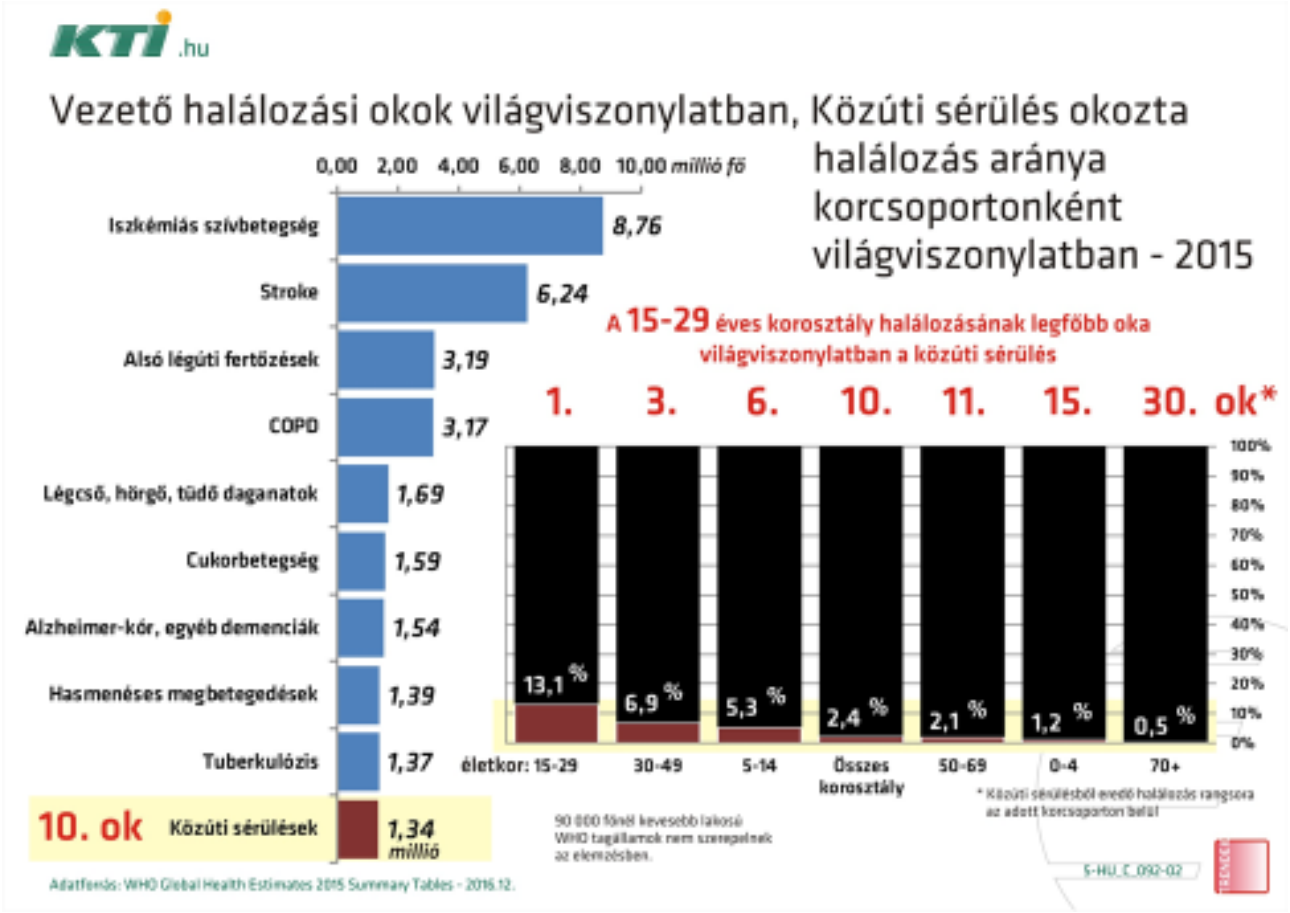
[29] http://kozlekedesbiztonsag.kti.hu/kozuti-baleseti-vesztesegek-aktualizalasa/

egy nagyon veszélyes üzem, és sajnos az emberek nem igazán élik meg ezt tudatosan, pedig sokkal felelősségteljesebben kellene közlekednünk.

Másként tekintve a kérdést, a statisztikák szerint minden tizedik elhalálozásért (17. ábra) a közlekedés okolható, a 15 és 29 éves korosztálynál ez az első halálok (18. ábra). Azok között, akik ebben a korosztályban meghalnak, nagyon nagy valószínűséggel közlekedési baleset áldozatai. A statisztikák a dokumentált balesetekről szólnak.



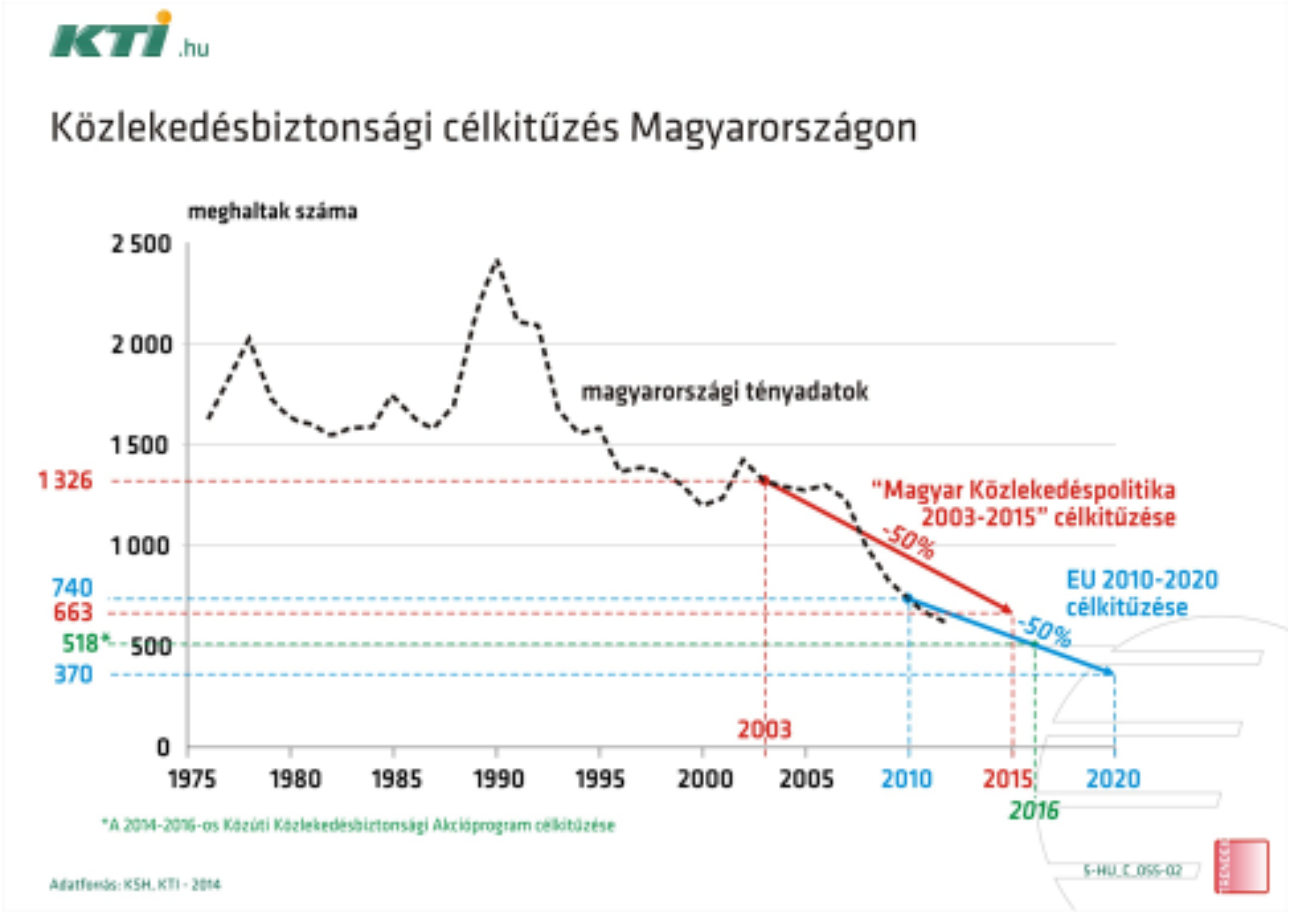
17. ábra: Halálozási okok



18. ábra: A 10. halálok

Nagyon sok olyan szituációval találkozhatunk a közlekedés során, amely nem dokumentált, és mégis jelentősen rongálhatja az egészségünket, pl. azzal, hogy fölösleges stresszt okoz számunkra. Ezek lehetnek az indokolatlan torlódások, a dugók és más kellemetlen közlekedési szituációk, amelyek miatt idegesek vagyunk, mert nem érünk el valahová időre. Rengeteg olyan problémával találkozhatunk folyamatosan a közlekedés során, amelyek megélése is nagyon komoly mindennapi frusztrációt okoz mindannyiunk számára. Ez hatását tekintve lassan ölő méreg a társadalom számára.

Minden kormányzat felismerte már ezt, és mindenhol, nem csak nálunk, törekednek arra, hogy biztonságosabb legyen a közlekedés. Japánban már 2005-ben megfogalmaztak egy nagy álmot, hogy 2020-ra elérik, hogy 0 legyen az országban a közlekedésből kifolyólag bekövetkezett haláleset. Magyarországnak (19. ábra) és az EU-nak is vannak hasonló célkitűzései. Sajnos, ezek nem valószínű, hogy így fognak teljesülni. Majd az év végére kiderül, hogyan alakul a statisztika. Lehet, hogy a pandémiahelyzet következtében javulni fog, de az már most is egyre inkább látszik, hogy sokkal hatásosabb intézkedéseket kell hozni ahhoz, hogy ez a helyzet érdemben megváltozzon.



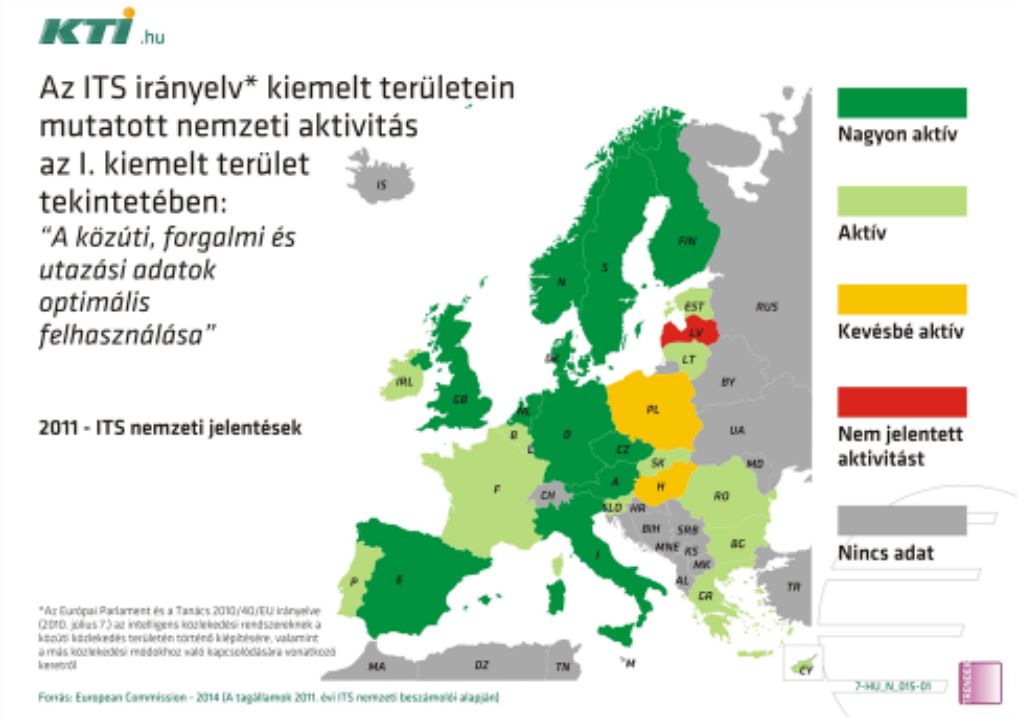
19. ábra: Közlekedésbiztonsági célkitűzések

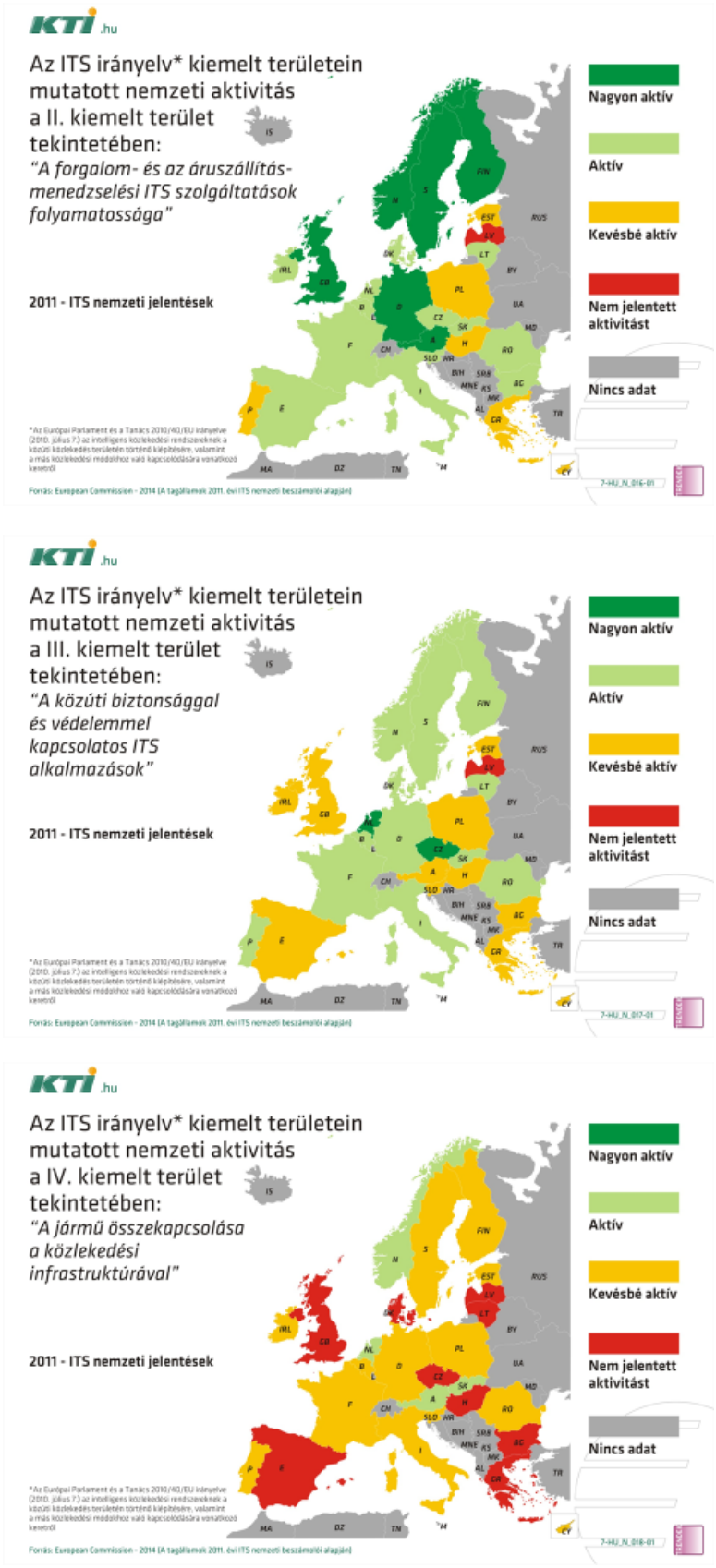
Az ITS Ökoszisztéma modell előzményei

A közlekedés fejlesztésénél már nagyon sok intelligens közlekedési rendszerrel és megoldással találkozhatunk, azonban ezek szigetszerű megoldásoknak tekinthetők. Ezekről ez a 2012-es állapotokat tükröző 20. ábra nagyon sok dolgot megjósol, sok minden ezek közül már meg is valósult, a követő távolságtartó tempomattól kezdve a flottakövetésig, a globális navigációig és így tovább, tehát a közlekedés során rengeteg adatot tudunk előállítani, és rengeteg célrendszerünk van. A gond alapvetően az, hogy ezek az adatok nem állnak össze egy komplex ökoszisztémává, a közlekedés egésze nem alkot egységes rendszert adatstruktúra és informatikai szempontból.

20. ábra: ETSI–2012

Az ITS-sel már nagyon régóta foglalkozik az Európai Unió, 2008-ban kezdték el az ITS-irányelvet kidolgozni, 2010-es ez az irányelv. Amennyiben a 21. ábrán a színeket nem nézzük, csak igazából már nem is mutatják pontosan a valóságot, egy tanulság van benne, hogy az Európai Unió nem igazán tudta elérni azt, hogy egységes rendszerek alakuljanak ki EU-n belül.





21. ábra: Az ITS Irányelv I–IV. kiemelt területei

Kis túlzással azt mondhatjuk, hogy ahány ország, annyi féle ITS-rendszer alakult ki, vagy országcsoportonként alakulnak ki hasonló kezdeményezések, de igazából nincsen közös kényszerítő erő, mert az ITS Irányelv alapjaiban csak egy ajánlás. Vannak benne részben olyan kötelező elemek, amelyeket végre kell vagy kellett már hajtania minden országnak, Magyarországon is már lassan több minden megvalósul a kötelező elemekből, de igazából összességében nem fogalmaztak meg olyan átfogó elképzelést, követelményt, ami az egységes adatterek irányába hatna.

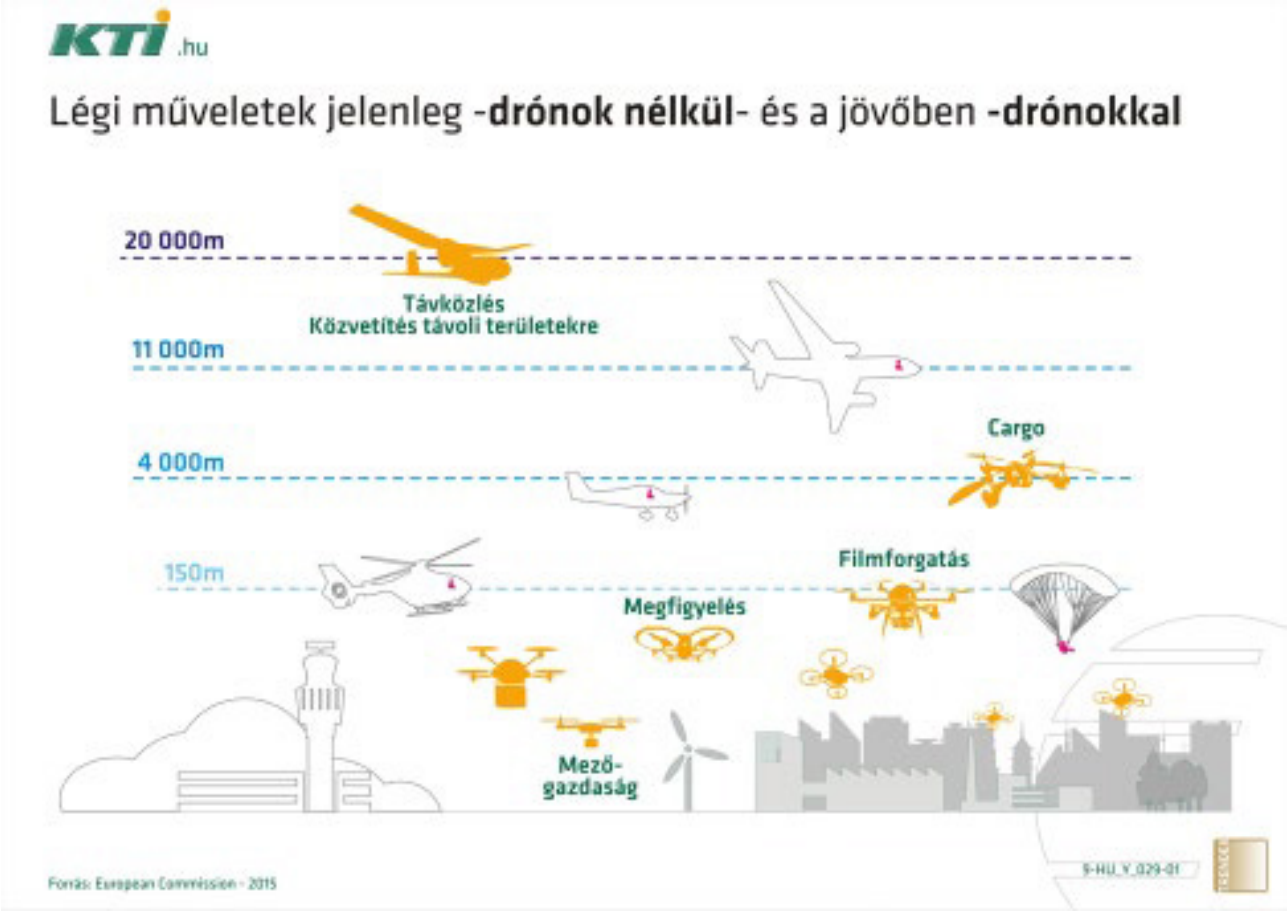
Szintén fontos szempont, hogy a járművek száma lineárisan növekszik, egyre több jármű közlekedik az útjainkon, az EU és Magyarország (22. ábra) szintjén is. A meglévő közlekedési infrastruktúrának egyre több járművet kell tudnia kiszolgálnia.

22. ábra: A gépjárművek száma

A technológiai fejlődés eredményeként megjelent egy újabb kihívó szereplő (23. ábra) is a közlekedés egészét tekintve. Új közlekedési formák, pl. a drónok szintén helyet kérnek maguknak a közlekedés bizonyos szegmensében. Egyre világosabban látszik, hogy a drónok alkalmazása önmagában is komoly lehetőségeket rejt, illetve számos előnyt is nyújt a többi közlekedés számára, vagy éppen komoly kihívásokat fog jelenteni. Számos hír volt azzal kapcsolatban, hogy nemzetközi repülőteret kellett leállítani huzamosabb időre drónok okozta problémák miatt.[30] Jogosan tartunk tőle, hogy egyszer akár a polgári életben is valami nagyobb probléma bekövetkezhet, és akkor már nagyon égetővé fog válni a kérdés megoldása. A pilóta nélküli rendszerekkel (UAV, drón) végzett műveletekre vonatkozó szabályokról és eljárásokról szóló (EU) 2019/947 végrehajtási rendelet (továbbiakban: EU rendelet) 2020. 07. 01-én lépett hatályba, ami új alapokra helyezte az ezekkel az eszközökkel való tevékenységek végzését. Egyre inkább igény jelentkezik a drónok felhasználására az egészségügyben,

30 http://iho.hu/hir/dron-sorozat-ferihegyen-szerdan-is-volt-leallas-191016

a mezőgazdaságban vagy akár az ipari és biztonsági megoldásoknál. A pandémiahelyzet is, újabb kihívásként, fokozott igényt kelt ezen megoldások legális használatára. Elemi erővel jelenik meg egy szélesebb kör, elsősorban a hobbi- és rekreációs felhasználók, továbbá a kereskedelmi célú felhasználás, amely EU szabályozási keretek között valósul majd meg. Figyelembe kell venni, hogy az UAV-k kontrolálhatatlan felhasználása nemzetbiztonsági[31] kockázatot[32] is jelent,[33] így az UAV-k esetében a cél kialakítani egy olyan rendszert, hogy a mozgásuk és a felhasználási tevékenységük „látható", kontrolálható legyen, és minden eszközhöz felhasználása során egyértelműen felelős személy legyen rendelhető letagadhatatlan módon. Szükségképpen cél, hogy ez a megoldás, a felelősség megállapításán kívül, növelje a jogkövető magatartást az üzembentartók és a távpilóták részéről.



23. ábra: Új szereplők: a drónok

Nem kerülhető meg a kérdés, hogy a közlekedésben használatos ITS-rendszereknél az IT- és információbiztonsági kérdésekkel is érdemben foglalkozni kell. Az információbiztonság tulajdonképpen három alapvető dologgal foglalkozik: az adatoknak bizalmassága, sértetlensége és a rendelkezésre állás, és mindennek van egy olyan felhasználó szempontú megközelítése, amely magának a személyes adatoknak a védelmét jelenti.

Amennyiben ebből a szempontból megvizsgáljuk a közlekedésben kialakult ITS-rendszereket, azt vehetjük észre, hogy vannak olyan igen nagy rendszerek, ahol az adatok igazából nincsenek megfelelően kezelve, vagy nem is állnak rendelkezésre, vagy IT-biztonsági vagy információbiztonsági szempontból nem állnak össze egy védhető és garantálható megbízhatósággal működő rendszerré.

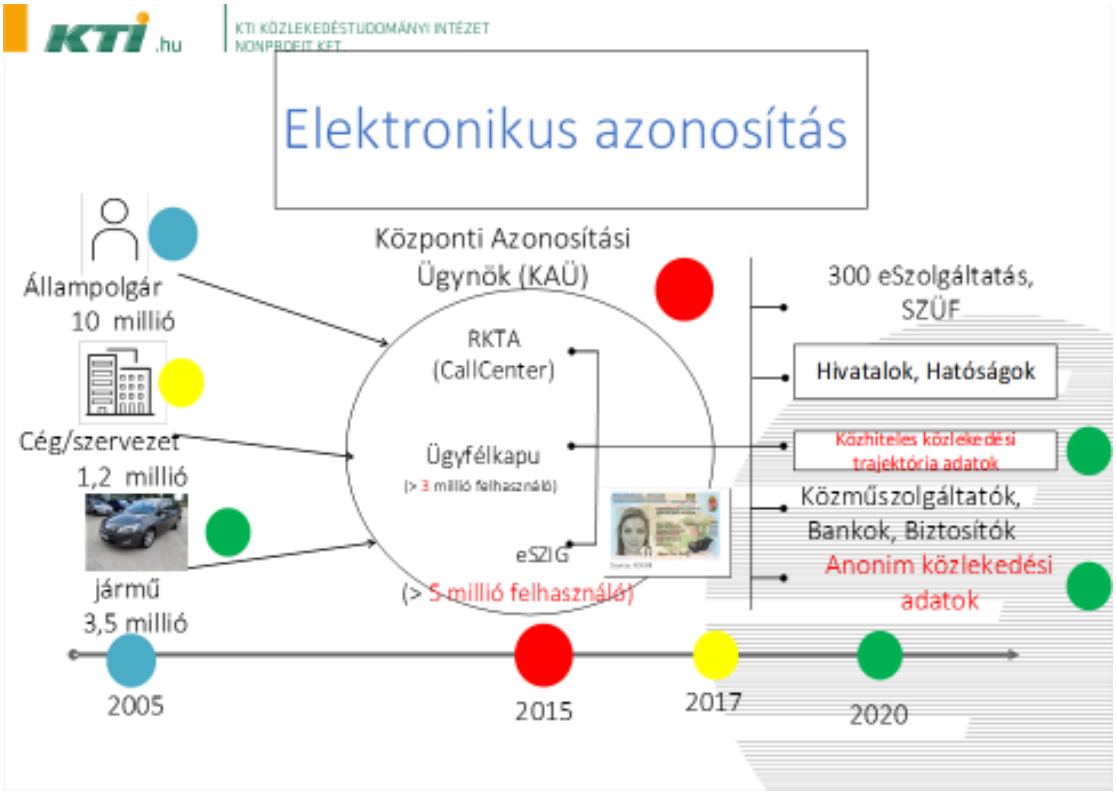
31 https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKI_Elemz%C3%A9sek_2019_21_A_kozel-keleti_dronproliferacio_eszkalacios_kockazata-(Etl%20A.%20-%20Penzvalto_N).pdf

32 https://24.hu/kulfold/2018/07/03/dront-reptetett-a-greenpeace-egy-francia-atomeromube/

33 https://g7.hu/vilag/20190916/nehany-dronnal-szetbombaztak-a-koolaj-vilagpiacat/

2.4.1. Az ITS Ökoszisztéma modell alkotása

Manapság, ha autóval elmegyünk A-ból B-be, csak abban az esetben keletkezik közhitelesnek tekinthető adat erről az utazásról, ha a közlekedésrendészet valamelyik rendszere gyorshajtásunkról vagy valamilyen más jellegű szabálytalanságunkról felvételt készít. A tehergépjárművek tachográfokkal történő hiteles nyomkövetését az Európai Unió – kötelező jelleggel – már 2005-től bevezettette. Ezen kívül elterjedtek egyéb járműkövető rendszerek is, amelyek jellemzően csak flotta szinten szervezettek, amelyben mindenki csak a saját adatát méri és gyűjti, ezért nem állhat össze egy összefüggő adatstruktúra. A Közlekedéstudományi Intézetben az ITS Ökoszisztémával foglalkozó munkacsoport egy olyan globális rendszer kialakítását javasolja, amely egységes követő rendszerként fog viselkedni. Elképzelésünk szerint minden járműre rákerül egy egységes duális nyomkövető eszköz, amely kétféle módon rögzíti a járművek által megtett pálya hely-, sebesség- és időadatait. Ennek az eszköznek a segítségével egyrészt a járműért felelős személy (járművezető vagy üzemben tartó) elektronikus személyigazolványával összerendelt titkosított adat, másrészt összerendelés nélküli közadat keletkezik. A kettős adatgyűjtés lehetővé teszi a személyes adataink védelmét is, mivel az eSZIG-hez kapcsolt adatok titkosítottan és a személyhez rendelten kerülnek rögzítésre (hasonlóan a banki adatkezeléshez). Ebben az esetben titkosítva tartalmazza a járműért felelős személy eID-jához kapcsoltan gyűjtött adatokat, amivel közhiteles módon lehet szükség esetén bizonyítani a személyi felelősséget. A GDPR szerint ezeknek az adatoknak garantálni kell a védelmét. Amennyiben meg kell állapítani a személyi felelősséget – pl. egy cserbenhagyásos gázolás esetén –, hatósági eljárás keretében lesznek felhasználhatók az adatok. Ezért el kell érni jogszabálymódosítással, hogy ez egy hatósági eszköz legyen, amely koncepcionálisan a digitális rendszámtábla bevezetését jelenti. Jogilag ugyanolyan védelme lenne, mint a jelenlegi rendszámtáblának vagy a hatósági lajstromszámnak. A rendszámtáblát sem lehet meghamisítani, nem lehet letakarni vagy eltávolítani, hatósági oldalról kell büntetni az ez irányú visszaélést. Az általunk elképzelt rendszerrel szemben lényeges elvárás lenne, hogy ne csak a létrehozás pillanatában, hanem a teljes életciklusára kiterjedően feleljen meg az auditelvárásoknak.



24. ábra: Elektronikus azonosítás kapcsolódása
Forrás: saját ábra

Az összerendelés nélküli közadatokból – amikor elválasztjuk a felelős eID-ját a mért adatoktól – matematikai értelemben egy olyan digitális teret hozhatunk létre, amely egy metrikus térként fog a továbbiakban viselkedni. Amennyiben az összes jármű közadatát össze tudjuk gyűjteni megfelelő Big Data-elemzéssel és MI (Mesterséges Intelligencia) felhasználással, minden súlyos deviancia könnyen kiszűrhető lesz. Gondoljunk olyan esetekre pl., ha valaki ellenkező irányból hajt föl egy autópályára, vagy ha az autópályán torlódás van, és valaki a leállósávon nagy sebességgel „elsuhan" a többiek mellett, ezek is könnyen észlelhetők és azonnal kiszűrhetők lesznek. Az anonimizált adatokból létrejövő metrikus teret neveztük el ITS Ökoszisztémának.

2.4.2. Az ITS Ökoszisztéma technikai kialakítása

Az egységes ITS Ökoszisztéma úgy lenne technikailag kialakítható, hogy minden, a közlekedés számára releváns mozgó és nem mozgó eszközön lenne egy hatóságilag kiadott, egyedi, integrált IoT-alapú GPS/GNSS-szenzor, amely egyben egy eIDAS szerint hitelesíthető chip is lenne. Az adatgyűjtést kezdetben NB[34] hálózaton vagy LoRa WAN[35] hálózaton vagy ezek kombinációjaként létrejövő, dedikált, államilag védett frekvencián lehetne megvalósítani. Ennek lenne rendszeres auditálási követelménye is, különös tekintettel az IT-biztonsági megfelelőségre, a rendszerek bizalmasságára, sérthetetlenségére és rendelkezésre állására a GDPR-elvárásoknak és -auditnak megfelelően. A kulcselem az eSZIG lenne, amely segítségével képesek lennénk a járművezetőket/üzembentartókat egyértelműen összerendelni a digitálisan rögzített adataikkal, titkosítottan, az EU-normáknak megfelelően, auditált módon. Az így létrejövő egységes ITS Ökoszisztéma kialakításának alapját a közlekedésben részt vevő mozgó – akár kiterjesztve a nem mozgó – eszközök folyamatosan mért, digitálisan tárolt, továbbított, védett, feldolgozott és szükség esetén közhitelesen tanúsított adatai adnák. Ezen kívül pozitív externália lenne a közlekedési eszközöket vezetők (objektív felelősség elve alapján az üzembentartók) tudatába beépülő felelősebb magatartás és ennek következtében a közlekedési szabályok fokozottabb betartása.

2.4.3. Az ITS ökoszisztéma elfogadása

Amennyiben ez a digitális transzformáció bekövetkezik, létrejön az ITS Ökoszisztéma, azaz az egész közlekedés digitalizálódni fog. Hogyan fogjuk megélni ezt a változást?

Valószínű, hogy rövid időn belül be fog épülni a hétköznapjainkba, mivel az emberek hamar képesek elfogadni a jelentős változásokat, amennyiben azok az egyénnek vagy a társadalomnak hasznosak. Eleinte szokatlan lesz számunkra, de előbb-utóbb el fogjuk fogadni, mert sokkal fegyelmezettebbé, hatékonyabbá és biztonságosabbá válik napról napra általa a közlekedés.

A legnagyobb eredmény, hogy drasztikusan csökkenni fog a balesetek száma. Hipotézisünk szerint elérhető lesz akár a zéró szint is. Nem fognak súlyos balesetek bekövetkezni emberi felelőtlenségből, mert alapjaiban megfontoltabban fognak az emberek vezetni, ugyanis a baleseti körülmények vizsgálata minden esetben közhiteles módon bizonyítható lesz.

Az ITS Ökoszisztémát tekinthetjük a közlekedés egészéhez rendelt speciális biztonsági lognak,

[34] A Low Power Wide Area (LPWA) technológia és a Narrow Band IoT (NB-IoT) az egyik legizgalmasabb témakörök egyikének tekinthető az Internet of Things – M2M kommunikáció témakörén belül. Az elemzők szerint 2023-ig körülbelül 3 milliárd LPWA-eszköz hálózatra kapcsolódása várható világszerte. Az olcsó, alacsony energiaigényű NB-IoT-megoldás nagy területi lefedettséget és hatékony beltéri használatot kínál a felhasználók számára.

[35] A LoRaWAN-technológia egyik legnagyobb előnye annak rendkívüli energiahatékonyságában rejlik, kiemelkedik egyszerűségével, rugalmasságával, nagyszámú csatlakozási lehetőséget kínálva a külvilág felé.

amely a közlekedés folyamatának az utólagos bizonyíthatóságát, valamint a dinamikus menedzselését egyidejűleg elő tudja majd segíteni. Ez a folyamatos kontroll be fog épülni az emberek várakozásaiba, mint ahogy beépültek a korábban szinte elképzelhetetlennek tűnő hasonló korlátozó intézkedések. Legjobb példa erre a dohányzási szokásnak és magának a dohányzáshoz kapcsolódó társadalmi attitűdnek a megváltozása. Ma már hihetetlennek és ambivalensnek tűnik számunkra egy olyan régi film, amelyben a szereplők dohányoznak az éttermekben, a vonaton, a repülőn vagy bármely zárt térben. Kevesebb mint húsz éve még ilyen világban éltünk. A dohányzás visszaszorítása sok pozitív eredménnyel járt. Azonban voltak, akiket negatívan érintettek ezek az intézkedések, pl. akik a dohánytermékek előállításából éltek. Számukra hátrányos volt ez az átalakulási kényszer, ugyanakkor az intézkedés társadalmi haszna sokkal jelentősebb lett, mivel növekedett a születéskor várható életkor, és az egészségtudatos életvitel szemléletmód is fontossá vált.

2.4.4. Az ITS Ökoszisztéma negatív hatásai

Bizonyára lesznek a közlekedésben kialakítandó teljes kontrollrendszernek negatív következményei is. Változtatnunk kell a kialakult közlekedési beidegződéseken, ezt a változást el kell tudnunk viselni annak érdekében, hogy a közlekedés „veszélyes üzem" jellegét jelentősen csillapítani tudjuk. Ezen kívül el kell fogadnunk, hogy folyamatosan képződik egy újabb „digitális lábnyomunk". Az egész közlekedésünk is hasonlóvá válik azokhoz a tevékenységekhez, amelyekről már most is folyamatosan képződik digitális lenyomat. Nem csak ökológiai értelemben van lábnyomunk, hanem digitális értelemben is. Pl. a mobiltelefon használatáról és mozgásáról, a banki átutalásokról, minden egyes elküldött e-mailről vagy akár egy szimpla keresésről is digitális lenyomat képződik. Ez manapság már megszokott dolog. A járműveink közhiteles követése is ebbe a kategóriába fog kerülni. Ilyen digitalizált világban élünk, digitális nyomokat hagyunk magunk után, és ezek a digitális nyomok gyűjthetők, felhasználhatók. Nem kell ettől megijednünk, hanem inkább tudatosan, a jogszabályi garanciákkal együtt kell ezeket a lehetőségeket a biztonságunk növelésére felhasználni.

2.4.5. Az ITS Ökoszisztéma pozitív hatásai

Ezzel szemben nézzük meg, hogy miért érdemes létrehozni ezt a rendszert. Vegyük sorra a várható előnyöket néhány eseten keresztül.

A relatív gyorshajtás, illetve nem az út- és forgalmi viszonyoknak megfelelő sebesség megválasztása kimutathatóvá válik. Pl. gyakori baleseti szituáció, hogy valaki az autópályán a belső sávban 130 km/h sebességgel halad, és a külső sávban a 90 km/h sebességgel haladó jármű hirtelen kivág elé, mivel előzi az előtte haladó kamiont. Ennek következtében egy ráfutásos baleseti szituáció alakul ki, amelyet nehéz a jelenlegi kontrollrendszereinkkel bizonyítani.

Egy településen belül lehet, hogy a közlekedési tábla megengedi az 50 km/h sebességgel való haladást, ugyanakkor mindenki 40 km/h-val halad valamilyen okból. Aki 50 km/h-val megy, relatív gyorshajtást követ el, és valószínűleg ebből kritikus közlekedési probléma is keletkezhet.

A legfontosabb következmény, hogy az összes járműmozgás adatainak lenyomata titkosítottan tárolásra kerül, ebből a teljes lenyomatból bármilyen eseménysorozat rekonstruálhatóvá válik. Az EU jogszabályi megfelelősségi garanciák biztosítják, hogy csak akkor lehessen ezekhez az adatokhoz hozzáférni, amennyiben hatóságilag indokolt. A közlekedők számára a törvény teljes körű védelmet biztosít azáltal, hogy a hatóság csak indokolt esetben és csak dokumentáltan férhet hozzá az adatokhoz.

Van egy további előnye is, ez az objektív bizonyíthatóság lehetősége. Közismert, hogy mint üzembentartók objektíve felelősek vagyunk a tulajdonunkban levő járműért. Ez azt jelenti, hogy

amennyiben a jármű elkövet valamilyen szabálytalanságot – az objektív felelősség elve alapján –, az üzembentartó vonható felelősségre. Például a VÉDA rendszer tévesen mér be gyorshajtást, akkor az üzembentartó automatikusan megkapja a büntetést, és neki kell bizonyítania, hogy a járműve nem is járt azon a területen. Jelenleg erre nincs mód. Az ITS Ökoszisztéma megteremthet egy független, objektív bizonyíthatósági lehetőséget a közhiteles nyomkövetése által.

Nagyon kedvező hatás lehet az is, hogy ezzel a módszerrel el lehet tüntetni a forgalmi dugókat. Pl. ha a lámpák nem statikusan váltanának, hanem az ITS Ökoszisztéma adatai alapján igényvezérelt módon, akkor onnantól kezdve a forgalom dinamikájához alkalmazkodva, annak megfelelően lehetne a közlekedési lámpákat vezérelni, és ettől kezdve megnövekedne az áteresztő képessége a kereszteződéseknek. Ez adatszinten alapja lehetne egy olyan globális közlekedésirányítási rendszernek, amely minden zavar esetén dinamikusan – az MI (Mesterséges Intelligencia) és Big Data alapokon – képes lenne azonnal beavatkozni. Az egyének szempontjából a navigációs rendszerek is pontosabbá tehetők, mivel az összes jármű adatai alapján tudnak közlekedési tanácsokat adni.

Az ITS Ökoszisztéma eredményeként a közlekedési kapacitások jobb kihasználhatósága meg fog nőni, ha az infrastruktúra-tervezéseknél nemcsak a becsült adatokból, hanem valós és folyamatosan mért idősori adatok alapján lehet a változtatásokról szimulációkat kialakítani.

Ha az egész közlekedést jellemző dinamikus állapottereket megismerjük, azzal további lehetőségek nyílnak. A pontos forgalmi idősorokkal egyenletesebbé tehetjük a meglévő kapacitások kihasználását minden időpillanatban. Ilyen lehet, ha dinamikus útdíjarazással történő visszacsatolásokkal időben szét lehetne húzni a forgalmi terhelési csúcsokat. Ezzel el lehetne laposítani a csúcsterheléseket, és ezzel az egész közlekedést hatékonyabbá lehetne tenni. Olcsóbb lenne a közlekedés, ha a közlekedők árérzékenységét kihasználva a kevésbé kihasznált napszakokra terhelné át a forgalom jelentős részét.

Továbbá az egész úthálózat fizikai állapotáról folyamatosan pontos képünk lehetne (az útkopásokról, az elhasználódásokról, kezdeti hibákról, a valódi megtett úthasználatról).

A fejlesztések azt mutatják, hogy a V2X technológia révén a járművek és az infrastruktúra közötti kommunikáció is ki fog alakulni. Az ITS Ökoszisztéma ehhez az elképzeléshez egy viszonylag könnyen kialakítható átmeneti rendszert tud létrehozni, ami magában hordozza az egész közlekedés digitalizációjának lehetőségét. Kezdetben az önvezető és a nem önvezető világ közötti átmenet elősegítésére alakítjuk ki ezt a rendszert. A továbbiak során ez magával fog hozni egy olyan fejlődést, amely minden közlekedési módra ki fog terjedni, és ezzel a közlekedés optimalizálása a digitális térben fog zajlani. A valóságban pedig ezzel a fizikai közlekedési térben jelentősen megnöveljük a hatékonyságot és a közlekedésbiztonságot.

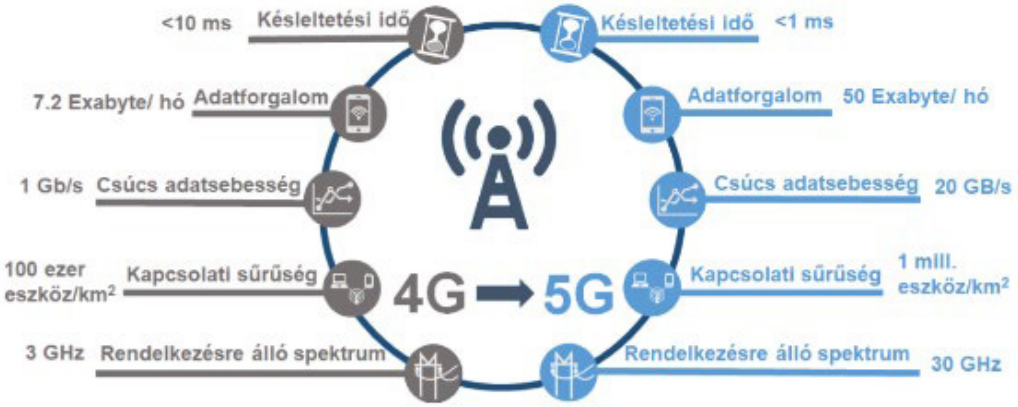
2.4.6. Az ITS Ökoszisztéma kiterjeszthetősége

Az absztrakciót tovább gondolva, nincs jelentősége annak, hogy autókról vagy bármilyen más járműről beszéljünk. Bele vehetjük ebbe a rendszerbe a drónokat, a paplanernyőket, a hajókat, a motorcsónakokat vagy akár a kerékpárokat is. Speciálisan akár a nem mozgó, statikus elemek elmozdulását vagy mozdulatlanságát is mérhetővé lehet tenni ezzel a módszerrel. Kialakulhat a közlekedésben szerepet kapó dolgok egyszerre közhiteles és publikus követhetősége duális módon és mindezt össze lehet szervezni egy komplex adatvezérelt ökoszisztémába. A duális követhetőség itt azt jelenti, hogy az egyik nézetben titkosított módon megvédjük az adat tulajdonosának a jogos érdekeit és evidenciáit, szigorúan védett biztonsági logot képezünk az adataiból. A másik nézetben az adatok másodlagos felhasználása kapcsán az adatvédelem érdekében az eredeti, az egyénhez kapcsolódó adatokat anonimizáljuk (és/vagy pszeudonimizáljuk). Az anonimizáció eljárás révén garantáltan megszüntetjük az összefüggést az azonosító adatkészlet és az érintett között. Ezzel a digitális ikerrendszerben lehetőségünk lesz a mesterséges intelligencia alkalmazásához elengedhetetlen adatokhoz való hozzáfé-

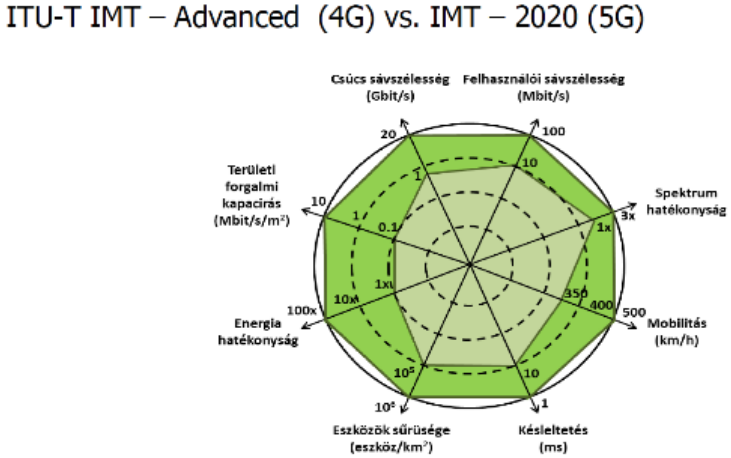
rés biztosítására. Az Európai Unió a jogszabályi háttér (FFD-rendelet és a GDPR) megteremtésével kívánja elősegíteni, hogy a mesterséges intelligenciára épülő megoldásokhoz, alkalmazásokhoz, fejlesztésekhez és a gépi tanuláshoz szükséges tömeges adatokhoz (Big Data) megfelelő keretek között lehessen hozzáférni. Az anonimizált adatok már nem tartoznak a GDPR hatálya alá, és a mesterséges intelligencia használatával a közlekedés egészének az adatelemzése egyszerűbbé, gyorsabbá és hatékonyabbá válik.

2.5. Az 5G hálózat kapcsolódása a közlekedéshez

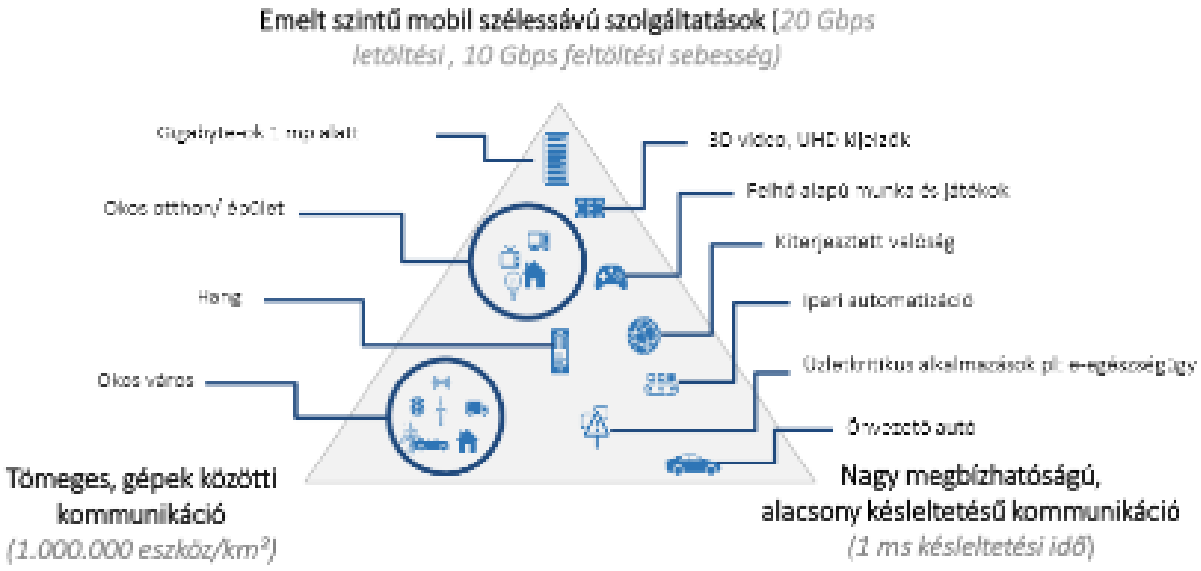
Az egész országra történő valódi 5G hálózati lefedettség kialakítása és annak különösen a közlekedésre kifejtett hatásának kérdései nagyon jelentősen befolyásolhatják Magyarország fejlődését az elkövetkező években. A jelenleg kiépült távközlési hálózati infrastruktúra felhasználása nem adhat megfelelő alapot jelentős változtatás nélkül arra, hogy teljes körű hálózati lefedettség tudjon kialakulni, mind a megfelelő kapacitású és késleltetésű adatátvitel, mind az aktív eszközök vonatkozásában az elektromos árammal történő ellátottság területén.



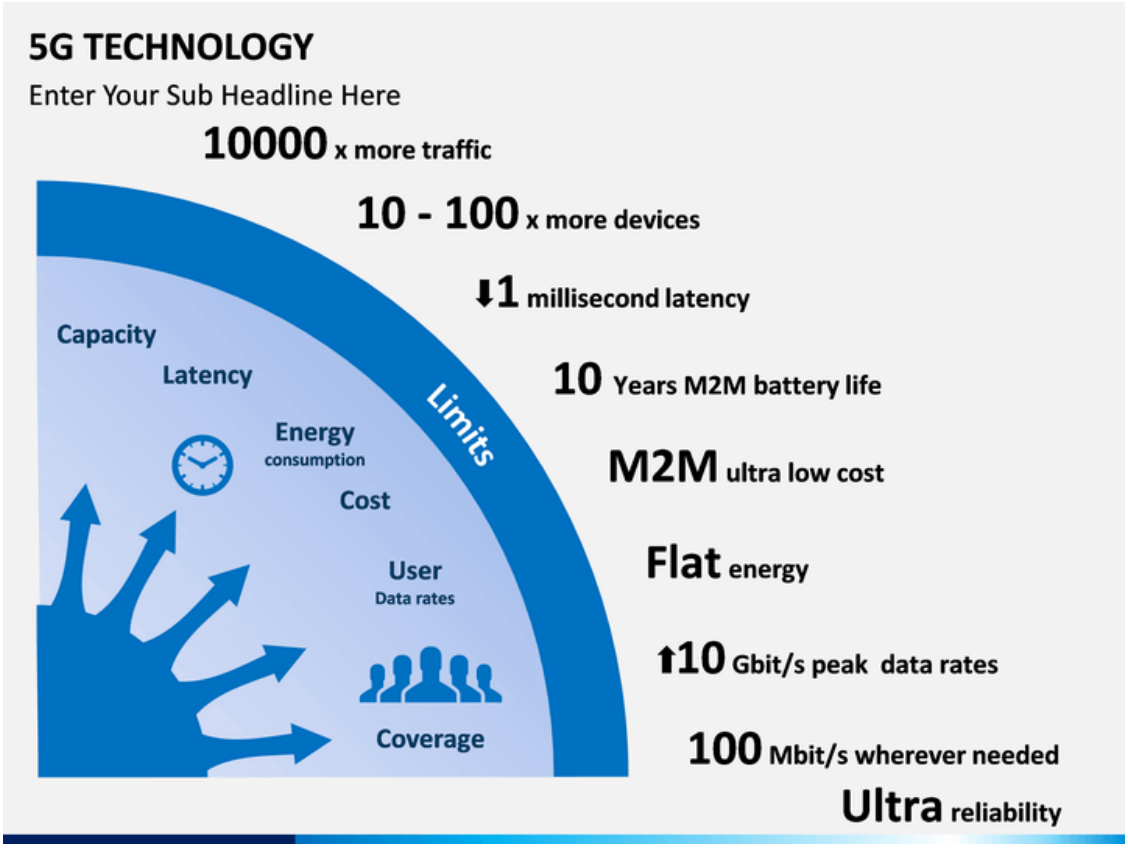
25. ábra: 4G és az 5G összehasonlítása
Forrás: 5G Magyar Mérnöki Kamara, továbbképzési anyag



26. ábra: Pókháló modell
Forrás: https://www.huawei.com/en/about-huawei/publications/communicate/80/up-in-the-air-with-5g



27. ábra: Az 5G hálózat felhasználhatósági modellje
Forrás: https://www.huawei.com/en/about-huawei/publications/communicate/80/up-in-the-air-with-5g



28. ábra: Felhasználási előnyök
Forrás: https://www.sketchbubble.com/en/presentation-5g-technology.html

2.5.1. Álhírek és kampány az 5G ellen a pandémiahelyzetet kihasználva

A közösségi médiában és a sajtótermékekben több hír számolt be a koronavírus-járvány és az 5G hálózat kapcsolatáról. Angliában és Hollandiában antennaszerelőket támadtak meg, és adótornyokat gyújtottak fel.

29. ábra: Az online média ráerősít az álhírekre
Forrás: index cikk https://index.hu/techtud/2020/04/17/koronavirus-5g-adotorony-sugarzas-osszeeskuves-elmelet/ link

Természetesen az 5G és a vírusjárvány közötti képzettársítás képtelenség,[36] nem lehet összepárosítani a biológiát egy technikai, kommunikációs eszközzel. Különösen érdekes lenne kideríteni, hogy kik állhatnak ezen akciók mögött valójában. Igen kellemetlen és hátráltató tényező az 5G-ellenes mozgalmak kibontakozása és túlságosan elnéző kezelése.

A mobilkommunikációt már 25 éve használjuk, és minden újabb generációváltásnál voltak olyanok, akik megpróbálták a tájékozatlanságot és az alaptalan emberi félelmeket kihasználva akadályozni a fejlődést. Tudjuk, hogy nem nagy a különbség az 5G és a korábbi generációs eszközök használata során megállapított hatásvizsgálat eredményei között. Konkrétan az 5G az alacsony és a közepes frekvenciasávokon terjed (24,25 GHz – 86 Ghz). E milliméteres hullámok miatt félnek a legtöbben, pedig ilyen hullámsávon működő eszközök már jó ideje használatban vannak, pl. a repülőtéri biztonsági szkennerektől az autók ütközéselkerülő és tolatóradarjáig. Ezeket már jóval az 5G előtt is sokféleképpen vizsgálták, és semmilyen egészségre káros hatást nem tudtak kimutatni. Az 5G-vel kapcsolatban is több szakmai világszervezet felügyeli azt, hogy minden szempontból megfeleljen a

[36] Generációváltás az infokommunikációban https://szon.hu/kozelet/helyi-kozelet/generaciovaltas-az-infokommunikacioban-3876453/

biztonságos egészségügyi normáknak, ilyen az ICNIRP[37] (International Commission on Non-Ionising Radiation Protection) és az IEEE-ICES (International Committee on Electromagnetic Safety). Az általuk meghatározott intervallumok jelentős plusz határértékkel is számolnak. Az eddigi vizsgálatok során nem találtak egyetlen olyan 5G-tulajdonságot sem, amely veszélyes lehetne az egészségre.

2.5.2. Az 5G hálózat kialakításának szükségessége

Az 5G technológia nem csak arról szól, hogy minél hatékonyabban lehessen videót letölteni vagy videókonferenciákon részt venni. A jövőben a sportközvetítéseknél eddig elképzelhetetlen minőségben látjuk majd pl. a focimeccseket a képernyőnkön, mintha ott lennénk a pályán. Az 5G elterjedését nagyon komoly gazdasági érdekek teszik szükségessé, és ez leginkább a negyedik ipari forradalomnak, rövidítve Ipar 4.0-nak az elterjedése miatt lesz fontos. Ez a távközlési fejlettségi szint elengedhetetlen a robotika, az önvezető autók, a virtuális valóság vagy a mesterséges intelligencia létrehozása és fejlesztése szempontjából, nem beszélve arról a sok milliárd egyéb IoT-eszközről, amelyek teljesen új alapokra fogják helyezni a civilizált társadalmakat.

Az 5G technológia kapcsán nagyon fontos megjegyezni, hogy az 5G szabvány végleges verziójának a kialakítása még folyamatban van. Az EU meghatározó szereplő világszinten az 5G-hez kapcsolódó szabadalmak és szabványok kidolgozásában. Ez a nemzetközi gazdasági verseny és kooperációk szempontjából is nagyon fontos.

Jelenleg az 5G fejlesztés az egyik legmagasabb szintű high-tech fejlesztés, itt mindent pontosan bevizsgálnak és megterveznek. Sem az eszközgyártók, sem a szolgáltatók nem engedhetik meg maguknak, hogy 20-25 milliárd majdani felhasználót jelentő globális piac esetén bármilyen egészségügyi kockázat legyen.

Az 5G hálózat hasonlítani fog a háztartásainkban használatos wifi-routerek által elérhető nagy sávszélességű internetkapcsolathoz, ehhez hasonló lefedettséget fog lehetővé tenni a külső térben. A routerekhez hasonló méretűek az 5G külső antennák, csak más technológiával és más sávszélességen működnek. Egy-egy antenna kb. 0,1 km^2 teret fog lefedni, és az antennák közötti távolság optimális esetben 112 méter lesz. Az elhelyezésük az elképzelések szerint az épületeken, a buszmegállók tetején, az utak mentén sorakozó oszlopokon lehetséges. A használatukkal feleslegessé válik majd a hegyek tetején éktelenkedő adótornyok többsége, ezek egy részét le is fogják bontani. Fontos paradoxon, hogy minél több antenna lesz körülöttünk, annál kisebb energiával kell majd az eszközöknek sugározniuk. A jelterjedés során a jel intenzitása a távolsággal négyzetesen csökken. A jelenlegi 4G hálózatoknál ez a távolság akár több km is lehet, az 5G-nél viszont a már említett 112 méterre csökkenhet (30. ábra). Így az IoT-eszközöket is kevesebbszer kell majd tölteni, kisebb lesz az áramfelvételük, amivel majd akár évekig tudnak működni. Az 5G tehát az energiamegtakarításról és az IoT-eszközökre épülő ökoszisztémákról (mint pl. az ITS Ökoszisztéma) szól.

[37] ICNIRP GUIDELINES FOR LIMITING EXPOSURE TO ELECTROMAGNETIC FIELDS (100 KHZ TO 300 GHZ) https://www.icnirp.org/cms/upload/publications/ICNIRPrfgdl2020.pdf

	Hagyományos hálózatok (2014)	Sűrített hálózatok (2015-2017)	Nagyon sűrű hálózatok (2017-2020)	Ultra sűrű hálózatok (2020 után)
Site/km²	7 állomás	21 állomás	26 állomás	93 állomás
Állomások közötti távolság	395 m	237 m	209 m	112 m
Forgalom sűrűség	~1 Gb/s/km²	~5 Gb/s/km²	~10 Gb/s/km²	~40 Gb/s/km²
Aktív felhasználók	250	625	1000	~2500

30. ábra: 5G lefedettség biztosítása

Jogos aggodalom, hogy az 5G milliméteres hullámhosszainak útját állhatják majd a fák, gátolva ezzel a kommunikációt. Mivel nem ionizáló rádióhullámokról van szó, az élő szervezetekbe csak kismértékben tudnak behatolni. Természetesen nem kell majd miattuk kivágni a fákat, hiszen az antennák átlapolással lesznek elhelyezve a jelenlegi elektromos elosztóhálózathoz kapcsolódóan.

2.5.3. Az 5G hálózat az utak mentén

Az 5G hálózat kialakításánál a legnagyobb probléma az adatátviteli nagy kapacitású optikai hálózat és az aktív eszközök áramellátásának a biztosítása. A Magyar Közút Nonprofit Zrt. adatai szerint a magyar úthálózat hossza meghaladja a 200 ezer km-t, minden egyes km²-re kb. 2 km hosszú közút jut. Azzal számolva, hogy kb. 112 méterenként elhelyezésre kerül egy-egy antenna, ehhez kb. 1 millió (kis méretű) antennának és 200 ezer folyókilométer többszörösen redundáns optikának kellene lenni az utak közvetlen közelében, hogy az 5G hálózat mindenhol kiszolgálható legyen. A Distribution System Operatorok (DSO-k, azaz Elosztóhálózati Rendszerüzemeltetők), akik az elektromos áram elosztását végzik, a közszolgáltatási főtevékenységet meghatározó jogszabály szerint – megfelelő feltételek teljesülése esetén – kötelesek tűrni a hírközlési hálózatok elhelyezését a közcélú hálózaton. Ezt a kötelezettséget a hírközlési tevékenységhez kapcsolódó igények növekedése motiválja, amely a jelenlegi pandémiahelyzetben segíthetne felgyorsítani a megnövekedett igények kielégítését, és új műszaki megoldásokat hozhatna így létre. Ezzel a fejlesztéssel egy új komplex nemzeti infrastruktúra jöhetne létre, amely illeszkedne a kormányzati stratégiákhoz (Magyarország 5G stratégiája, Digitális Jólét Program 2.0), költséghatékony, gyors és biztonságos megoldást jelentene. Az 5G hálózati lefedettséget lehetővé tevő alaphálózattal egyszerre ki lehetne alakítani a végfelhasználói FTTH-hálózatot, a smart metering/grid alkalmazásokat áramhálózati üzemviteli célokra és további innovatív smart megoldások (okos város) kialakításával további pozitív hatásokat lehetne elérni.

2.5.4. Az 5G hálózattól elvárt legfontosabb paraméterek.

Table 2 5G performance requirements for low latency and high reliability scenarios [12]

Scenario	End-to-End Latency	Communication Service Availability	Reliability	User Experienced Data Rate	Connection Density	Service Area Dimension
Discrete automation – motion control	1 ms	99,9999%	99,9999%	1 Mbps to 10 Mbps	100 000/km^2	100 × 100 × 30 m
Process automation – remote control	50 ms	99,9999%	99,9999%	1 Mbps to 100 Mbps	1000/km^2	300 × 300 × 50 m
Process automation – monitoring	50 ms	99,9%	99,9%	1 Mbps	10 000/km^2	300 × 300 × 50
Electricity distribution – medium voltage	25 ms	99,9%	99,9%	10 Mbps	1000/km^2	100 km along power line
Electricity distribution – high voltage	5 ms	99,9999%	99,9999%	10 Mbps	1000/km^2	200 km along power line
Intelligent transport – infrastructure backhaul	10 ms	99,9999%	99,9999%	10 Mbps	1000/km^2	2 km along a road

Scenario	Experienced Data Rate (Down-link)	Experienced Data Rate (Uplink)	Area Traffic Capacity (Down-link)	Area Traffic Capacity (Uplink)	Overall User Density	UE Speed
Indoor hotspot	1 Gbps	500 Mbps	15 Tbps/km^2	2 Tbps/km^2	250 000/km^2	Pedestrians
Dense urban	300 Mbps	50 Mbps	750 Gbps/km^2	125 Gbps/km^2	25 000/km^2	Pedestrians and users in vehicles (up to 60 km/h)
Urban macro	50 Mbps	25 Mbps	100 Gbps/km^2	50 Gbps/km^2	10 000/km^2	Pedestrians and users in vehicles (up to 120 km/h
Rural macro	50 Mbps	25 Mbps	1 Gbps/km^2	500 Mbps/km^2	100/km^2	Pedestrians and users in vehicles (up to 120 km/h
Broadband in a crowd	25 Mbps	50 Mbps	3,75 Tbps/km^2	7,5 Tbps/km^2	500 000/km^2	Pedestrians
Broadcast-like services	Maximum 200 Mbps (TV channel)	Modest (e.g., 500 kbps per user)	N/A	N/A	15 TV channels of 20 Mbps	Stationary to in vehicles (up to 500 km/h)
High-speed train	50 Mbps	25 Mbps	15 Gbps/train	7,5 Gbps/train	1000/train	Users in trains (up to 500 km/h)
High-speed vehicle	50 Mbps	25 Mbps	100 Gbps/km^2	50 Gbps/km^2	4000/km^2	Users in vehicles (up to 250 km/h)
Airplanes connectivity	15 Mbps	7,5 Mbps	1,2 Gbps/ plane	600 Mbps/ plane	400/plane	Users in airplanes (up to 1000

31. ábra: Az 5G hálózattól elvárt legfontosabb paraméterek

2.6. Publikációk

1. Bódi Antal – Maros Dóra (2019): A komplex ITS ökoszisztéma alapjai. *Acta Periodica (Edutus) 17.* 48–70. 23.

2. Bódi Antal (2019): A komplex ITS ökoszisztéma kialakítása jelenti a közlekedésbiztonság új digitális alapokra történő emelését. In Tokody Dániel – Balla Esztella – Németh Katalin szerk.: *Okos Közlekedési Tudományos Konferencia 2019. Absztraktkötet*. Budapest, Doktoranduszok Országos Szövetsége Műszaki Tudományok Osztály.

3. Bódi Antal – Szabó Tivadar – Maros Dóra – Gáspár László (2018): ITS ökoszisztéma – a közlekedés egészének digitalizációja. In Munkácsy András – Jászberényi – Melinda szerk.: *Utazás a tudományban: Konferencia a 70 éves Pálfalvi József tiszteletére. Konferenciakötet.* Budapest, Budapesti Corvinus Egyetem. 82–84., 3.

4. Bódi Antal – Szabó Tivadar – Maros Dóra – Nagy Viktor – Gáspár László (2018): A komplex ITS ökoszisztéma kialakításának közgazdasági előnyei. In Földi Péter – Borbély András – Kápolnai Zsombor – Zsarnóczky Martin Balázs – Gerencsér Ilona – Gódor Amelita Kata – Gubacsi Franciska – Nyírő András – Bálint Csaba – Szeberényi András – Fodor-Borsos Eszter szerk.: *Innovatív társadalom – Innovatív gazdaság. Absztraktkötet.* Budapest, Doktoranduszok Országos Szövetsége. 6–6., 1.

5. Bódi, Antal – Szabó, Tivadar – Maros, Dóra (2018): The bases of the its ecosystem. In Rajnai, Zoltán – Schmidt, Peter – Szivosová, Mária – Jurík, Pavol szerk.: *Seventh International Scientific Videoconference of Scientists and PhD. students or candidates „Trends and Innovations in E-business, Education and Security": Proceedings Bratislava.* University of Economics in Bratislava. 9–12., 3.

6. Beke, Éva –Bódi, Antal (2018): The role of drones in linking Industry 4.0 and ITS ecosystems In: Rajnai Zoltán szerk.: *Kiberbiztonság – Cyber Security : Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból.* Budapest, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 313–327., 11.

7. Beke, Éva – Bódi Antal – Takácsné György, Katalin – Kovács Tibor – Maros Dóra – Gáspár László: The role of drones in linking industry 4.0 and ITS Ecosystems. In Szakál, Anikó ed. (2018): *IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI 2018) Budapest, Magyarország: IEEE Hungary Section.* 191–197., 7 p. DOI Scopus

8. Bódi Antal – Szabó Tivadar – Dr. Wührl, Tibor (2017): Drónok követése közhiteles módon. *Repüléstudományi Közlemények*, 2017: 2. 111–118., 8.

3. TÓTH KORNÉL – AZ EGÉSZSÉGÜGYI INFORMÁCIÓS RENDSZEREK INFORMÁCIÓBIZTONSÁGA

3.1. Bevezetés

Az informatika és a digitalizáció mára már mindennapjaink részévé vált, ez alól nem kivétel az egészségügy sem. A vállalatirányításban és az egészségügyben is az információs és döntéstámogató rendszerek szerepe hatványozottan növekedett, amelyekkel a rendelkezésünkre álló adatokat információvá, majd tudássá transzformálhatjuk. Ackoff[38] bölcsességhierarchiája alapján az adat rendelkezésre állása önmagában nem elégséges, az értelmezéséhez releváns, használható formában kell lennie. Az adat és az információ közötti különbség nem strukturális, hanem funkcionális, valamint az információk az adatok alapján a leírásokban találhatók, választ adhatnak a mennyi, mikor, ki, mi, hol kérdésekre. Amikor megkapjuk a választ, akkor válik az adat információvá.

Az egészségügyben sem elegendő csupán az adatok rendelkezésre állása, azokat rendszerezni, strukturálni szükséges annak érdekében, hogy információt lehessen kinyerni belőlük. Ezen folyamatot az információs rendszerek használata biztosítja. Az adatnak önmagában nincs értéke, azonban, ha az a megfelelő struktúrában érhető el, abból információ nyerhető ki, akkor már a gyógyítási folyamatban eszközként tudja támogatni az orvoslást, az egészségügyi szolgáltatásnyújtást.

Az értékkel, információval bíró adatok és az azokat kezelő információs rendszerek tekintetében különösen fontos a biztonság, a védelem, mivel az illetéktelen felhasználásukkal visszaéléseket generálhatnak. Az információs rendszerek és a tárolt adatok kompromittálásával befolyásolhatók a döntéselőkészítési folyamatok, így akár egy beteg gyógyítása is, amellyel félrekezelhető a páciens. A jogi, szabályozási oldalon a hazai elektronikus információbiztonságra vonatkozó jogszabályokon felül az Európai Unió is kiemelten kezeli az IT-biztonság kérdését. Ezt támasztja alá az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS-irányelv).

Az egészségügyben kiemelt szerepe van az adatok védelmének és az információbiztonságnak, mivel egy állampolgárról rengeteg különösen érzékeny személyes információ és egészségügyi rekord érhető el. A hazai egészségügyben a közigazgatással szemben még nem kezdődött el az informatikai rendszerek konszolidációja. Így sok intézményben a hardver- és a szoftver-eszközpark és -infrastruktúra jellemzően heterogén képet mutat. Az ezeken kezelt információk más-más biztonsági szintnek felelnek meg. A régi, úgynevezett hagyatéki vagy örökölt (legacy) rendszerek esetében ma már ritkán érhető el gyártói támogatás, a biztonsági rések befoltozására sem várhatók gyártói frissítések. Másrészről viszont 2017 októberében elindult az Elektronikus Egészségügyi Szolgáltatási Tér[39] (EESZT), ahová a legtöbb egészségügyi információs rendszer csatlakoztatásra került/kerül. Az EESZT magas biztonsági színvonalon szolgálja ki a felhasználókat, de IT-biztonsági szempontból fontos megjegyezni, hogy a közigazgatással ellentétben egy személy (például orvos) az adott páciens minden

[38] ACKOFF, R. L.: From data to wisdom, https://www.isko.org/cyclo/dikw

[39] https://e-egeszsegugy.gov.hu/eeszt

személyes adatához és egészségügyi rekordjához hozzáfér. Természetesen ez nem jelenti azt, hogy jogosulatlanul megnézheti az adatokat[40].

Jelen dokumentumban a hazai egészségügyi információs rendszerek, a jogi, szabályozási háttér és a kezelt, tárolt adatok információbiztonsági szempontú megközelítése kerül bemutatásra. Az egészségügyi adatok nemzetgazdasági szempontból kiemelt jelentőséggel bírnak, a nemzeti adatvagyon részei, így azokat kiberbiztonsági szempontból is megfelelően szükséges kezelni és tárolni. Áttekintésre kerülnek a rendszerek főbb kockázatai és az enyhítési technikák, lehetőségek is. Az IT-biztonsági tudatosság növelése érdekében két esettanulmány mutatja be példák alapján a kiberincidens lehetőségét.

3.2. Az egészségügyi információs rendszerek áttekintése

Az egészségügyi információs rendszer (HIS – Health Information System) egy olyan rendszer, amelynek célja az egészségügyi intézményekben gyűjtött és tárolt adatok kezelése, amely szolgáltatások nyújtása formájában támogatja az egészségügyi intézmény munkáját. Számos különféle egészségügyi információs rendszer létezik, amely függ az egészségügyi intézmény típusától és a konkrét specifikus igényektől is. Ide tartoznak az orvosi rendelők, a magán- és állami klinikák, valamint a kórházak. Ezek gyűjtik, tárolják, kezelik és (tovább)küldik a páciensek elektronikus egészségügyi rekordjait. Az egészségügyi információs rendszerek használatának célja az, hogy javítsa a páciensek kezelését azáltal, hogy a legfrissebb, valamint az előzményi páciensadatokkal rendelkeznek minden olyan orvos számára, aki ezt az „ügyfelet” kezeli. Nyilvánvaló, hogy ezek a páciensadatok nagyon érzékenyek, így minden egészségügyi információs rendszernek biztosítania kell az összegyűjtött adatok pontosságát és a (páciens)adatok bizalmas kezelését. A páciens adatainak az egyéni ügyfélkezelésen kívüli egyéb felhasználásai közé tartozik az orvosi kutatás, a politikai döntéshozatali adatok, a vezetői döntéshozatali információk és a pénzügyi elszámolási adatok a finanszírozó felé. Az egészségügyi információs rendszerek rendszeresen hozzáférnek, feldolgoznak vagy tárolnak nagy mennyiségű érzékeny páciensinformációt. Ennek eredményeként a biztonság döntő jelentőségű.

Az egészségügyi információs rendszereket többféleképpen csoportosíthatjuk. Az IT-biztonság szempontjából a legcélravezetőbb csoportosítási kategóriák lehetnek, hogy ki az, aki hozzáfér a rendszerhez, valamint hogy ezen információs rendszerek infrastruktúrája hogyan épül fel, hogyan valósul meg az adatok tárolása és kezelése.

A. Felhasználói szempontú, hozzáférés-alapú csoportosítás

- Alapellátás
  - háziorvosok, házi gyermekorvosok, védőnők, iskola-egészségügy, fogorvosi alapellátás
- Szakellátás
  - szakorvosok, járóbeteg-, fekvőbete- ellátás
- Életmentés
  - mentők
- Gyógyszertárak
  - gyógyszerészek, gyógyszertári rendszerek

[40] http://medicalonline.hu/eu_gazdasag/cikk/jogosulatlanul_kert_le_adatokat_az_orvos

- Páciensek
  - EESZT saját felület, EHR, PHR, e-Recept stb.

- Adminisztrációs jellegű
  - egészségügyi intézményközi információs rendszerek
  - pénzügyi elszámolási rendszerek
  - lokális vezetői információs rendszerek
  - központi információs rendszerek (például ÁEEK központi adatszolgáltatási rendszerek)

B. Infrastruktúra szempontú csoportosítás

- Lokális üzemeltetés
  - kórházi, medikai rendszerek
  - háziorvosi (praxis) rendszerek (például GP-k, védőnői rendszer)
  - ERP rendszerek (például: statisztika, munkaügy, pénzügy, vállalatirányítás)

- Központi üzemeltetésű
  - EESZT – Elektronikus Egészségügyi Szolgáltatási Tér
  - MIR – Mentésirányítási rendszer
  - ESR 112 – Segélyhívó rendszer

A másik csoportosítási szempont megközelítése az egészségügyi ellátást biztosító infrastruktúra módja, amely lehet lokális és központi üzemeltetésű. Magyarországon az ellátást biztosító intézmények túlnyomórészt helyben üzemeltetik IT-infrastruktúrájukat, amelyet saját erőforrásból oldanak meg. A központi rendszerüzemeltetés tekintetében kielemelendő az EESZT, amelynek infrastruktúrája a Kormányzati Adatközpontban került elhelyezésre, így a rendszert egy biztonságos, magas rendelkezésre állású, redundáns informatikai környezet tudja kiszolgálni. Az EESZT-be a legtöbb medikai rendszer becsatlakoztatásra került, vagy csatlakoztatása folyamatban van. Funkciói közül kiemelendő az e-Recept, amely modult a háziorvosok, a szakorvosok és a gyógyszerészek is használják a páciensek mellett.

Az egészségügyben a személyes és szenzitív páciensadatokat kezelő egészségügyi információs (HIS – Healthcare Information System) rendszerek mellett használatosak a 'klasszikus' vállalatirányítási rendszerek is, úgymint SAP, vagy a gazdálkodási rendszerek is (CT-EcoSTAT).

3.3. Jogi, szabályozási környezet

Az állam és szervezetei, valamint az állampolgár is kiszolgáltatottá vált a különböző információs rendszereknek, amelyek nélkül az állam működése, működtetése és az egyes szolgáltatások biztosítása mára már szinte elképzelhetetlenné vált. Ennek okán is kiemelten fontos az adatok védelme és megfelelő kezelése érdekében az információs rendszerek jogi szempontból történő szabályozása. A 'közfeladatot' ellátó információs rendszerek által kezelt adatok sértetlensége, bizalmassága és folyamatos rendelkezésre állása alapvető fontossággal bír, amelynek hátterét a jogszabályok és uniós rendeletek biztosítják, valamint irányelvek és ajánlások támogatják.

A jogszabályok és ajánlások listáját az 1. számú melléklet tartalmazza.

A vonatkozó szabályozás alapvetően három szintre tagolható, a következők szerint:

a) hazai jogszabályok,

b) helyi, intézményi szintű szabályozás
c) uniós szintű szabályozás.

3.3.1. Hazai jogszabályok

A magyar jogszabályok közül az adatkezelést érintően keret jelleggel irányadó az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), illetve speciálisan az egészségügyi ágazatra vonatkozóan került megalkotásra az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről 1997. évi XLVII. törvény (a továbbiakban: Eüak.).

Az Infotv. az adatok kezelési módjától (elektronikus vagy egyéb) és az adatkezelő személyétől (állami, önkormányzati, vagy magán) függetlenül definiálja a személyes adat, különleges adat fogalmát, az adatkezelés lehetséges célját és alapelveit, meghatározza az érintettek jogait, valamint rögzíti az alapvető adatbiztonsági követelményeket. Az Eüak. speciálisan az egészségügyi ágazat vonatkozásában rögzíti az adatkezelés lehetséges céljait, és meghatározza az egyes célokkal összefüggésben kezelhető személyes adatok körét, tartalmazza továbbá az EESZT-vel összefüggő adatvédelmi rendelkezéseket.

A fenti törvényeken túlmenően az abban meghatározott állami, illetve önkormányzati szervek által használt elektronikus rendszerek tekintetében irányadó az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.).

Az Ibtv. meghatározza az alapvető elektronikus információbiztonsági követelményeket, rögzíti, hogy a rendszerek teljes életciklusában meg kell valósítani és biztosítani kell

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása, a poszt-kvantumtitkosítás alkalmazásra kötelezett szervezetek esetén a fizikailag elkülönített helyszíneik közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatásaik igénybevétele során a hagyományos kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantum titkosítási alkalmazással történő zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. Ezen védelem biztosítása érdekében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják a *megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, a biztonsági események kezelését.*

3.3.2. Helyi, intézményi szintű szabályozások

A szabályozás harmadik szintjét a helyi szintű, az érintett intézmény által készített, kiadott belső szabályozások alkotják. Ebben a körben az Infotv. előírja, hogy ha 1) az adatkezelő, illetve az adatfeldolgozó állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot lát el – kivéve a bíróságokat –, vagy 2) ha törvény vagy az Európai Unió jogi aktusa azt előírja, *adatvédelmi tisztviselő*t alkalmaz. Az Infotv. rögzíti továbbá azt is, hogy ha az adatkezelő adatvédelmi tisztviselő kijelölésére köteles, az adatbiztonsági intézkedések részeként köteles *belső adatvédelmi és adatbiztonsági szabályzatot* megalkotni és alkalmazni.

A fentieken túlmenően az Ibtv. hatálya alá tartozó szervezet köteles *elektronikus információs rendszer biztonságáért felelős személy*t kinevezni, illetve megbízni, továbbá *informatikai biztonsági szabályzat*ot (IBSZ) is alkotni, amely tartalmazza az általa kezelt adatok biztonsági osztályba, illetve a szervezet biztonsági szintbe történő besorolását. A biztonsági osztály jelenti az elektronikus információs rendszer védelmének elvárt erősségét, a biztonsági szint pedig a szervezet felkészültségét a vonatkozó jogszabályokban meghatározott biztonsági feladatok kezelésére. A biztonsági osztályba sorolás során – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt. A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet meghatározott szempontok szerint. A biztonsági osztályba sorolás és a biztonsági szint megállapításának ellenőrzését a Nemzeti Kibervédelmi Intézet végzi.

3.3.2.1. EESZT rendelet

Az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) egy egységes digitális egészségügyi platform, amellyel valamennyi magyar állampolgár egészségügyi adatai, kórtörténete és leletei egy helyen elérhető. A rendszerhez való csatlakozás feltételeit és rendjét, valamint a csatlakozásra köteles szervek körét a *39/2016. (XII. 21.) EMMI rendelet* szabályozza. A csatlakozás előtt a csatlakozó szervnek kötelessége megvizsgálni informatikai rendszerét a rendeletben hivatkozott követelmények teljesülése érdekében. Ezt követően kezdődhet meg az egészségügyi ellátást nyújtó általi adatszolgáltatás az EESZT felé, valamint ekkor nyílik lehetőség a páciensek adataihoz való hozzáféréshez is.

3.3.3. Uniós szabályozás és ajánlások (NIS, GDPR, ENISA)

Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, azaz a NIS-irányelv célja annak biztosítása, hogy az IT-infrastruktúra ellen irányuló esetleges kibertámadásokra az uniós tagállamok felkészüljenek, bekövetkezésük esetén pedig azokat megfelelően kezelni tudják. Az irányelv szükségességét az egyre növekvő kibertámadások számossága, valamint a biztonsági incidensekből fakadó adatlopások, rendszer- és hálózatfeltörések (hack) is indokolja.

A kibertámadások főbb típusai az alábbiak, melyek módszerét tekintve egyre kifinomultabbak:

- APT-támadás – célja az információszerzés, a folyamatos jelenlét, és nem a károkozás;
- Phishing, adathalászat – célja a megtévesztésen alapuló érzékeny információk megszerzése (például: személyes adatok, jelszó, bankkártyaadatok stb.);
- Denial of Service (DoS), szolgáltatásmegtagadással járó támadás – célja egy informatikai szolgáltatás teljes vagy részleges megbénítása, elérésének korlátozása vagy ellehetetlenítése;
- Malware, azaz a rosszindulatú szoftverek – célja, hogy kárt tegyenek az IT-rendszerekben (infrastruktúrában, programokban);
- Social Engineering, azaz az emberi befolyásolhatóság – célja, hogy a támadó bizalmi kapcsolatba kerüljön az áldozattal annak érdekében, hogy belső információkhoz férhessen hozzá

A GDPR rendelet és a NIS-irányelv közötti különbség, hogy a GDPR rendelet minden olyan szervezetre vonatkozik, amelyik személyes adatot kezel, a NIS viszont a társadalmat érintő szolgáltatókat érinti. A NIS esetében ilyen a szolgáltatást nyújtók, például a bankszektor, a közműszolgáltatók, az egészségügyi intézmények és a közlekedési vállalatok, és minden olyan szervezet, intézmény, amely működésének korlátozása vagy kiesése társadalmi vagy gazdasági károkat okozna. Ennek megfelelően az egészségügyi adatok és az azokat kezelő intézmények, szervezetek is a NIS-irányelv és a GDPR rendelet hatálya alá tartoznak.

A NIS esetében az irányelveket a belső, tagállami jogrendszerbe kell átültetni, a GDPR pedig egy alkalmazandó, közvetlenül hatályos joganyag.

A NIS-irányelv és a GDPR rendelet lehetőséget kínál az egészségügyi szektor számára stratégiák kidolgozására az adatok és rendszerek nyomon követéséhez (naplózás, log), ezáltal lehetővé téve a szabályoknak való megfelelést, valamint az adatvagyon integrált, biztonságos kezelésére vonatkozó módszertanok kidolgozását is elősegítik.

A NIS-irányelv három részből áll:

1. Nemzeti képességek: Az EU-tagállamoknak rendelkezniük kell az egyes EU-országok bizonyos nemzeti kiberbiztonsági képességeivel, például nemzeti CSIRT-tel kell rendelkezniük.
2. Határokon átnyúló együttműködés: Határokon átnyúló együttműködés az EU országai között, például az operatív EU CSIRT hálózat, a stratégiai NIS együttműködési csoport stb.
3. A kritikus ágazatok nemzeti felügyelete: Az EU-tagállamoknak felügyelniük kell a kritikus piaci szereplők kiberbiztonságát az országukban: előzetes felügyelet a kritikus ágazatokban (energia, közlekedés, víz, egészségügy és pénzügyek), és utólagos felügyelet a kritikus digitális szolgáltatók esetében (internet exchange points, doménnév-rendszerek stb.).

A NIS együttműködési csoport az a stratégiai együttműködési csoport, amelyben az EU tagországai együttműködnek, információcserét folytatnak, és megállapodnak abban, hogy a NIS-irányelvet az EU-ban következetesen hogyan kell végrehajtani. A NIS együttműködési csoport stratégiai iránymutatást is ad az alapul szolgáló EU CSIRT hálózathoz. A NIS együttműködési csoport tagjai az illetékes nemzeti minisztériumok és a nemzeti kiberbiztonsági ügynökségek képviselői.

Az ENISA az alábbiakkal segíti az együttműködési csoportot feladataiban:

- A NIS-irányelv végrehajtásával kapcsolatos bevált gyakorlatok meghatározása a tagállamokban;
- Az EU egészére kiterjedő kiberbiztonsági események jelentési folyamatának támogatása sablonok és eszközök kidolgozásával;
- Megállapodás a közös megközelítésekről és eljárásokról;
- A tagállamok támogatása a közös kiberbiztonsági kérdések kezelésében.

Mivel a kiberbiztonság egyre inkább prioritássá válik a kórházak – beleértve a más egészségügyi szervezeteket is[41] – számára, elengedhetetlen, hogy holisztikusan integrálják az egészségügyi IKT Ökoszisztémát befolyásoló különféle folyamatokba, alkotóelemekbe és szakaszokba. A beszerzés a modern kórházak IKT-környezetét meghatározó kulcsfontosságú folyamat, és mint ilyen, élen kell állnia a kiberbiztonsági célkitűzések elérésében. Az egyik ilyen dokumentum az ENISA által publikált Kiberbiztonsági beszerzési útmutató a kórházaknak,[42] amely a kiberbiztonsági célok elérésének biztosítása érdekében a bevált gyakorlatokat mutatja be a beszerzési életciklust a tervezés, forrás és menedzsment szakaszok szerinti bontásban. A kiberbiztonsági megfontolások mindhárom szakaszra vonatkoznak, és ez a jelentés a kórházak számára könnyen használható útmutatót kínál

41 Lásd a kutatóintézeteket ért támadások.

42 ENISA – Procurement guidelines for cybersecurity in hospitals – Good practices for the security of Healthcare services; February 2020.

a beszerzési folyamat javításához kiberbiztonsági szempontból. Az általános jó gyakorlat szerint a kórházakat ösztönözni kell arra, hogy a beszerzések lebonyolítása során vonják be az IT-területet, azonosítsák a lehetséges biztonsági réseket, és sérülékenységi pontokat, szabályozzák a hardver- és szoftverfrissítéseket és a tesztelést, valamint vegyék figyelembe az interoperabilitással kapcsolatos kérdéseket.

Az ENISA által kiadott ajánlások, és jó gyakorlatok implementálásával csökkenthető az IT-biztonsági kitettség.

3.4. Az egészségügyi információs rendszerek, a kezelt és tárolt adatok információbiztonsága

Az egészségügyi kiberbiztonság célja, hogy a megfelelő intézkedések végrehajtásával eleget tegyen az információk titkosságának, hozzáférhetőségének és épségének (kompromittálódás mentes adatok) védelme érdekében. Cél a hitelesség, elszámoltathatóság és auditálhatóság is.

Az egészségügyi információs rendszerekben nagyon nagy mennyiségben található szenzitív személyes adat, ezért is kiemelt jelentőségű a magas IT-biztonsági színvonal kialakítása, amelyet az egészségügyi digitalizációs törekvésekkel együttesen kell fejleszteni. Javasolt tehát már a tervezés fázisában is kiemelt figyelmet fordítani a kiberbiztonságra, azaz ajánlott az intézmény/külső kompetencia bevonása a beruházás legelejétől kezdődően.

A magyarországi egészségügyi információs rendszerek követelményeit egy korábban, a GYEMSZI (jelenleg ÁEEK) által összeállított dokumentum foglalja össze.[43] A kidolgozandó informatikai feltételrendszer és a rendszerminősítési kritériumok praktikus, gyakorlati alkalmazhatóságát közérthetően fogalmazza meg, és az ajánlások között szerepel az IT-biztonság is. A dokumentum leírja a minősítési eljárással szemben támasztott elvárásokat is.

Az Ibtv.-hez szorosan kapcsolódik a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, illetve az egészségügyi ágazat tekintetében az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet (a továbbiakban: Korm. rendelet), amelyek azonosítják az egészségügyben az európai, illetve a nemzeti létfontosságú rendszerelemeket. Ezekkel összefüggésben az Ibtv. 2. § (2) bekezdés c) pontja rögzíti, hogy az európai vagy nemzeti létfontosságú rendszerelemmé - a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján - kijelölt rendszerelemeknek a létfontosságú tevékenységben közreműködő elektronikus információs rendszerei védelmére az Ibtv. rendelkezéseit kell alkalmazni. (Ilyen rendszerelemek a teljesség igénye nélkül például: a Korm. rendeletben meghatározott szempontoknak megfelelő aktív fekvőbeteg-ellátók, mentésirányítási központok, az Állami Egészségügyi Tartalék bizonyos elemi, az országos vérkészlet nyilvántartási rendszerei, az egészségbiztosítás meghatározott feltételeknek megfelelő informatikai rendszerei). Az Ibtv. hatálya alá nem tartozó információs rendszerekre ugyanakkor nem kötelezőek az abban rögzített szigorú elvárások, így az egyes, az egészségügyi ágazatban használt információs rendszerek informatikai biztonsági szempontból nem feltétlenül „egyenszilárdságúak”.

Az Ibtv. végrehajtási rendelete (41/2015. (VII. 15.)) katalogizálja a védelmi intézkedéseket az egyes biztonsági osztályok (szintek) kötelező teljesítését, az alábbi három főkategória szerint:

- adminisztratív védelmi intézkedések;
- fizikai védelmi intézkedések;
- logikai védelmi intézkedések.

[43] Az egészségügyi információsrendszerek követelményei v 9.0 – https://era.aeek.hu/zip_doc/kutatas/2012/Eredeti/Rendszerk%C3%B6vetelm%C3%A9nyek-2011%2011%2029-v9.0-v%C3%A9gleges.pdf

3.4.1. Az információs rendszerek biztonsági besorolása

A közigazgatással ellentétben az egészségügyben a medikai és más információs rendszerek biztonsági besorolása még nem történt meg teljeskörűen. Az Ibtv. végrehajtási rendelete alapján az EESZT biztonsági besorolása már megtörtént, amely a legmagasabb 5-ös szintű. Ezzel szemben az EESZT rendszerhez csatlakozott rendszerek biztonsági besorolása még várat magára.

Az EFOP-1.9.6-16 Elektronikus egészségügyi ágazati fejlesztések kiemelt projekt keretében célként került meghatározásra az IT-biztonsági szint növelése a kórházak működését veszélyeztető behatolásokkal szemben, mivel az egészségügyi informatikában különösen meghatározó az információs rendszerek komplex védelmének kialakítása, amire sajnos az esetek többségében csak akkor kerül sor, ha már bekövetkezett valamilyen támadás, kár, botrány vagy katasztrófa. A projekt elkötelezett célja, hogy a bevont intézmények informatikai biztonságát emelje, közel azonos szintre hozza. Ezen intézkedések a humán erőforrás információbiztonság-tudatosságának fejlesztése, az információbiztonsági működéssel kapcsolatos folyamatok és megfelelést célzó fejlesztések, az informatikai biztonság technológiai szintű megerősítését célzó intézkedések, valamint a központi és egységes címtár, valamint jogosultságkezelő rendszer kialakítása és kikényszerítése.

Tehát a projekt egy hiátust pótol az egészségügyi intézmények biztonsági auditjával, melynek keretében a jelenlegi helyzet felmérésére, a problémás és fejlesztendő területek azonosítására kerül sor egységes szempontrendszer és módszertan alapján.

Az Ibtv. hatálya alá tartozó elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából. Ez egy 1–5-ig skálázott biztonsági szint fokozatot jelent, az 5-ös szint a legszigorúbb előírásoknak való megfelelést jelenti. A biztonsági osztályba való besorolást az érintett szervezeteknek kell elvégezniük. Tehát az érintett egészségügyi szolgáltató intézmények feladata az Ibtv. szerinti megfelelés, de ez nem történik meg egységesen, melynek oka, hogy az egyes intézmények eltérő IT-biztonsági fejlettségi szinten állnak, valamint, hogy a különböző projektekből finanszírozott lehetőségekkel beszerzett új IT-környezetek arányai és ezek együttműködései eltérőek lehetnek.

Az egészségügyi intézményekben az informatikai rendszerek hivatottak biztosítani a folyamatos és hatékony betegellátást. A napi betegellátási munka támogatásán felül a rendszereknek ki kell szolgálnia az orvosok, gyógyszerészek, adminisztrációs feladatokat végzők és a kutatók igényeit is, melynek következtében ezek a rendszerek nemcsak a páciensek személyes szenzitív adatait és az intézmény finanszírozásához szükséges adatokat tárolják, hanem a gyógyító munkával kapcsolatos egyéb információkat is.

Az egészségügyi információs rendszerekben tehát a páciensekről minden adat megtalálható, így a páciensek különösen érzékeny személyes adatai is szemben a közigazgatással, ahol szakrendszerenként és nyilvántartásonként lehet személyes adatokat kinyerni, amely rendszerek és nyilvántartások magasabb IT-biztonsági szinten védettek. Az EESZT rendszerből az egészségügyi adatok egy „gombnyomásra” kinyerhetőek. A megfelelő biztonság garantálásához az adatokat szenzitivitásukból adódóan egészen a végpontig védeni kell, nem elegendő, hogy az EESZT 5-ös biztonsági besorolású.

Általánosságban elmondható, hogy Magyarországon alacsony szinten van az egészségügyi informatikai rendszerek biztonsága (kivéve EESZT), amelyen a legrövidebb időn belül javítani kell, az ellátórendszer egészének a biztonságos működése érdekében.

3.4.2. Az egészségügyi ágazati IT-infrastruktúra

Az egészségügyi ágazati informatika decentralizált, ebből fakadóan mind hardver, mind szoftver oldalról teljesen heterogén képet mutat. A fejlesztések – az EESZT-t kivéve – lokálisan és időben elhúzódva valósultak meg, így az intézmények és telephelyeik különböző infrastruktúrával, eszközparkkal, és kapacitásokkal rendelkeznek. Az intézmények maguknak finanszírozzák az informatikai beruházásaikat, amelyek a betegellátással szemben hátrasorolódnak, így sok esetben nincsenek megfelelően licenszelt termékek, megoldások, valamint támogatás (support) sem, továbbá nehezen vagy nem megoldott a régebbi (legacy) rendszerek biztonságos üzemeltetése.

Az informatikára és az IT-biztonságra fordított forrás nem minden esetben elegendő az IT-infrastruktúra magas biztonsági szinten történő üzemeltetésére, amely kockázatot tovább fokozzák a régi, elavult hagyatéki rendszerek, amelyek zöme alapbeállításokon üzemel, valamint már megszűnt hozzá a támogatás, a gyártók már nem adnak ki hozzájuk újabb biztonsági frissítéseket sem. Továbbá az intézmények régebbi rendszereinek üzemeltetése kapcsán ún. humán monopóliumok alakulhatnak ki, azaz már nem, vagy csak nehezen és drágán találni olyan kompetenciájú szakembert/vállalkozót, aki hibaelhárítás esetén megfelelő szakértői hozzáértéssel rendelkezne.

A lokális üzemeltetésű, heterogén IT-infrastruktúra mellett szükséges megemlíteni azon speciális eszközöket is, melyek nem az adott egészségügyi intézmény tulajdonában vannak (például: MRI képalkotó, laboreszköz), hanem azokat bérli egy külső gyártótól/szállítótól. A gyártó/szállító általában az intézményi gépteremtől szeparáltan, lezártan helyezi el a szükséges háttérinfrastruktúrát, amelyhez csak neki van hozzáférése.

A hardverelemek mellett a biztonságos üzemelés másik fontos eleme a szoftverek folyamatos és biztonságos frissítése. A külső vállalkozó által fejlesztett termékek, például a háziorvosi (GP-k), vagy a kórházi információs rendszerek (Hospital Information System) vonatkozásában túlnyomórészt külső vállalkozó által fejlesztett termékekről beszélhetünk, melyek továbbfejlesztésére és biztonságos üzemeltetésére kiemelt figyelmet fordítanak az intézmények.

A medikai eszközök, gépek, berendezések alaprendszerén futó szoftverek fokozott kockázatnak vannak kitéve. Ezen eszközök életkorából fakadóan nagy biztonsággal vélelmezhető, hogy több, mint négyötödökön elavult operációs rendszer fut, és már nem kapnak szoftverfrissítést. Ez különösen aggasztó az orvostechnikai eszközöknél, ahol egy – gyakran beépített – operációs rendszer támogatásának megszüntetése rengeteg kockázatot és sérülékenységi veszélyt hordoz magában. Pl. az elterjedt Microsoft Windows XP és Windows 7 verziók gyártó általi frissítése és támogatása kivezetésével a továbbra is használatban lévő eszközök már nem fogják megkapni a szükséges javításokat.[44]

Ez természetesen nem azt jelenti, hogy ezeket a gépeket ki kellene vonni a forgalomból, hanem hogy fokozottan és folyamatosan ki vannak téve a kiberfenyegetéseknek, ezért IT-biztonsági szempontból javasolt a szeparált környezetben – például külön hálózaton –történő üzemeltetés és az indirekt módon – megfelelő tűzfalakon és határvédelmi rendszereken keresztül – történő internetes csatlakoztatás.

3.4.3. Az egészségügyben keletkezett adatok

Az egészségügyi adatok minden olyan információt tartalmaznak, amelyek az egyének vagy a lakosság egészségi állapotaival, reproduktív kimenetelével, halálának okaival és életminőségével kapcsolatosak. Az egészségügyi adatokat többféle aspektus szerint is csoportosíthatjuk. A legtágabb megközelítés szerint az egészségügyben keletkeznek strukturált (személyes adatok, vércsoport) és

[44] https://www.wired.com/story/most-medical-imaging-devices-run-outdated-operating-systems/

strukturálatlan (orvosjegyzet, hangfelvétel) adatok. Keletkeznek a páciens kezeléséből (kórkép), és az egészségügyi ellátással összefüggésben is adatok (orvosi eszközök, infrastruktúra). Felhasználási cél szempontjából is csoportosíthatók az adatok az egyének, a közegészségügy, valamint az orvosi kutatás és fejlesztés javára. Itt megkülönböztetünk elsődleges (ellátás nyújtása annak a páciensnek, akiről az adatgyűjtés történt) vagy másodlagos felhasználási célú adatokat. Az adatok újbóli felhasználása vagy másodlagos felhasználása a klinikai adatok más célra történő felhasználására vonatkozik, mint amelyre eredetileg összegyűjtötték az adott személy egészségügyi ellátásán kívül, például kutatási célból. Míg az egészségügyi információs technológia fejlődése kibővítette az adatgyűjtést és felhasználást, az egészségügyi adatok összetettsége akadályozta az egészségügyi ágazatban a szabványosítást.

Az egészségügyi nyilvántartásoknak három fő típusa létezik:

- Elektronikus betegrekord – Electronic Medical Records (EMR),
- Elektronikus egészségügyi feljegyzés (EESZT-ben: eKórtörténet) – Electronic Health Record (EHR),
- Személyes egészségügyi nyilvántartás – Personal Health Record (PHR).

Az orvosok és az ápolók jellemzően a papíralapú orvosi nyilvántartásokra támaszkodtak, hogy megismerjék a pácienst. Ha valamelyik dokumentum elveszett vagy megsérült, akkor a kezelő orvos nem férhetett hozzá ehhez az információhoz. Az elektronikus egészségügyi nyilvántartások fejlődésével az egészségügyi szakemberek könnyen elérhetik a páciensekkel kapcsolatos információkat. Az EMR a pácienst ellátó intézmény által rögzített és kezelt ellátási eseményének adatait rögzítő rekord, amely egymástól függetlenül történhet például a háziorvosi szoftverben vagy egy kórházi információs rendszerben is. Ezek a fájlok tartalmazzák a szükséges egészségügyi információkat, az állapotváltozásoktól a kezelések történetéig és az aktuális gyógyszeres kezelésig. A PHR a páciens állapotára vonatkozó, de nem az ellátórendszer szereplőinél keletkező adatokat, hanem a páciens a saját maga által végzett mérési eredményeit, naplóbejegyzéseit tartalmazza. Az EHR az egészségügyi ellátás során keletkező, a páciensre vonatkozó összes meglévő információra vonatkozik, amely az összes orvos vagy intézmény által gyűjtött valamennyi adatot tartalmazza. Míg az EMR szoftver az orvosi rendelő (ellátó intézmény) zökkenőmentes és hatékony működésének elősegítésére koncentrál, addig az EHR arra szolgál, hogy megosztott adatbázisba kerüljön a páciensre vonatkozó orvosi információk továbbítása érdekében. Ezek az adatok megoszthatók az engedélyezett felhasználókkal és több egészségügyi intézménnyel is.

Az EESZT-ben az elektronikus egészségügyi rekordként (EHR-ként) az olyan orvosi iratok kerülnek rögzítésre, mint a vizsgálatok, diagnózisok, beavatkozások, zárójelentések dokumentumai. Az EESZ-ben ezen iratok jelenleg strukturálatlanul kerülnek feltöltésre, azaz az elkészült dokumentum csak feltöltésre kerül szöveges dokumentum, vagy pdf formátumban, azok tartalmának megismeréséhez egy másik orvosnak meg kell nyitnia és átnéznie a fájlokat, amely időigényes folyamat. Az ellátó szakemberek számára az adatoknak a megfelelő mennyiségben és minőségben kell rendelkezésre állnia a döntéstámogatáshoz, ezért ennek feloldása érdekében az egységes adatstruktúra kialakítása kritikus szerepet játszik. Továbbá az unióban a tagállamok megkezdték az orvosi adatok határokon átnyúló megosztását az európai polgárok szabad mozgásának javítása érdekében. Ezek a kezdeményezések az interoperabilitást, mint az EHR-k létrehozásának lényeges tényezőjét ösztönzik. Az átjárhatóság széles körben való elérése azonban bonyolult kérdés. Az Európai Bizottság elindította az európai interoperabilitási keretet (EIF), amely meghatározza a közszolgáltatások interoperabilitásának elveit, különféle nézőpontokat átfogva. A megvalósítási szintre összpontosítva az európai interoperabilitási referencia-architektúra (EIRA) iránymutatásokat és specifikációkat nyújt, a vállalati architektúrák koncepcióját követve. Az EIRA újrahasznosítható építőelemeket kíván biztosítani, amelyek garantálhatják a műszaki és gazdasági fenntarthatóságot.

Az EU 2016/679 adatvédelmi rendelete az egészséggel kapcsolatos adatokat (tehát az EHR alapját) különleges kategóriának tekinti. Ezenkívül az EU 2016/1148 irányelv II. Melléklete az „egészségügyi ellátó intézményeket (ideértve a kórházakat és magánklinikákat is) alapvető szolgáltatások üzemeltetőjének minősíti". Az eIDAS-ra vonatkozó politikáról szóló véleményében az e-egészségügy hálózatának támogatására irányuló együttes fellépés (JASeHN.eu) azt sugallja, hogy az EHR-k cseréje során az eIDAS „lényeges" szintű rendszerét kell használni. A tagállamok azonban szorgalmazzák a magas eIDAS biztosítási rendszer elfogadását.

Az egészséggel kapcsolatos, az EHR formájában megfogalmazott adatok tehát olyan eszközök, amelyek átlépik a különféle biztonsági zónák határait (az egészségügyi intézmények az egymás közötti adattovábbításkor néha nyilvános internetet használnak). Az ilyen adatok megosztása potenciálisan kiteheti a veszélyeztetett páciensek életét, aminek következtében a rendszerben az értékelés szintje lényeges vagy magas lehet. Ezért az EHR-cserét működtető szoftverrendszereknek meg kell felelniük a tanúsítási rendszereknek jelentős vagy magas bizonyossági szinttel. A két szint közötti potenciális különbség: a jelentős lehet olyan szoftver esetében, amely csak a páciensek demográfiai adataival (név, kezelési kapcsolatok) és az orvosi dokumentumok kezelésével kapcsolatos cseréjével foglalkozik, míg a magas használható olyan szoftver komponensek esetében, amelyek képesek az orvosi dokumentumok cseréjére.[45]

Az adatok másodlagos felhasználása kapcsán az adatvédelem érdekében az eredeti, az egyénhez kapcsolódó adatokat anonimizálják, és pszeudonimizálják (álnevesítik). Az anonimizáció mint adatvédelmi módszer az az eljárás, amely megszünteti az összefüggést az azonosító adatkészlet és az érintett között. Ezt kétféle módon lehet megtenni. Először, a jellemzők eltávolításával vagy átalakításával a kapcsolódó adatkészletben úgy, hogy az asszociáció már nem egyedi, és egynél több érintettre vonatkozik. Másodszor, azáltal, hogy megnöveli az érintettek körét, így az adatkészlet és az érintett közötti kapcsolat már nem egyedi. Ez az adatvédelem leggyakoribb és legszélesebb körben elfogadott módszere az egészségügyi kutatásokban és az adatok másodlagos felhasználásában. A pszeudonimizálás, álnevesítés az anonimizálás egy speciális típusa, amely az érintettel való kapcsolat megszüntetése után asszociációt hoz létre az érintettre vonatkozó meghatározott jellemzők halmaza és egy vagy több álnév között. Ez azonban abban különbözik, hogy az információ eredeti szolgáltatója megőrizhet eszközöket az egyének azonosítására. Ezt gyakran kódok vagy más egyedi hivatkozások hozzáadásával érik el, hogy az adatok csak azok számára legyenek azonosíthatók, akik hozzáférnek a kulcshoz vagy az indexhez. A pszeudonimizálás lehetővé teszi ugyanazon egyénről szóló információk összekapcsolását oly módon, ahogyan a valódi anonimizálás nem.

A mesterséges intelligencia alkalmazásához elengedhetetlen az adatokhoz való hozzáférés. Az Európai Unió a jogszabályi háttér (FFD-rendelet[46] és a GDPR) megteremtésével kívánja elősegíteni, hogy a mesterséges intelligenciára épülő megoldások alkalmazásához és továbbfejlesztéséhez, a gépi tanuláshoz szükséges tömeges adatokhoz (big data) megfelelő keretek között lehessen hozzáférni. Az anonimizált adatok már nem tartoznak a GDPR hatálya alá, és a mesterséges intelligencia használatával az egészségügyi adatelemzés egyszerűbbé, gyorsabbá és hatékonyabbá válik.

[45] ENISA – Standards Supporting Certification – Analysis of Standards in Areas Relevant to the Potential EU Candidate Cybersecurity Certification Schemes; December 2019.

[46] Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről

3.4.4. Adattárolás, mentés

Az Eüak. törvény az egészségügyi és személyazonosító adatokkal kapcsolatban meghatározza, hogy a nyilvántartás eszköze lehet minden olyan adattároló eszköz vagy módszer, amely biztosítja az adatok biztonságát a véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

Az adattárolás módszerét és biztonsági követelményeit az intézménynek kell biztosítani, hogy megfeleljen a törvényben előírtaknak, arra vonatkozóan további hazai hivatalosan minősített technikai jellegű (architekturális, kibervédelmi) szabályozás nincs, iránymutatás a hazai, EU-s és nemzetközi ajánlásokban érhető el.

Az egészségügy speciális adattárolási és mentési igénye, hogy az adatok, információk rendelkezésre állását az emberi életciklusnak megfelelően kell biztosítani. A páciensek papír alapú betegrekordjai kartonozókban kerülnek/kerültek nyilvántartásra, a digitalizáció elterjedésével azonban ezek az adatok már egészségügyi információs rendszerekben kerülnek rögzítésre és tárolásra. A hosszú távú (a páciens élethosszáig tartó) adattárolás, adatmegőrzés tekintetében ez kihívás elé állítja az egészségügyet, hiszen a technológia fejlődésével az egészségügyi információs rendszereket is továbbfejlesztik, és kezelni szükséges, hogy a régebbi típusú (fájl)rendszerekben rögzített adatok is folyamatosan elérhetőek legyenek.

Ez egy információs rendszer esetében történhet adatmigrációval, azaz a régi rendszerből az adatok betöltésre kerülnek az új rendszerbe, de a korábbi rendszerekből történő adatbecsatornázással, a rendszerek összekötésével is, ez esetben a régi rendszer nem kerül teljesen kiváltásra. Az adatok becsatornázása esetén kihívás, hogy a korábbi fájlokat, fájlrendszereket is meg kell védeni a kor szerinti megfelelő titkosítással, kriptográfiával, valamint biztosítani szükséges annak kompromittálódásmentességét.

Az IT-infrastruktúráknál korábban említésre került, hogy az intézmények túlnyomórészt lokális infrastruktúra megoldásokat alkalmaznak, szigetszerű működésre vannak berendezkedve, továbbá az eltérő pályázati források a szigetszerű kialakítást és a heterogén eszközpark alkalmazását csak tovább növelik. Az adattárolás is lokálisan valósul meg az intézményeknél, a rendszerek tekintetében külön-külön infrastruktúrán, így a képalkotó rendszereknél (PACS-ok), az orvosi információs rendszereknél (HIS medical sysmtems) és az egyéb, intézményt kiszolgáló gazdálkodási rendszereknél is.

A gyakorlati tapasztalatok alapján általánosságban elmondható, hogy az intézményeknél a backup, azaz a másodlagos mentés ugyanazon géptermi infrastruktúrában megoldott, több esetben azonos elektromos hálózaton, amely nem nevezhető redundáns megoldásnak. A backup, másodlagos mentési megoldások esetében is előfordulnak olyan esetek, amikor csak az adatbázisokról készül egy mentés, azaz két példányban mentik, ún. replikát készítenek. Az intézmények IT-biztonsági szintjének felmérését a megvalósítás alatt álló EFOP-1.9.6 projekt hivatott felmérni.

Az adatok kezelésére és feldolgozására az ENISA által kiadott dokumentáció hasznos ajánlásokat tartalmaz. A jelentés bemutatja az ENISA online platformjának fókuszát és főbb funkcióit a személyes adatok feldolgozásának biztonsága érdekében. Ez a platform csak egy eszköz, amely nem helyettesítheti az adatkezelők vagy adatfeldolgozók oldalán a személyes adatok védelmére vonatkozó nagyobb megfelelési és elszámoltathatósági keret szükségességét. Ezenkívül az ENISA megközelítés csak akkor lehet hasznos a szervezetek számára, ha a személyes adatok biztonságának sajátosságait megfelelően átfogják és integrálják a biztonsági kockázatkezelési módszertanokba.[47]

[47] ENISA - Online platform for security of personal data processing – Reinforcing trust and security in the area of electronic communications and online services; December 2019

3.4.5. Az egészségügyi információs rendszerek felhasználói

Az egészségügyi információs rendszerek felhasználó szempontú csoportosítása bemutatásra került a rendszerek áttekintésekor. A kibervédelem szempontjából a legfontosabb tényező, hogy a felhasználó biztonságos csatornán, azonosítását követően és a jogosultságainak megfelelően férjen hozzá a rendszerekhez, az adatokhoz. Az egészségügyi szenzitív adatoknál a páciensek személyes adatainak védelme különösen fontos, ezért szükséges a megfelelő információvédelmi intézkedések kialakítása a rendszerekben és azok alkalmazása.

A legelterjedtebb a hagyományos biztonsági azonosítás, azaz az egyfaktoros azonosítás, ami a felhasználó azonosítójából és egy statikus jelszóból tevődik össze. A legtöbb egészségügyi rendszerben ez a legelterjedtebb módszertan, amelynek egyik sérülékenységi pontja, hogy a felhasználó személy megoszthatja jelszavát egy másik szereplővel, aki a jogosult nevében adatrögzítési és adatkezelési tevékenységet végez. A biztonság fokozása és a felhasználó tényleges azonosítása érdekében a többfaktoros azonosítás fokozza a biztonságot például egy fizikai eszközzel, amit csak a felhasználó birtokol.

Az EESZT rendszer az ágazati dolgozók számára kialakított Ágazati Portál felületen keresztül kétfaktoros azonosítással érhető el, amelynek egyik módja az eSzemélyi igazolvány használata. Ez az authentikációs folyamat a gyakorlatban például egy orvos vagy egy gyógyszerész esetében úgy működik, hogy a számítógéphez egy kártyaolvasó van telepítve, és az eSzemélyi Kliens program használatával az eSzemélyi igazolvány használható (eSZIG), mint autentikációs eszköz. Az eSZIG-gel történő e-azonosításhoz szükséges továbbá a felhasználó egyedi 6 számjegyű PIN kódja is, amelyet követően elérhetővé válik az EESZT felület.

Az EESZT fizikai kártyaolvasó hiányában elérhető hagyományos (fizikai) tokennel melyet igényelni szükséges, valamint az elterjedt webes banki belépéshez hasonlóan mobilTokennel is[48]. Az EESZT mobilToken applikáció mobiltelefonra történő letöltésével egy kényelmesebb alternatív kétfaktoros azonosítást nyújt az ágazati felhasználók számára, ahol a felhasználónéven kívül az említett applikációval generált egyszer használatos jelszó megadásával lehet hozzáférni az EESZT-hez.

Az EESZT Lakossági Portált ügyfélkapus azonosítóval és a TAJ szám megadásával lehet elérni.

A felhasználók tekintetében megkülönböztetünk normál és privilegizált felhasználókat. A privilegizált felhasználók olyan személyek, akik az átlagnál sokkal több jogosultsággal rendelkeznek, szinte az összes rendszert és adatbázist elérik. Az ilyen típusú fiókok feltörése minden hacker célja, hiszen minden rendszerhez könnyen hozzáférnek, és befolyásolhatják azok működését, adatokat nyerhetnek ki belőlük. A privilegizált felhasználók általában a rendszergazdák, rendszeradminisztrátorok és operátorok, akik az egész rendszer működését felügyelik, valamint az alkalmazás gazdák vagy adminisztrátorok, akik egy-egy alkalmazás felhasználónak nyújtanak támogatást, rendezik a jogosultságaikat.

Az információs rendszerekben történő eseményekről naplóbejegyzést (log) érdemes készíteni, hogy egy esetleges incidens esetén visszakereshetők legyenek a tevékenységek. Az információs rendszerek naplózás és tevékenység megfigyelés követelménye megjelenik az ISO 27001 szabványban is. Az ISO szabvány nem írja elő a központi naplózás végzését és naplóelemzési rendszer használatát (például SIEM), azonban egy incidens esetén az is nagy segítség lehet a felderítésben, ha a rendszer naplófájlba menti a tevékenységeket, azonban ez egy időigényesebb feladatot vetít előre. Az EESZT-ben teljes körű naplózás történik, mivel minden olyan rendszer, amely 5-ös besorolású, annak rendelkeznie kell nem megmásítható biztonsági naplózással is. Az eSZIG felhasználása, mint kétfaktoros azonosító eszköz, ezért is jelent a rendszer szempontjából extra biztonságot, mivel a személyigazolványát senki sem ruházza át másra, mivel az mindenki számára nagyon nagy személyes kockázatot jelentene.

[48] https://portal.eeszt.gov.hu/hu/belepes-az-eeszt-be

3.5. Kockázatok

Az egészségügyi ágazat az ismert és a még ismeretlen kockázatok kiküszöbölésével, valamint a szabályozási megfelelési követelmények összetettségének is meg kell felelnie. Az intézmények különösen kiszolgáltatott helyzetben vannak a páciensek személyes adatainak kezelése és védelme, az időkényszer és a napi működtetés jellege miatt.

Említésre került, hogy a hazai egészségügyi intézmények IT-biztonsági felmérése a folyamatban lévő EFOP-1.9.6-os projekt keretében valósul meg. Fontos, hogy a felmérés egy egységes módszertan és szempontrendszer alapján azonosítsa a kockázatokat és a fejlesztendő területeket. Meg kell határozni a védendő adatköröket, az adatgazdákat és a rendszer kulcsszereplőit. A kockázatelemzés eredménye alapján ki kellene alakítani egy központi szabályozást, egy minimumelvárást, melyet az egyes intézmények implementálnak a szabályzataikban és folyamataikban. Természetesen ehhez forrást is szükséges biztosítani az intézmény fenntartó részéről.

Az egészségügyi információs rendszerekre jellemző kockázatok lehetnek:

- elavult és hagyatéki (legacy) rendszerek használata – a régi rendszerekhez a feltárt biztonsági rések megszüntetése érdekében már nem adnak ki újabb biztonsági frissítést (patch), ezzel a rendszer ismert sérülékenysége nem kerül elhárításra;
- gyártói támogatás nélküli rendszerek;
- az elavult eszközök és régi kódnyelven írt rendszerekből fakadó beszállítói kitettség, megfelelő kompetencia hiánya – a régebbi eszközök használata kapcsán a megfelelő alkatrész beszállítás nehezebben oldható meg, szűkül a beszállítói kör, valamint a régebbi programozási nyelveken írt rendszerek kapcsán is szűkül az a programozói nyelvet ismerő kompetencia kör, akik az esetleges igényeket, problémákat kezelni tudnák, ezzel nő az intézmény kitettsége a szakemberek felé is;
- elavult kriptográfiai algoritmus használata – a szimmetrikus kulcsú titkosítási módszerek (például AES – Advanced Encryption Standard) egy kulcsot használ az üzenetek és fájlok titkosítására és dekódolására, az RSA aszimmetrikus eljárása egy privát és egy nyilvános kulcsot használ, és az informatika fejlődésével a kvantumszámítógépek már képesek lesznek az aszimmetrikus kódolást is feltörni ezért ún. „Kvantum-kriptográfiai”[49] kvantumrezisztens kriptográfiai módszereket kell kialakítani sürgősen. Az új fejlesztéseknél így lenne célszerű elindulni, mivel a nagytömegű szenzitív adatfelhasználás tekintetében az elavult kriptográfiai algoritmusok használata (DES, 3DES, RC4, IDEA) kockázatnövelő tényező;
- humán erőforrás – az emberi tényező minden esetben egyfajta kockázat, veszélyforrás, a hackerek is sok esetben használják az úgynevezett social engineering támadás formáját. Az alkalmazottak könnyen hozzáférhetnek az adatokhoz, rendszerekhez, így az érzékeny információkat személyes kapcsolat útján gyűjtik, és olyan emberi tulajdonságokkal élnek, mint a bizalom, a félelem vagy a segítőkészség (például: hallgatózás, váll szörf – váll felett átnéz a monitorra –, figyelemelterelés, megtévesztés) és számítógépes munka, amelyet az informatika segítségével hajtanak végre (például adathalászat, csali);
- rosszindulatú szoftver és adathalász-kísérletek – rosszindulatú szkripteket, kódokat telepítenek egy számítógépre vagy ellopják a bejelentkezési adatokat, veszélyeztethetik a teljes rendszert. Az egyik legnagyobb kihívást jelentő kérdés a rosszindulatú szoftverekkel kapcsolatban az, hogy csak egy látszólag hiteles linkre van szükség a rosszindulatú számítógépes

[49] „Kvantum-kriptográfia” (quantum cryptography): olyan technikák összessége, amelyekkel egy adott fizikai rendszer kvantummechanikai tulajdonságainak mérése révén – beleértve a kifejezetten a kvantumoptika, kvantumtérelmélet vagy kvantum-elektrodinamika által meghatározott fizikai tulajdonságokat is – közös „rejtjelezési” kulcs hozható létre.

jelenlét bevezetéséhez a hálózatába. Az egyik általános csalás az, ha az e-mailek hiteles megjelenésű webhelyekről kérnek bejelentkezési információkat;
- nem biztonságos mobil eszközök – a mobil eszközről történő bejelentkezés nem a megfelelő csatornán történik, például nyilvános wifi-hálózaton, vagy az egészségügyi intézmény belső hálózatára olyan külső eszközt csatlakoztatnak – BYOD, azaz hozd a saját eszközödet keretében, amelyen akár kártékony kód is lehet, ezzel kompromittálva a biztonságos működést, valamint kockázati forrás lehet az IoT eszközök sérülékenységi pontjai is;
- elvesztett és ellopott mobil eszközök – bármely mobil eszköz (laptop, mobiltelefon, tablet), amellyel egy rendszerhez hozzáférnek, felelőssé válik, mihelyst elveszik vagy ellopták. Az eszközhasználat korlátozásának hiányában (például PIN-kód, ujjlenyomat) rossz kezekben a felhasználó régi vagy tárolt bejelentkezési adataival könnyen hozzáférhetnek a rendszerhez. Ha a bűnöző hozzáfér a hálózathoz, kihívást jelenthet a káros tevékenységének a felismerése;
- gyenge felhasználói azonosítás – a kizárólag a felhasználónév és jelszó kombinációval történő rendszerbelépés nem garancia arra, hogy valóban a jogosult személy használja a rendszert, ezért egyre inkább a többfaktoros azonosítási technológiák használata javallott, ahol a felhasználó egy fizikai eszközzel is azonosítja magát (például token/mobiltoken, eSZIG).

A hazai egészségügyi információs rendszerekre általában jellemző:
- egységes üzemeltetési szabályok nélküli, decentralizált informatikai üzemeltetés (fontos megjegyezni, hogy önmagában a decentralizált üzemeltetés is lehet biztonságos, megfelelő szabályozási környezetben);
- elavult géppark, szerverek, hálózati eszközök és belső hálózat;
- elavult szoftverek, információs rendszerek, operációs rendszerek (például Windows XP);
- sokféle informatikai megoldások, egyedi, szigetszerű megoldások alkalmazása;
- ad-hoc jellegű fejlesztések, amelyek alapvetően a probléma elhárítására irányulnak;
- magas beszállítói kitettség;
- üzemeltetés gyártói támogatás hiánya;
- ingyenes megoldások használata forráshiány miatt;
- kevés magasabban kvalifikált munkaerő, motiváció, megfelelő bérezés hiánya.

Hazai példával élve a megfelelő biztonság garantálásához nem elég, hogy az EESZT 5-ös biztonsági besorolású, az adatokat szenzitivitásukból adódóan egészen a végpontig védeni kell. Erre tekintettel az egészségügyben is egységes IT-biztonsági elvárásokat kell megfogalmazni és biztosítani kell azok betartását is. Az adatvédelmi incidensek sajnos egyre gyakoribbak, melynek egyik példája az OGYÉI-t érintő adatvédelmi incidens,[50] ahol több ezer felhasználó neve, születési helye, ideje, lakcíme, mobiltelefonszáma és jelszava került a támadókhoz.

A kockázatok között megjelenik a nulladik napi támadás (zero day attack). A nulladik napi támadás egy olyan biztonsági rés, ami még ismeretlen a szoftver, a hardver vagy a firmware fejlesztője számára, és ezt a sérülékenységet használják ki a támadók haszonszerzés céljából. Azért hívják nulladik napinak, mert a gyártó/fejlesztő még nem fedezte fel a biztonsági rést, és még nem adott ki rá javítást (patch-et), valamint a kibervédelmi szoftverszállítók adatbázisába sem került még be, így ezek a programok sem ismerik fel ezt a fajta fenyegetést.

[50] https://infostart.hu/belfold/2019/10/28/tobb-tizezer-magyar-adatait-loptak-el

3.6. Enyhítési technikák

Az informatikai megoldások elterjedésével a kibervédelem minden ágazatot érint. Az intézmények évek óta próbálnak választ találni a kiberbiztonsági kérdésekre, és az egyik leghatékonyabb módszer az összes alkalmazott bevonása a hálózat biztonságának megőrzésébe. A konkrét támadások és az ellenintézkedések tovább fejlődnek a technológiával, de vannak általános alkalmazotti iránymutatások, amelyek segíthetnek a számítógépes bűnözők visszatartásában.

Az enyhítési technikák között megjelennek:
- humán oldalról az IT-biztonsági tudatosság növelése;
- biztonsági log, naplózás kialakítása;
- a jogosultságmenedzsment kialakítása és kikényszerítése;
- infrastruktúra oldalról a hardver- és szoftverelemek, azaz a rendszerek védelme és a megelőző intézkedések megvalósítása, szabályzatok és folyamatok kidolgozása;
- konfiguráció- és release-menedzsment kialakítása;
- a biztonságos adatkapcsolat, összeköttetés biztosítása;
- korai figyelmeztető rendszer (EWS – Early Warning System) használata a gyanús, deviáns esetek felderítésére és az incidensek megelőzésére;
- az incidens bekövetkezése esetén üzletmenetfolytonossági- és katasztrófa-elhárítási terv protokolljai mentén történő gyors és hatékony helyreállítás.

IT-biztonsági tudatosság növelése

A humán erőforrás kritikus pontja az IT-biztonságnak, az információvédelemnek. A munkavállalók oktatásával be kell mutatni, hogy a kiberbiztonságban milyen szerepük van, és az milyen hatást gyakorol egy páciens életére. Az intézmény rendszereinek biztonságáról szóló rendszeres eligazítások és kommunikációs csatornák használatával folyamatosan felhívható a munkavállalók figyelme a kiberbiztonságra. Az eljárások szabályozásával felállíthatók a kezelési protokollok az információk és a hálózatok - mind fizikai, mind virtuális – kezelésére, melyek teljesülését ellenőrizni szükséges.

A számítógépes bűnözők gyakran kihasználják az elavult szoftverek vagy más nem biztonságos hozzáférési pontok hibáit. Ennek leküzdése érdekében el kell végezni a szoftverfrissítéseket a gépeken, valamint a kétfaktoros hitelesítéssel és az automatikusan indított havi jelszófrissítéssel – amelyek megkövetelik az „erős” jelszó jellemzőit – lehet csökkenteni a kockázatot. A távmenedzselt munkaállomásokon és mobileszközökön segítség lehet az automatikus frissítések és az új jelszó kérések ütemezett beállítása. A mobil eszközkezelő (MDM – mobile device management) szoftver lehetővé teszi az informatikai rendszergazdák számára, hogy biztosítsák, ellenőrizzék és végrehajtják a táblagépekre, okostelefonokra és más eszközökre vonatkozó irányelveket, biztosítva, hogy az alkalmazottak ne sértsék meg a jelentős irányelveket, és adataik biztonságban maradjanak.

Infrastruktúra védelme

A 100%-ig biztos informatikai védelem nem létezik, de minimalizálni lehet az egészségügyi számítógépes rendszerek sebezhetőségét. Ehhez azonban egy robusztus kiberbiztonsági rendszert kell telepíteni, amely lefedi az egész hálózatot, beleértve a felhőalapú tárolást is, valamint természetesen ennek a forrásigénye is határtalan, és ez sem garancia a teljeskörű védelemre.

Az adatok titkosításával, a biztonsági követelmények betartásával és az enyhítési technikák alkalmazásával minimalizálható az incidens bekövetkezése.

Az információs rendszerek és hálózatok javasolt biztonsági intézkedései:

- Hálózati térkép megértése –olyan technológia használata, amely áttekintést nyújt a hálózaton lévő eszközökről és tárolóeszközökről, amellyel láthatóvá válnak, hogy az információk milyen módon sebezhetők, valamint amikor új vagy jogosulatlan eszközök csatlakoztak/próbálnak csatlakozni a rendszerhez. Ez a hálózati térkép segít a hálózat minden eszközéhez a hozzáférés és a korlátozások meghatározásában, csökkentve a rosszindulatú tevékenységet.
- Szoftverek frissítése, karbantartása – fontos, hogy a szoftverek és operációs rendszerek minden információja naprakész legyen. Ezek a frissítések kritikus javításokat tartalmaznak, amelyek visszatartják a potenciális számítógépes bűnözőket, akik a korábban felfedezett szoftverek hiányosságaira támaszkodnak. Szoftverfrissítés hiányában a bűnözők kihasználhatják a korábbi verziók által hátrahagyott lyukakat.
- Vírusirtó és kémprogram eltávolító programok – az esetleges támadások ellen az eszközünk mindig legyen védve naprakész vírusirtó és kémprogram eltávolító szoftverrel, valamint mielőtt egy hordozható eszközt (például pendrive) csatlakoztatunk számítógépünkhöz, végezzünk rajta víruskeresést.
- Események naplózása (log), valamint SIEM használata – a valós idejű IT-környezetben történő biztonsági incidensek vagy események azonosítására, megfigyelésére, rögzítésére és elemzésére a központosított naplózási rendszer (security log) használatos. A SIEM (Security Incident and Event Management) technológia összegyűjti és integrálja a biztonsági eszközök, hálózati infrastruktúra, rendszerek és alkalmazások által előállított eseményadatokat. Az elsődleges adatforrás a naplóadatok (logok), de a SIEM technológia másfajta adatot is feldolgozhat, például hálózati telemetriát (folyamatok és csomagok). Az eseményadatokat összekapcsolják a felhasználókkal, eszközökkel, fenyegetésekkel és sebezhetőségekkel kapcsolatos környezeti információkkal. Ez a technológia az események valós idejű elemzését nyújtja a biztonsági megfigyeléshez (pl: viselkedéselemzés), a lekérdezéshez és a hosszú távú elemzésekhez – például a történeti elemzéshez – és az események kivizsgálásának és kezelésének, valamint a jelentéseknek az egyéb támogatásához. Egy SIEM rendszer segítségével viszont gyorsan áttekinthetők a releváns információk az összefüggések keresésével, megkönnyítve a gyanús események felismerését, kivizsgálását.
- Kibervédelmi műveleti központ (SOC – Security Operations Center) felállítása – a kiberbiztonsági fenyegetések és események megelőzésére, felfedezésére, értékelésére és azokra való reagálásra szolgáló eszközzel.
- Virtuális magánhálózati titkosítás használata – a hálózati kapcsolat titkosítása remek lehetőség a hálózati adatvédelem fokozására és a lehetséges hackerek blokkolására. A virtuális magánhálózat (VPN) kódolja az adatokat, így mások nem láthatják, mi történik a számítógépen. Tehát még ha megfigyelik is a számítógép adatkapcsolatát, akkor sem lehet belőle információt kinyerni. Kiemelten fontos a titkosított csatorna használata a távoli hozzáférés, távmunka esetén.
- Rendszeres auditok lebonyolítása – a rendszergazdáknak, rendszeradminisztrátoroknak rendszeres ellenőrzéseket kell végezniük, és legyen kétlépcsős az azonosítási folyamat, amely megköveteli a személyazonosság ellenőrzését. A hozzáférési hitelesítő adatokat szintén rendszeresen felül kell vizsgálni annak biztosítása érdekében, hogy a korábbi vagy áthelyezett alkalmazottak ne férjenek hozzá a páciens adataihoz.
- Jogosultságbeállítások kezelése – javasolt csak a munkavégzéshez szükséges rendszerekhez és adatokhoz való hozzáférés biztosítása a jogosultságok beállításával, csökkentve ezzel a visszaélések lehetőségét. Természetesen a jogosultságbeállításokat időnként felül kell vizsgálni.
- Professzionális szakértői támogatások igénybevétele (support) – egy egészségügyi intézményben számos különféle informatikai eszköz, információs rendszer, orvosi-medikai szoftver és eszköz van, amelyek gyártói/szakértői, azaz specifikus támogatás igénybevétel esetén biztonsági szempontból is naprakésszé tehetők.

Biztonságos adatkapcsolat, összeköttetés

- Az egészségügyi intézményeknél elengedhetetlen az adatkapcsolat folyamatos, biztonságos és magas színvonalú rendelkezésre állása. Az internet biztosítását dedikált vonalon valósítják meg, ez lehet egy külső szolgáltató által biztosított bérelt vonal, vagy a hazai egészségügy kiszolgálását biztosító Nemzeti Távközlési Gerinchálózat (NTG). Az ilyen típusú összeköttetések biztonságosak, és az egyes intézményi telephelyek között is zárt kapcsolat kerül felépítésre, azaz az adatáramlás nem kerül ki a publikus internetre.

Üzletfolytonossági és katasztrófaelhárítási terv, rendszer-helyreállítás

- Az életmenet folytonosság terv (BCP – Business Continuity Plan) technikailag azokra az eszközökre utal, amelyekkel elkerülhető az üzleti veszteség. Meghatározza a vészhelyzeti állapot esetén a rendelkezésre álló erőforrások és kompetenciák felhasználásával a működés folyamatosságára vonatkozó üzleti követelményeket, beleértve a katasztrófa utáni helyreállítási terv (DRP) üzleti követelményeit is.
- Az informatikai katasztrófaterv (DRP – Disaster Recovery Plan) egy olyan haváriaterv, ami az incidens bekövetkezése esetén részletesen leírja, hogy a lehető leggyorsabban hogyan lehet visszaállítani a kritikus funkciókat ellátó rendszereket, valamint hogyan lehet visszaállítani a normál üzletmenetet. Ezt az intézményeknek az üzemelő rendszereik alapján szükséges összeállítaniuk, amely tartalmaz minden olyan információt és lépést, ami az 'újraindításhoz' kell.

Az enyhítési technikák lehetőségeit az intézmények sajátosságai alapján lehet pontosabban meghatározni – mennyi telephelyen üzemel az intézmény, milyen típusú ellátást valósít meg – így természetesen többféle módszer létezik. Ezen módszerek és technológiák lehetnek például:

- felhőtechnológia, felhőalapú adattárolás;
- központilag üzemeltetett és menedzselt megoldások (munkaállomás, adatkapcsolat, orvostechnikai eszközök, HIS-ek);
- georedundáns megoldások;
- hardver/szoftver konszolidációs megoldások.

3.7. Esettanulmány

A kibertámadások komoly fenyegetést jelentenek az egészségügy számára is. A kiberbűnözők a különböző támadási technikákkal akár a páciensek adatait is módosíthatják. Ezzel olyan károkat is okozhatnak, mint a betegek diagnózisainak manipulálása, ami félrekezeléshez is vezethet. A különböző képalkotó, diagnosztizáló medikai eszközök feltörésével egy páciens esetében akár rákbetegséget is lehet tévesen azonosítani.

Egészségügyi szektor specifikus eset, egy 2019-ben publikált tanulmány szerint[51] a hackerek tüdőrák esetén megtéveszthetik a radiológusokat és a mesterséges intelligencia szoftvereket. Egy ilyen módszer lehet a közbeékelődéses támadás (man-in-the-middle device), amely eltéríti a szkenner és a számítógép közötti kommunikációt úgy, hogy a telepített eszköz a CT-szkennelés képét elfogja, manipulálja, és már a hamisított képet továbbítja a számítógép felé.

[51] https://healthcare-in-europe.com/en/news/hackers-can-manipulate-cancer-scans.html

A 2020. márciusában kitört európai koronavírus járvány kapcsán is több IT-biztonsági incidens történt. Egy cseh kórházat ért kibertámadás, amely során az egyes alrendszerek megbénításával ellehetetlenítették az egyes laboratóriumi rendszerekből történő adatátadást a központi adatbázisba, késleltetve ezzel a koronavírus teszt eredményeit.[52] Szintén a járvány európai kibontakozásakor akarták megszerezni a WHO dolgozóinak jelszavait úgy, hogy a hackerek egy olyan adathalász oldalt hoztak létre, amelyik a WHO saját belső levelezésének az arculatát utánozza, miközben a dolgozó a belső levelezésbe szeretett volna belépni.[53]

Az alább bemutatott két esetben a támadó(k) célja, hogy korlátozzák, vagy teljesen blokkolják a tárolt egészségügyi adatokhoz való hozzáférést, amelyet csak egy bizonyos pénzösszeg kifizetését követően oldanak fel, vagy a páciensek személyes betegrekordjait tulajdonítsák el, esetleg módosítsák azokat. Az adatok titkosítása esetén azonban nincs arra garancia, hogy a feloldásához szükséges kulcsot a támadók valóban átadnák, ellenben további váltságdíjat követelhetnek. Minkét esetben érzékeny egészségügyi adatok kerülnek veszélybe, és a támadás sikerességéhez szükséges a belső, humán tényező hozzájárulása is.

3.7.1. Rosszindulatú, kártékony szoftvertámadások az egészségügyi információs rendszereknél

A malware, azaz malicious software a kártékony programok összefoglaló neve. Ezek lehetnek trójai vírusok, férgek, zsaroló programok, kéretlen programok stb., amelyek általában a felhasználó tudtán kívül jutnak a rendszerbe, a biztonsági réseket kihasználva, ami visszavezethető emberi mulasztásra is, valamint a rendszer sebezhetőségének kihasználására is.

A rosszindulatú programok komoly veszélyt jelentenek a kórházak számára. Ennek oka, hogy a rosszindulatú programok lehetővé teszik számos szervezet megtámadását meglehetősen alacsony erőfeszítéssel, nagyon heterogén felülettel a heterogenitás és az eszközök (hordozható eszközök, számítógépek, mobil eszközök stb.) számát tekintve. Ami a rosszindulatú programok kategóriáit illeti, az alábbiakat különböztetjük meg:

- zsarolóvírusok (ransomware), fájlok eltérítése rendszerekről;
- spyware, megfigyelő rendszerek;
- belső rendszeren terjedő vírusok;
- férgek (számítógépek között terjednek);
- trójai (rejtett módon);
- rootkitek;
- exploit kitek (rosszindulatú eszközkészletek, amelyekkel a biztonsági rések, sebezhetőségek kihasználásra kerülnek).

Az elmúlt néhány évben a kórházak különösen a zsarolóvírus-támadások célpontjai voltak - ez egy olyan kártékony program, amely korlátozza a fertőzött számítógéphez való hozzáférést. A fertőzött számítógép fájlrendszer elemei titkosításra kerülnek, és a rendszergazda / felhasználó számára már nem állnak rendelkezésre (például CryptoLocker, e-mail csatolással és botnettel terjesztve). Ennek terjedése még veszélyesebbé válhat, ha megfertőzi a kórházi hálózatba kapcsolt eszközöket, esetleg IoT-okoseszközöket. A támadó általában váltságdíjat követel a felhasználótól, hogy a fájlok titkosítását, a korlátozások megszüntetését feloldja. Ennek okán kiemelt figyelmet kell fordítani a zsarolóvírusokra a teljes rosszindulatú program spektrumon belül.

[52] https://www.scmagazineuk.com/coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194

[53] https://www.businessinsider.com/world-health-organization-hack-tried-steal-passwords-with-fake-website-2020-3

A bemutatásra kerülő incidens összefüggései

Azért, hogy az információs rendszerhez való hozzáférés korlátozásra kerüljön a zsarolóvírus például a fertőzéssel zárolhatja a rendszert, vagy titkosíthatja a fájlok egészét vagy egy részét a merevlemezen. Elmondható, hogy a zsarolóvírusok befolyással vannak az információs rendszerekre (például vállalati rendszerek vagy klinikai hálózatba kötött rendszerek) és a nem rendszerszinten tárolt adatokra, információkra is.

A megelőzés érdekében a legjobb gyakorlatok általában a következők:

- a szoftver javítása (patch) és folyamatos frissítése (update) a leggyakoribb és legismertebb sérülékenységek megakadályozása érdekében, a sikeres malware támadások kezelésére;
- antimalware és anti-spam szoftverek futtatása, amely ez lehetővé teszi a rosszindulatú szoftverek felismerését és eltávolítását vagy karanténba helyezését. Ezt nemcsak az informatikai eszközökön / felhőalapú adatokon / alkalmazásokon, hanem a klinikai hálózatba kapcsolt információs rendszereken, az orvostechnikai eszközökön, az egészségügyi információs rendszerhez való csatlakozáshoz szükséges mobil eszközökön is meg kell tenni;
- teljes vagy növekményes (változások átvezetésével) biztonsági mentések készítése rendszeres időközönként, amely védi a kórházi rendszert a zsarolóvírusok, a fizikai támadások és akár a természeti katasztrófák esetén is.

A zsarolóvírusok magas biztonsági kockázatúak, mivel fennáll annak a veszélye, hogy a kódolt adatok örökre elveszhetnek, azokat már nem lehet visszaállítani, valamint – jelen esetben – érzékelhetően csökkentheti a kórház működési képességeit és az elérhető szolgáltatásait. Egy ilyen támadás bekövetkezésének valószínűsége közepes, de növekvő tendenciát mutat. A hatások lépcsőzetes fokozása az átlagos kórházakban korlátozottak, mert véget ér a támadás miután a fájlokat titkosították, vagy korlátozták a rendszer hozzáférhetőségét. Azonban ez nem mondható el egy okos kórházról, ahol minden digitális rendszer szorosan egymáshoz kapcsolódik, és a hálózatba kapcsolt orvostechnikai eszközök működése attól függ, hogy képes-e elérni az adott (kezelő) rendszert.

A biztonsági másolat rendelkezésre állása jelentősen befolyásolhatja a rosszindulatú programok (ransomware) támadásainak helyreállítási idejét és erőfeszítéseit. A rendszerképek (image-ek) vagy biztonsági mentések visszaállításának folyamatait, a támadás észlelésének és a támadásra való reagálás gyorsaságát is figyelembe kell venni.

Az esettanulmányban bemutatott incidenssel mérhető a kórház képessége, hogy hogyan reagál az adatok ellenőrzésének hiányára, a vállalati vagy a klinikai rendszer irányíthatatlan hanyatlására, valamint az elérhető szolgáltatások számának csökkenésére.

Az esettanulmány a következő felhasználási eseményeket foglalja magában, amelyek egyenértékű fenyegetéseknek felelnek meg:

- támadás az IT-infrastruktúra ellen;
- zsarolóvírus támadás.

A fenti, tipikus sebezhetőségek a rosszindulatú szoftverekkel kapcsolatosak. A rosszindulatú szoftverek komoly veszélyt jelentenek az okos kórházak számára, mivel egy olyan rosszindulatú szoftver, amely többé-kevésbé egy meghatározott szervezethez vagy egy meghatározott típusú szervezethez irányul, átveszi az irányítást vagy megtagadja a berendezésekhez, eszközökhöz vagy rendszerekhez való hozzáférést. A rosszindulatú programok olyan személyek vagy szervezetek (támadók) digitális szándékos cselekedetei, amelyek célja egy másik személy működési képességének jelentős csökkentése, veszélyeztetése vagy ellehetetlenítése.

Általában az érintett rendszerek/ szereplők a következők:

- információs rendszerek;
- kórházi berendezések és eszközök;
- kórházi személyzet;

különös tekintettel a hálózatba kötött orvostechnikai eszközökre, a mobil és hordható eszközökre, a PC-kre és laptopokra, valamint a biztonsági mentési és tárolási eszközökre.

Szükséges megjegyezni, hogy egy zsarolóvírus támadás sikerességéhez szükséges az emberi mulasztás is, egy belső alkalmazott hozzájárulása is. Ezért is elkerülhetetlen az intézmények részéről a munkatársak képzése, IT-biztonsági tudatosságának növelése.

Az ellenintézkedések a következők:

- javítani kell a szervezeti folyamatokat, például az időszakos biztonsági mentések ütemezését, védetté és igény szerint elérhetővé tételét;
- a személyzet képzése és tudatosságnövelése a támadás gyors észlelése és a fertőzött elemek kikapcsolásával történő megfelelő reagálás érdekében;
- antivírusok és anti-spam, szoftverek javítása és frissítése;
- hálózati szegmentálás a hálózat kritikus részeinek elkülönítésére;
- hitelesítési és engedélyezési infrastruktúra beállítása.

3.7.2. Támadás IT-infrastruktúra ellen

Kezdeti szakasz, előkészítés

Egy bűnszervezet támadást tervez a kórházi információs rendszerben az érzékeny páciensadatok és elektronikus egészségügyi nyilvántartások ellen.

A zsarolóvírus támadások támadási vektorokként vezeték nélküli kommunikációt használnak, a bűnözők spam és e-mailek útján továbbítanak rosszindulatú szoftvereket, amelyek célja a kórházi felhasználók megtévesztése a melléklet megnyitásával vagy egy linkre történő kattintással. Az e-mail tárgya és a melléklet közvetlenül kapcsolódik a kórházi tevékenységhez, amelyek olyan fájlokat reprezentálnak, mint például csatolt számlák, repülőjegyek, megrendelések, valamint mindenféle adminisztratív jellegű, hamis tartalmú fájlok.

A fertőzés rendszerbe való kerülésével a rosszindulatú szoftver titkosítja az irodai alkalmazások fájljait, a pdf dokumentumokat, szöveges fájlokat, adatbázisokat és multimédia fájlokat is. A fertőzés minden kórházi osztályt kritikusan érint.

A dokumentumok titkosítása után az áldozat kórház megkeresésre kerül, hogy a titkosítás feloldása érdekében fizesse meg a váltságdíjat, ami általában az intézmény profiljától és a becsült árbevételtől függ.

Kiberbiztonsági szakértők azt tanácsolják a fertőzött felhasználóknak, hogy ne fizessék meg a támadóknak a szükséges visszafejtési díjat, hanem készítsenek másolatot a veszélyeztetett adatokról és forduljanak a rendőrséghez. A váltságdíj megfizetése után nem garantálható, hogy az elkövetők betartják ígéretüket és valóban megadják az adatok feloldásához a kulcsot, ráadásul ugyanaz a csoport ismét megcélozhatja ezt az intézményt, további összegeket követelve. Végül, de nem utolsósorban, ezek a pénzügyi hasznok tovább segíthetik a támadókat, hogy egyre kifinomultabb számítógépes fenyegetéseket alakítsanak ki, amelyek hosszú távon egyre több incidenshez vezetnek.

Lépések
1. lépés: A hackerek kriptoférget fejlesztenek ki a fájlrendszerek megfertőzésére és a fertőzött számítógépekhez való hozzáférés akadályozására.

2. lépés: A hackerek számos e-mailt küldenek a kórház különféle osztályaihoz: adminisztratív csoporthoz, az informatikai részleghez, orvosi személyzethez, és a csatolt fájlok tartalmazzák a kriptoférget.

3. lépés: Az aktiválást követően a kriptoféreg terjed a kórház számítógépes hálózatán, és elkezdi a rendszerfájlok titkosítását, megakadályozva a felhasználók hozzáférését.

4. lépés: A kórház informatikai osztálya leállítja az informatikai infrastruktúrát, megszakítja a számítógépek csatlakoztatását, és mindegyiküknél újratelepítést végez, továbbá új biztonsági protokollok kerülnek bevezetésre.

5. lépés: A kórház vezetője a hatóságokhoz (rendőrséghez) fordul, hogy speciális informatikai segítséget kapjon a kórházi adatok helyreállításához és a váltságdíj megfizetésének elkerüléséhez.

Kezdeményező szereplő

Külső hacker – távoli támadó (szervezett bűnözés). Egy kórházi alkalmazott, aki kap egy e-mailt egy csatolt fertőzött fájllal vagy linkkel.

Támogató szereplők

Az IT-csoport és az összes kórházi személyzet, aki hozzáférést biztosít az e-mailhez a kórházi hálózaton keresztül.

Végső rendszerállapot

A művelet sikere esetén az összes hálózat, páciensadat, orvosi információ és a legtöbb számítógépes fájl nem érhető el, mivel a hackerek az összes informatikai alapú rendszert titkosították, beleértve a biztonsági mentést is. A követelt pénzösszeget a hackerek megkapják.

A művelet sikertelensége esetén az informatikai osztály tudatában van, hogy mely adatállomány került titkosításra, és újrakonfigurálja a hálózati hitelesítési beállításokat. A fertőzés mértékétől és az érintetlen biztonsági mentési fájlok újratelepítésének idejétől függően a titkosításra került adatok visszaállítása megkezdődik.

Bementek

Információ a kórházi e-mailekről: az adminisztráció, az informatikai csoport és az egészségügyi személyzet elérhetőségei (telefonszám, email cím) megtalálható az interneten.

Kimenetek

A rosszindulatú programok támadása veszélyezteti az érzékeny információkat. A célpont a páciensadatok és az egészségügyi nyilvántartás hozzáférhetőségének korlátozása. Mivel a legtöbb kórházban lévő számítógép csatlakozik az internethez: adminisztratív, informatikai csoport, orvosi személyzet, a rosszindulatú programok sikeres támadása blokkolhatja a kórházak tevékenységét, és ezzel elveszthetti az egészségügyi adatbázisok, a páciensek adatainak és az egészségügyi szolgáltatások elérhetőségét, azaz mindent, ami IT-alapú rendszert használ.

3.7.3. Humánalapú támadás a kórházi személyzet ellen

Kezdeti szakasz, előkészítés

Az emberi befolyásolhatóságra alapozó úgynevezett social engineering támadások során a támadók általában három célkitűzést határoznak meg: információgyűjtés, csalás elkövetése vagy a rendszerekhez való hozzáférés. Az esetben bemutatásra kerül egy kórházi dolgozó (orvos) fiókjához tartozó bejelentkezési adatok megszerzése.

A kórházi nagy forgalom és a különféle szerepekben részt vevő különböző alkalmazottak száma miatt az orvosok gyakran nem ismerik jól az informatikai alkalmazottakat, amely fordítva is igaz lehet. Ebben a helyzetben könnyű olyan hamis, kritikus fontosságúnak tűnő kérdést létrehozni, amelylyel megszerezhetőek a hitelesítési adatok. A felhasználói adatok megszerzéséhez gyakran elegendő egy telefonhívás, és hatékonyabb, mint egy adathalász kísérlet, mivel az áldozat nyomás alá kerül a telefonhívás során, a reakcióidő, válaszidő másodpercekre rövidül.

Lépések

1. lépés: A külső személy (hacker) szeretné megszerezni egy vagy több páciens adatait.

2. lépés: Ehhez a hacker az interneten vagy a kórház webhelyén megkeresi azokat a speciális orvosokat, akik kapcsolódhatnak a beteghez (például sebészet, patológia stb.). A szóba jöhető orvosok ismeretében pár perc alatt telefonszámot, azaz elérhetőséget is lehet találni az interneten keresztül.

3. lépés: A hacker összegyűjti a szükséges információkat a kórházon belüli informatikai csoportról, annak érdekében, hogy hitelesebben tudja magát kiadni az egyik informatikusnak.

4. lépés: A hacker telefonhívás útján kapcsolatba lép az orvossal, még ha az asszisztens is veszi fel és úgy tesz, mintha egy informatikai személyzet tagja lenne, azaz belső munkatársnak adja ki magát. Elmondja, hogy a kórházi adatokat tartalmazó programok karbantartásáról és / vagy frissítéséről van szó. A beszélgetés során nyomás alá helyezi az orvost, hogy milyen bonyolult lépéseket igénylő műveletekről van szó, ami időigényes, és meggyőzi az orvost, hogy adja meg a bejelentkezési adatait, azaz felhasználónevét és jelszavát, hogy elvégezhesse a feladatát. Ha gyanúsnak is tűnik az beszélgetés, nem minden orvos hívja vissza az informatikai személyzetet ellenőrzés céljából. Ez a módszer súlyos sebezhetőséget eredményez a hitelesítési és engedélyezési rendszerben, ha a személyes azonosítási adatokat illetéktelenek kezébe kerülnek.

5. lépés: A hacker az orvos fiókján keresztül hozzáférhet a rendszerekhez, és adatokat tulajdoníthat el, valamint módosíthatja (kompromittálhatja) is azokat.

Kezdeményező szereplő

A hacker, aki rövid időn belül akar hozzáférni egy regisztrált felhasználó bejelentkezési adataihoz.

Támogató szereplők

Az orvos és/vagy az informatikai csoport jóhiszeműségből elősegítheti a hacker a belső információkhoz való hozzáférését.

Végső rendszerállapot

A művelet sikere esetén a páciensek személyes betegrekordjainak és érzékeny adatainak eltulajdonítása komoly következményekhez vezethet, valamint az orvos és az érintett intézmény hírneve is csorbul. Nagyobb mennyiségű, akár több ezer betegrekord ellopása esetén az adatok a sötét weben történő értékesítése is előfordulhat.

Súlyos következményei lehetnek, ha a hacker az orvos jogosultságával a nyilvántartó rendszer(ek)ben a betegrekordokat módosítja, kompromittálja.

A támadás észlelése esetén az érintett orvos fiókjából végzett események a naplóbejegyzésekből visszakereshetők, a módosított adatok a mentésekből visszaállíthatók, ez a műveletsor azonban hetekig is eltarthat. Az meghackelt orvos bejelentkezési adatait haladéktalanul módosítani kell, javasolt a kétlépcsős bejelentkezés bevezetése, például mobiltelefonra SMS-ben küldött jelszó használatával.

Bemenetek

Az orvosokkal, orvoscsapatokkal kapcsolatos információk széles körben elérhetők az interneten és a kórház honlapján. A névjegyeket (e-mail címek, telefonszámok stb.) könnyű megtalálni. Az informatikai személyzettel kapcsolatos információk általában szintén könnyen megtalálhatók a kórház honlapján.

Kimenetek

A humán alapú támadás az érzékeny információk eltulajdonításához, kompromittálódásához vezethet, amellyel a hacker egyik vélhető célja a pénzszerzés. Mivel az információs rendszerek és eszközök szorosan kapcsolódnak egymáshoz egy kórházban, sikeres humán alapú támadás esetén veszélybe kerül az infrastruktúra nagy része.

3.8. Összegzés

Az egészségügyi információs rendszerek kibervédelme kiemelten fontos, tekintettel a rendszerekben kezelt személyes adatok szenzitivitására, a gyógyításban betöltött funkciójára és a páciensek rekordjaira.

Szabályozási oldalról az Európai Unió is felismerte az adatok, kiváltképp az egészségügyi adatok fontosságát, amelynek védelme érdekében többek között a NIS-irányelv és a GDPR rendelet ad keretet. A GDPR rendelet egy közvetlenül hatályos joganyag, addig a NIS-irányelvet implementálni szükséges a hazai joganyagokba. Az egyenszilárdságú, egységes hazai szabályozási környezet megteremtése a jogalkotó részéről hozzájárul az egészségügyi adatok, információs rendszerek kibervédelmi színvonalának emeléséhez.

Összefoglalva a kibervédelmi lehetőségek tárházát az egészségügyi információs rendszerek biztonsági színvonalának növeléséhez és az egészségügyi adatok védelméhez az alábbi intézkedések megvalósítása járul hozzá:

- Követelményrendszer, minimumelvárás megfogalmazása az intézményi informatikai architektúra, az infrastruktúra- és az alkalmazásüzemeltetésre vonatkozóan.
- Intézményi (és/vagy állami) szintű központi IT-biztonsági megoldások bevezetése melyek lehetnek:
  - egységes vírusirtási, és hálózati adatforgalom monitorozási készség megteremtése;
  - tevékenység naplózási, monitorozási és elemzési feltételek megteremtése a biztonsági incidensek azonosítása érdekében;
  - egyedi IT-biztonsági megoldások kiváltása, központilag üzemeltetett és menedzselt megoldások kialakítása;
  - biztonsági mentések készítése, (geo)redundáns infrastruktúra kialakítása;
  - kibervédelmi műveleti központ (SOC) kialakítása (méretgazdaságossági okokból megfontolandó egy centralizált működési modellben történő működtetés);
  - biztonsági incidens esetére katasztrófaterv, haváriaterv készítése a rendszerek mielőbbi üzemszerű működésének visszaállítása érdekében;

- Az elavult, gyártói támogatás nélküli eszközök cseréje, lehetőség szerint homogén eszközpark kialakítása, az eszközökre kiadott javítások telepítése.
- IT infrastruktúra konszolidáció, a régi, hagyatéki (legacy) rendszerek kiváltása, a szigetszerű üzemeltetési környezet felszámolása.
- Zárt rendszerű, biztonságos adatkapcsolat kialakítása az intézmények és telephelyeik között (bérelt vonal, távközlési gerinchálózat stb.).
- Tűzfalakon és határvédelmi rendszereken keresztüli indirekt internetes be- és kilépési pont kialakítása.
- Szoftverek folyamatos frissítése, a már nem támogatott termékek (Windows XP, 7) cseréje.
- A munkatársak IT-biztonsági tudatosságának növelése (oktató anyagok, hírlevelek, képzések).
- Az intézményi informatikusok oktatása, folyamatos továbbképzése.

Kitörési pont lehet a hazai egészségügy számára a célzott informatikai pályázati források biztosítása, amellyel a pályázatot kiíró kormányzati szerv az egységes IT-infrastruktúra és követelményrendszert a pályázati feltételek között nevesíthetné.

Az egészségügyi ágazatot irányító minisztériumnak fontos szerepe van a stratégiai célok meghatározásában, a szereplők részére történő iránymutatásban. A jelenlegi működési modell alapján az intézmények infrastruktúrájukat egyedileg alakítják ki, amely csak növeli a szigetszerű működési környezetek számát. Megfontolandó bizonyos tevékenységek esetében a központi, centralizált működési modell kialakítása és működtetése az egységes IT-biztonsági megoldások alkalmazása érdekében.

3.9. Melléklet

Áttekintett, felhasznált jogszabályok, rendeletek, ajánlások:

- 1992. évi LXVI. törvény a polgárok személyes adatainak nyilvántartásáról és lakcímének nyilvántartásáról
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről és az azt felváltó 2021. évi XCI. törvény a nemzeti adatvagyonról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról; érintett szakaszok: 1. számú melléklet
- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól és az azt felváltó 271/2018. (XII. 20. Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 386/2016. (XII. 2.) Korm. rendelet az egészségbiztosítási szervekről
- 39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról
- Az Európai Parlament és a Tanács 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (GDPR)
- Az Európai Parlament és a Tanács 2016. július 6-i 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS-irányelv)

4. JERABEK GYÖRGY– INFORMÁCIÓBIZTONSÁG AZ ÖNKORMÁNYZATI SZEKTORBAN

4.1. A kezdetekről

A 2013. évi L. törvényt (a továbbiakban: Ibtv.) megelőzően sem az entrópia uralta a magyar közigazgatás – köztük az önkormányzati szektor – IT-biztonsági rendszereit. Jelen voltak a Közigazgatási Informatikai Bizottság (KIB) ajánlásai,[54] elérhetők voltak a ma is létező – azóta természetesen megújított – IT-biztonsági szabványok,[55] rendelkezésre álltak ágazatspecifikus követelményeket és kialakult egy egészséges félelem – mai szóhasználattal: információbiztonsági tudatosság - a felhasználókban is. Az Ibtv. hatályba lépését követően már egészen pontos környezeti feltételeket határoztak meg a jogalkotók, amelyet 2015-ben - a törvény végrehajtási utasításában[56] - konkrétan ki is fejtettek.

Jelentős mérföldkő az ágazat életében az ASP[57] rendszer bevezetése, amely egy uniós pályázat[58] keretében biztosított forrást a szektornak. A „*Működésfejlesztési és szabályozási keretek kialakítására*" tétel a pályázati kiírásban *eredménydokumentumnak* jelölte az IT-biztonsági szabályzatot (IBSZ).

Az önkormányzatok egy részének ekkor adódott először lehetősége, hogy IT-biztonsági rendszer kialakítására ilyen nagyságrendű anyagi forrást biztosíthasson. Korábban hasonló mértékű támogatási intenzitással nem hirdettek olyan pályázati lehetőséget, amelyet célzottan erre a területre használhattak fel a hivatalok. Gyakorlatilag önerő bevonása nélkül biztosított keretet a pályázóknak, hogy felmérjék jelenlegi helyzetüket és értékeljék kockázataikat – stratégiát alkothassanak azok kezelésére és kialakíthassák szabályzati struktúrájukat, amely biztosíthatja részükre a jogszabályi környezetnek megfelelő – kockázatarányos és biztonságos – működést.

A pályázati kiírást nagy várakozás előzte meg – szállítói és megrendelői oldalról egyaránt. Sokan remélték, hogy az egységes követelményrendszer olyan ajánlatokat generál majd, amely lehetővé teszi az uniós források hatékony elosztását és kedvező lesz minden szereplőnek. Ezek az elvárások csak részben valósultak meg. Jelen dokumentumnak nem célja az ASP projekt ilyen megközelítésű értékelése: az IT-biztonsági szempontokra fókuszál és ebből a megközelítésből azt valódi előrelépésnek tartja. Az önkormányzati szektor IT-biztonságának kialakításában ez a pályázat valódi mérföldkő – ismételten rámutatva, hogy korábban ilyen mértékű forrás erre a területre még nem érkezett!

---

54 Közigazgatási Informatikai Bizottság - 25. számú Ajánlása - Magyar Informatikai Biztonsági Ajánlások.

55 Ma: MSZ ISO/IEC 27001:2014 –s .

56 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

57 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről.

58 KÖFOP-1.2.1-VEKOP-16 - CSATLAKOZTATÁSI KONSTRUKCIÓ AZ ÖNKORMÁNYZATI ASP RENDSZER ORSZÁGOS KITERJESZTÉSÉHEZ.

4.2. Alapozás

4.2.1. Információbiztonsági irányítási rendszer kialakítása

A Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzésén több, mint 10 évfolyam végzett eddig, de az elmúlt – frissnek tekinthető - szakdolgozatok témaválasztásait megfigyelve az tapasztalható, hogy a hallgatók, akik egy részét olyan szervezetek iskolázták be, amelyek az Ibtv. hatálya alá tartoznak és IBF – információbiztonsági felelős - kinevezésére kötelezettek – nem a már meglévő IT-biztonsági rendszerek továbbfejlesztéséhez kapcsolódó területeket választanak kidolgozásra: az alapoknál kezdenek – az információbiztonsági irányítási rendszer[59] kiépítését tűzik ki célul. Ebből az a következtetés is levonható, hogy a 2013. évi törvény és a 2015-ös végrehajtási rendeletének hatálybalépése óta eltelt idő alatt teljeskörűen nem kerültek kialakításra információbiztonsági irányítási rendszerek. Hozzátartozik a teljes képhez, hogy új szervezetek is létrejönnek, új ágazatok is a törvény hatálya alá kerültek és alapvető szerkezeti átalakítások is indokolhatják a témaválasztásokat.

Az önkormányzati szektor – részben az előző fejezetben leírt ASP pályázatnak köszönhetően – erős alapokra építkezhet: a korábban saját üzemeltetésű rendszerek fenntartására biztosított erőforrásait a meglévő IT-biztonsági rendszer fenntartására és fejlesztésére fordíthatja. Ennek ismeretében kerülnek megemlítésre a bevezetések során elvégzett feladatok és megosztásra a gyűjtött tapasztalatok.

Az IBIR kialakításakor kifejezetten célszerű a *projektszemléletű* megközelítés. Ha a vezetői elköteleződés adott, akkor kijelölésre kerülhetnek a célok, rendelhetőek hozzájuk felelősök, rögzítésre kerülhetnek az eredménytermékek és a határidők. Ezek ismeretében alakítható ki a *projektszervezet* és határozható meg az előrehaladási jelentések gyakorisága, tűzhetőek ki a mérföldkövet és érhetőek el a kijelölt célok.

4.2.1.1. Vezetői elköteleződés

Az önkormányzatok és az általuk létrehozott intézmények pontosan meghatározott struktúrában jöttek létre, szervezeti felépítésük adott. Az önkormányzat választott vezetője a polgármester, a hivatal törvényes működéséért a jegyző felel. Az ASP pályázaton történő elinduláshoz a képviselőtestület határozata is szükséges volt: a támogatás intenzitására is hatással bírt ez a döntés. (Voltak hivatalok, ahol a teljes és azonnali csatlakozás mellett döntöttek – így került napirendre és előterjesztésre a képviselőtestületi ülésen – és voltak, ahol – időlegesen - fenn kívánták tartani a meglévő rendszereiket - saját üzemeltetésben. Olyan hivatalokról is voltak, ahol nem kívántak élni a pályázat adta lehetőségekkel – saját forrást biztosítottak a csatlakozásra. Az ASP törvényben leírtak egyértelműen meghatározzák a hatálya alá tartozó szervezetek mozgásterét: a csatlakozásuk a rendszerhez – az átmeneti időszak lejártát követően - kötelező.

Úgy tűnhet a fentiekből, hogy a fejezet címéül választott *vezetői elköteleződés* adott volt minden településen. A tapasztalatok még a 2015-ben pilotként elindított hivatalok esetében is árnyaltabb volt ennél: akadt, ahol újabb tehernek érezték, hogy ezzel a területtel is foglalkozniuk kell. Természetesen kedvező fogadtatásról is be lehetett számolni: az IT-rendszereket üzemeltető kollégák hamar felismerték, hogy ezeket a forrásokat a biztonságos üzemeltetési környezet fejlesztésére is lehet – sőt: egyenes célszerű – fordítani és ehhez külső támogatást kínálhatnak a bevezetésben résztvevő tanács-

[59] IBIR - információbiztonsági irányítási rendszer – ISO 27001 -s terminológia. Az Ibtv. 11.§ 3. bekezdés *„szervezeti szintű informatikai biztonsági szabályok”*-ként hivatkozik az IT-biztonsági rendszerhez kapcsolódó dokumentumokra – továbbiakban a szabvány szerinti terminológiában megszokott rövidítés kerül alkalmazásra.

adók. A pályázat lakosságszám alapján három kategóriára osztotta a településeket és ez határozta meg az egyes területekre fordítható keretösszegeket is. A keretösszegek felosztásának tervezése során ismerték fel a hivatalok ezzel megbízott projektvezetői, hogy az eredménydokumentumként nevesített IBSZ csak az egyik eleme az IT-biztonsági rendszernek – annak további mellékletei és kapcsolódó eljárásrendjei más típusú tapasztalatot és tudásanyagot kívánnak meg az alkotóitól, mint amivel már a hagyományosnak tekintett IT-üzemeltetői és -fejlesztői kör bírt.

Azok a vezetők – polgármesterek, jegyzők, IT-vezetők – akik helyesen mérték fel, hogy a rendszer kiépítésére milyen belső erőforrásokat tudnak igénybe venni és melyek azok a kompetenciák, amelyeket a szervezeten kívül kell megtalálniuk, nem kerültek bajba a pályázati pénzek elszámolásakor. Természetesen itt sem lehet általánosítani: sok hivatal már jóval a pályázat elindítását megelőzően teljesítette az Ibtv.-ben rögzített kötelezettségeit – néhányuknál még IBF is kinevezésre került – szabályzatokkal is rendelkeztek – ők örömmel kaptak a lehetőségen, hogy az IT-biztonsági stratégiájukban meghatározott célokhoz extra erőforrásokat rendelhettek.

Összefoglalva: azok a hivatalok, ahol a vezetők megértették, hogy az IT-biztonsági rendszer milyen módon járul hozzá feladataik ellátásához kellően átgondolt és felépített projektszervezet került felállításra és a megfelelő döntési jogkörökkel lettek felruházva a résztvevők. Jól elhatároltak voltak a felelősségi körök és a felmerülő akadályokat sikerrel vette a szervezet. Ahol az „asztalfióknak" készült a szabályzat és a motivációt egy esetleges hatósági ellenőrzéstől való félelem inspirálja sokkal nehezebb eredményeket elérni és működő – üzemeltetésre átadható – IT-biztonsági rendszert kialakítani.

4.2.1.2. Politika, stratégia, szabályzat – eljárásrendek és munkautasítások

Az Ibtv. eredeti formájában (elfogadására 2013. április 15-én került sor) még az *„Értelmező rendelkezések"* között sorolta fel az IT-biztonsági politikát és az IT-biztonsági stratégiát. Ez utóbbiban kerültek megfogalmazásra a hosszú-, közép- és rövid távú (de még mindig éves időtartamú) tervek, határidővel és felelősökkel. A felelősök a feladat végrehajtásán túl az ahhoz rendelt erőforrások biztosításáért is feleltek és beszámolási kötelezettség terhelte őket. Sajnos a törvény egy későbbi módosítása olyan változtatásokat hozott, amelyek már nem nevesítik ezeket a dokumentumokat, de a tapasztalatok azt mutatják, hogy az IBIR átláthatósága/áttekinthetősége és felépítése sérül, ha ezek az elemek nem kerülnek beépítésre.

Az „*informatikai biztonságpolitika"* a törvény eredeti előterjesztésekor az értelmező rendelkezések 23. pontjaként így került meghatározásra: „*a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;"*

Az *„informatikai biztonsági stratégia"* ugyanebben a szakaszban (értelmező rendelkezések) volt fellelhető és a következő – 24. pontban így definiálták: *„az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;"*

Egy világos, átlátható - jól felépített - szabályozási környezetben a *politika* a *hitvallás,* a szervezet általános működésével összhangban kerül megfogalmazásra és azt annak elérésében segíti. A *stratégia* a *politikában* meghatározott erőtérben az irányok és célok elérésének alapdokumentuma: már konkrét feladatokat tartalmaz, amelyeket az aktuális helyzet ismeretében fogalmaz meg és amelyek eléréséhez erőforrásokat és felelősöket rendel. Mérhető, hogy a kijelölt célok milyen időtávon valósulhatnak meg és éves felülvizsgálata során az elért eredmények ismeretében ezek értékelhetőek, pontosíthatóak és módosíthatóak.

A *szabályzatok* - köztük az egyik nevesített alapdokumentum a sokat emlegetett IT-biztonsági szabályzat – IBSZ – szintén a *politika* által generált erőtérben alakulnak és egy-egy konkrét terület általános viselkedését mutatják be, írják le a folyamataikat. (Az IBSZ az Ibtv. ben először a biztonsági osztályba soroláshoz kapcsolódóan kerül említésre, mint olyan dokumentum, amelynek kötelezően tartalmaznia kell azt.)

A szabályzati struktúra egy újabb szintjén az eljárásrendek találhatóak, amelyek már a szabályzatokban foglaltaknál is kisebb területet írnak le és adnak konkrét utasításokat a bennük megfogalmazott területekre. (Jó példa lehet erre a *„A jogviszony létesítésére irányuló, annak megváltozásakor és megszűnésekor alkalmazandó eljárásrend”*, amely a szervezet személyzeti politikájával összhangban leírja, hogy milyen IT-biztonsági szempontokat érvényesítsünk a kiválasztáskor (toborzáskor); melyek a felvételi eljárás során követendő szabályok; hogyan történik az oktatás; az adott munkakör betöltéséhez milyen típusú nyilatkozatok aláírása szükséges, illetve részletszabályokat fogalmaz meg a jogviszony megszűnésekor, vagy más munkakörbe történő áthelyezéskor.)

Tovább haladva a szabályozási környezet legalsó szintjén a munkautasítások találhatóak, amelyek az adott munkakörhöz kapcsolódóan egy-egy folyamat pontos végrehajtása érdekében - szinte pontokba szedve - írják le az elvégzendő résztevékenységeket/feladatokat – beleépítve abba a megfelelő kontrollokat is. (Ismertek olyan szervezetek, ahol vezetői körlevelekben utasítanak egyes munkafolyamatok elvégzésére – ezek vagy meglévő és elfogadott gyakorlatokat pontosítanak/írnak le, vagy épp arra szolgálnak, hogy egy bevett gyakorlatot változtassanak meg – például a közösségi hálózatokon tiltják meg a szervezetre utaló posztok/képek/vélemények közzétételét/megosztását.)

4.2.1.3. Jogosultságok, szerepkörök, hatókörök

Bizalmasság, *sértetlenség*, *rendelkezésre állás* – ezek az IT-biztonsági terület sokat emlegetett kulcsszavai, alapfogalmai. Az első – a *bizalmasság* – így került definiálásra az Ibtv. *„Értelmező rendelkezések”* 1.§ -nak 8. pontjában: *„az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.”*

Az új uniós adatvédelmi rendelet – ismertebb nevén: GDPR – is az egyik alapelveként határozza meg az *elszámoltathatóságot* – betarthatóságának alapvető feltétele, hogy olyan jogosultsági rendszert alakítsunk ki, amely mindenki számára átlátható, egyértelmű, követhető és betartatható – és minden esemény vagy változás a *„Naplózás, naplóelemzés”* fejezetben leírtak szerint rögzített és visszakereshető.

Az önkormányzati szektorban több olyan elektronikus információs rendszerrel (EIR) találkozhatunk, amelyek egy része új fejlesztésű – más részük pedig korábbi időszakok termékei, amikor még nem volt elvárás, hogy az adott alkalmazást egynél több gépen is futtassuk, azok különböző felhasználói azonosítókat kezeljenek és elválasszák egymástól az adminisztrátori és normál szerepköröket. Azoknak a követelményeknek, amelyeket jelenleg támasztunk egy újonnan bevezetendő alkalmazás fejlesztésekor természetszerűleg nem képesek megfelelni ezek a régről megörökölt rendszerek. Fontos, hogy felismerjük és lehetőségeink szerint kezeljük – egyéb lehetőség híján szűntessük meg – az ezekben rejlő kockázatokat.

Elektronikus információs rendszerekről az Ibtv. közlönyállapotában még az *„Értelmező rendelkezések”* 2. és 3. bekezdésében olvashattunk, melyet aránylag hamar módosítottak. A jelenleg hatályos verzióban már a fogalmi meghatározások részébe emelték (14.b pont) ezzel a definícióval: *„**a)** az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; **b)** minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy **c)** az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;”*

Elektronikus információs rendszereink osztályba sorolásának egyik feltétele, hogy erről pontos nyilvántartásunk legyen – a bevezetéskor hatékony módszernek bizonyult feltérképezésükre a *jogosultságigénylő* lapok elemzése.

4.2.1.3.1. Az ASP keretrendszere[60] – jogosultsági mátrix

Az ASP új fejlesztésnek minősül, és feltehetően az IT-biztonsági követelmények maximális figyelembevételével került kiválasztásra és továbbfejlesztésre a keretrendszere, amely felépítéséből adódóan a jogosultságok komplex nyilvántartásának vezetésére is alkalmas. A rendszer indulásakor az úgynevezett *„Tenant adminisztrátor"* kapja az *ős jogot*, hogy az adott szakterületek adminisztrátorait létrehozza, akik aztán az alájuk rendelt felhasználóknak oszthatták ki: milyen jogosultságokat kapnak feladataik elvégzéshez. Az oktatás során mindenki figyelmét felhívták a szakemberek, hogy fontos szempont: a szereplők az *elégséges* jogosultságokat kapják – épp annyit, amennyi a munkájuk elvégzéséhez szükségesek. Az IT-biztonsági szakemberek azért tartják fontosnak az adminisztrátori és felhasználói szerepkörök szétválasztását, mert eltérő hitelesítési eljárásokat kell alkalmaznunk a megfelelő kockázati szintekhez. Gondoljuk át: korábban egy-egy hackertámadás csak az adott hivatal ügymenetét zavarhatta meg – a hitelesítő kulcsok kompromittálódása vagy adatvesztés esetén nem volt magas az érintettek száma – ha ezt a számot az ország teljes lakosságára vetítjük. Az ASP viszont országos rendszer – minden önkormányzat a felhasználói közé tartozik – a biztonságos üzemeltetés és tudatos felhasználói magatartás ebben az esetben felértékelődik. A keretrendszer 77 oldalas felhasználói kézikönyve részletesen megmutatja, hogy milyen típusú hitelesítési eljárásokat implementálhatóak, de hiába adottak a lehetőségek, ha azok nem kerülnek alkalmazásra. Egy tavaly közzétett felmérés szerint például sok olyan eszközzel lehet még ma is találkozni, amelyeket az alapértelmezett – gyakran a neten is lekérdezhető – jelszavakkal „védenek". Megfontolásra érdemes: ha az otthoni wifi-hálózati hozzáférést erős titkosítással védik abból a célból, hogy illetéktelenek ne csatlakozzanak fel a rendszerekre, de a wifit szolgáltató eszköz alapértelmezett beállításai nem kerülnek módosításra milyen biztonsági szint érhető el?

A jogosultságokra az *adatvédelmi szakemberek* másképpen tekintenek, mint az előzekben említett IT-biztonsági kollégák. Számukra az IT-biztonság csak megteremti a szükséges védelmet, de vizsgálatuk fókuszában a *személyes adatok* hozzáférhetősége áll. Egy nem hazai példa:[61] Kórházban vizsgálták egy ellenőrzés során, hogy kik férnek hozzá a betegek adataihoz. A kórház aktuális személyi állományát többszörösen meghaladó orvost, nővért és egyéb egészségügyi dolgozót találtak a rendszerben, akik már évek óta nem voltak az adott szervezet állományában. Nem vonhatók felelősségre, ha a felhasználói azonosítóikkal történik visszaélés – súlyos bírsággal és az adott intézménybe vetett bizalom elvesztésével kellett szembenéznie a menedzsmentnek. Feltételezhető, hogy a fenntartó is tett lépéseket, hogy az adatvédelmi előírásokra nagyobb hangsúly kerüljön a továbbiakban.

Az IT-biztonsági ellenőrzéseket végző hatóság ellenőrzési tervében gyakran található olyan követelménypont, amelyben azt kérik, hogy kerüljenek bemutatásra egy-egy rendszer jelenleg bejegyzett felhasználói - beleértve azokat a jogosultságokat is, amelyeket hozzájuk rendeltek. Ha az ASP keretrendszerét vesszük alapul és hasonlóan szofisztikált – szerepkörökre és különböző felhasználói csoportokra bontható - jogosultsági mátrix kerül bemutatásra, amelynek kialakításához az IBSZ -ben meghivatkozott eljárásrend lett alapul véve, akkor a vizsgálat emeli a szervezetbe vetett bizalmat. Ha a jogosultságok igényléséhez használt – kitöltött és minta – űrlapokat is be lehet mutatni, akkor az auditori jelentésbe ehhez a követelményponthoz a „maradéktalanul megfelelt" státusz kerül rögzítésre.

Összefoglalva: használjuk az ASP keretrendszerét referenciaként a meglévő alkalmazásaink jogosultságainak beállításához. Ha ennek kialakításához fejlesztői segítség szükséges: szabadon megoszthatjuk azt az üzleti logikát, amelyet e rendszer kialakítása során alkalmaztak. Az uniós pályázatok egyik szépsége éppen abban rejlik, hogy a kidolgozott eljárások mindannyiunk javára fordíthatóak!

60 https://alkalmazaskozpont.asp.lgov.hu/sites/asp/files/2018-02/Keretrendszer_felhasznaloi_kezikonyv.pdf
61 https://gdpr-okosan.hu/hirek/400-ezer-euros-birsag/

4.2.1.3.2. Felvételi eljárás(ok) rendje

Az előző fejezetben már említésre került egy eljárásrend, amelynek hatóköre kiterjed az adott munkakör meghirdetésekor alkalmazandó szabályokra, a kiválasztási folyamat során alkalmazandó eljárásokra, a jogviszony keletkezésekor aláírandó nyilatkozatokra, a munkakör ellátáshoz szükséges IT-biztonsági ismeretekre és egyéb feltételekre. Tartalmazza az oktatásra vonatkozó feltételrendszert, amely bizonyos szint elérésére kötelezi a jelentkezőt, amely egyrészt feltétele az adott munkakör betöltésének, másrészt a szervezet rendszereihez történő hozzáféréseknek. Követelményeket fogalmaz meg a jogviszony bárminemű megváltozásából adódóan – beleértve a távozó jogosultságainak elvételét igazoló „bizonyítékokat[62]" és figyelmének felhívását arra, hogy kilépése után milyen titoktartási és egyéb kötelezettségek terhelik. Ezek a szabályok korábban már a személyzeti – HR – osztályokon is elkészültek, de most azok kiegészítése történik az IT-biztonsági szabályok figyelembevételével és alkalmazásával. Az internetes viselkedés szabályain ma egészen mást értünk, mint akár csak egy évvel ezelőtt: a koronavírus okozta helyzet pedig alapjaiban változtatta meg az otthoni munkavégzés eddig ismert és alkalmazott szabályait.

A képviselőket nem a hagyományos módon toborozzák – választják őket. Számukra külön szabályok alkalmazása szükséges – szerencsére a hivatali ügyintézés operatív tevékenységei nem tartoznak a feladataik közé. A hivatali infrastruktúrát azonban igénybe vehetik – javasolt ennek olyan módon történő kialakítása, amely szabadságaiban nem sérti a tevékenységüket és a hivatal IT-biztonságát sem veszélyeztetik. A képviselőtestületi ülések során gyakran kérnek segítséget, hogy eszközeikkel az internetre csatlakozhassanak. Semmiképpen nem javasolt a hivatal éles rendszereivel azonos tartományt kijelölni ilyen célra: az ügyfeleknek és a képviselőknek külön – egymástól és a hivataltól elszeparált – hálózat kialakítása célszerű. Sokszor felmerül kérésként például, hogy bizonyos anyagokat az ülés megkezdését megelőzően kinyomtathassanak. Volt példa arra, hogy olyan pendrive került így a „segítő" irodai számítógépébe, amelyet korábban nem vizsgáltak antivírus programokkal. Javasolt olyan számítógép és nyomtató rendszerbe állítása, amely NEM csatlakozik a hivatal éles rendszereihez és *megfelelő* védelemmel van ellátva. (Elvárható, hogy az így biztosított eszköz ne legyen vírusgazda, vagy hordozó!) A képviselők egy részének már elektronikusan kerülnek birtokába az ülések anyagai. Van, ahol e-mail csatolmányként, hivatkozásként, vagy más digitális eszközzel – pl.: NAS - segített módon. Ilyen esetekben szintén javasolt az elővigyázatosság: a képviselői laptopok merevlemezeit és az általuk használt pendriveokat titkosítsuk – elvesztésük esetén ne legyenek hozzáférhetőek a rajtuk tárolt adatok – a biztonságos e-mail és eszközhasználatot pedig mutassuk be – amely bemutatónak része, hogy ismertetjük: a szabályok megszegése milyen következményekkel járhat.

A hivatal különböző státuszokban és jogviszonyokban foglalkoztathat munkavállalókat. Közmunkás, közalkalmazott, köztisztviselő, megbízott – nagyon vegyes képet nyertünk a szektorban dolgozva. Fontos megértenünk, hogy az adott rendszer biztonsága NEM biztosítható a felhasználók IT-biztonsági tudatosságának megfelelő szintű megerősítése nélkül. Ahogy az adatvédelmi ismertetőt is olyan nyelvezettel kell megfogalmazni, hogy azt az a célcsoport megértse, úgy az adott munkakör betöltéséhez szükséges és elégséges IT-biztonsági kompetenciákat is célszerű úgy meghatározni, hogy a kezdeti szint az alaptevékenység ellátásához elegendő, a további – elvárt – működéshez pedig továbbfejleszthető legyen – munkáltató és munkavállaló közös megelégedésére.

[62] A „sétálópapíron" a rendszergazda ellenjegyzését, hogy a rendszerekhez történő hozzáféréseit a szükséges mértékre korlátozta/megszüntette.

4.2.1.4. Leltárak

4.2.1.4.1. Eszközök, programok, licenszek

A törvény végrehajtási rendeletében [41/2015 (VII. 15)-s BM rendelet] a *Logikai védelmi intézkedések* fejezetben a *Konfigurációkezelés* szakaszban írja elő, hogy a hatálya alá vont szervezetek rendelkezzenek ilyen nyilvántartással: *„Elektronikus információs rendszerelem leltár"*. A jogszabályi megfelelésen túl természetesen gyakorlati okai is vannak, hogy a szervezet ismerje a használatában lévő eszközöket és azok pontos konfigurációját. (Ezek az adatok az üzemeltetés során elengedhetetlenek – pl. szoftverjavítások [patchek] kihelyezésekor vagy egy ellopott notebook adatainak megadásához – a büntetőfeljelentéshez.)

Önkormányzati IBIR-rendszerek bevezetése során nyert tapasztalat, hogyha az IT-eszközök jelenlegi leltárába kérnek betekintést, akkor erre a válaszadó – beosztásától függően – többféle megoldást kínál. A vagyongazdálkodás és a számvitel azokat a számlákat tartja nyilván, amelyen nagyobb értékű eszközök szerepelnek – a tárgyi eszköz kartonokat, az értékcsökkenési leírást mutatják be. Előfordul, hogy az immateriális javak között a nagyobb értékű szoftvereket is felsorolásra kerülnek. A pályázati elszámolásokat felügyelő csoport azokat a dokumentumokat tartja nyilván, amelyeket a pályázati kiírásban szerepeltettek, beleértve az ajánlatokat és az értékelési jegyzőkönyveket. Megőrzésre kerülnek az értesítések, amelyek a résztvevőknek kerültek kiküldésre, a szerződések és a teljesítésigazolások a leszállított és üzembe állított berendezésekről/szolgáltatásokról. Az IT-üzemeltetés a hálózati végpontokon található eszközökről tud adatokat szolgáltatni – az infrastruktúra azon elemeit is beleértve, amelyek az eléréshez szükségesek – ilyenek például: routerek, switchek, passzív eszközök, vezeték nélküli hozzáférést biztosító eszközök. A komplex nyilvántartás vezetése erőforrásigényes – ritka, hogy olyan eljárásrend kerüljön kihirdetésre, amely a hivatal különböző osztályainak nyilvántartásait összekapcsolja. Az IT-biztonsági rendszer több olyan elemet is tartalmaz, amely segíti, hogy az adott szervezetnél kialakult gyakorlat megfelelő támogatást kapjon és minden résztvevő számára világos és átlátható legyen.

Eszközeink működtetésének feltétele, hogy megfelelő szoftverelemekkel és legális licenszekkel legyenek ellátva. A BSA[63] néhány éve nagyszabású felvilágosítási kampányba kezdett, hogy legális szoftverhasználatra ösztönözzön. Sokakat meglepett, hogy a plakátokon is bemutatott jogszabályok a szervezetnél tapasztalt szerzői jogsértéseket (ideértve az illegális szoftverhasználatot is) a szervezet vezetőjének róják fel és a kiszabható büntetési tétel akár letöltendő szabadságvesztés is lehet. Találkoztunk olyan hivatallal, ahol a NAV a nem megfelelően licenszelt eszközöket lefoglalta és a vizsgálat megszűnését követően szolgáltatta csak vissza. Ennél a hivatalnál azóta a pontosan vezetett licenszleltár az IT-üzemeltetésre szerződni kívánók felé támasztott egyik alapkövetelmény.

Az eszközök és a működésüket biztosító operációs rendszerek mellett alkalmazásokat, alkalmazói programokat, friss, megbízható eszközillesztőket és firmware -ket telepítünk az eszközeinkre. Magasabb biztonsági szintre sorolt szervezetek esetében nagyon pontosan meghatározott, hogy a felhasználók az IT által rendelkezésükre bocsátott alkalmazáskatalógusból milyen elemeket választhatnak. Ide letesztelt, megfelelően támogatott és frissített programokat helyeznek el az alkalmazásgazdák. Ha valakinek olyan programra vagy szolgáltatásra lenne szüksége, amelyet a katalógusban nem talál meg, akkor a megfelelő indoklás és engedély birtokában igényelheti, hogy a gépére ez az alkalmazás is felkerülhessen. Az IT-ilyen feltételekkel tud felelősséget vállalni, hogy a rendszer biztonságos üzemeltetése megvalósítható legyen és az ismert sérülékenységeket időben javíthassa. (Az NKI – Nemzeti Kibervédelmi Intézet – heti rendszerességgel teszi közzé a statisztikákat, amelyek az adott időszakra vonatkozóan tartalmazzák milyen típusú támadásokat szenvedtek el az általa támogatott szervezetek. A heti rendszeres jelentések – sajtószemlék és hírlevelek – mellett *tájékoztatást* nyújt egyes elterjedt támadási formákról és r*iasztást* küld, ha valamely program gyártója javítást ad ki a termékéhez. A javítások kiadása egyben annak a sérülékenységnek a publikálása is, amelyre

[63] Business Software Alliance - https://hu.wikipedia.org/wiki/Business_Software_Alliance.

a „folt" kiadásra kerül, ezért érdemes minél hamarabb telepíteni ezeket a frissítéseket! Az Ibtv. a biztonsági események bekövetkezésének *megelőzését* is kötelezettségeink között említi – a fogalomra az „*Értelmező rendelkezések*" 1. bekezdésében olvashatunk definíciót a 36. pontban: „*a fenyegetés hatása bekövetkezésének elkerülése*".

Külön érdemes megemlíteni az „idegen" eszközöket, amelyek a hivatali rendszerekre csatlakoznak. Az ügyfélterekben szinte már elvárt a wifi-csatlakozási lehetőség – az ide telepített hozzáférési pontokra csatlakozó eszközökre vonatkozóan pedig nincs mód megkötéseket tenni: potenciális fenyegetésként javasolt kezelni ezeket. A megfelelő tájékoztatást nyújtása tulajdonosaiknak – még a csatlakozást megelőzően lényege: ismertetendő, hogy a szolgáltatás igénybevétele esetén milyen viselkedési szabályok várhatóak el. Az uniós adatvédelmi rendelet (GDPR) által nevesített *adatvédelmi tisztviselő* (DPO) általában külön tájékoztatót készít, amelyben a szolgáltatás igénybevételéhez szükséges adataik kezeléséről kaphatnak felvilágosítást és dönthetnek, hogy ezen feltételek mentén élni kívánnak-e a felkínált lehetőséggel?

Az ügyfelek mellett – egyes hivatalokban – a munkavállalók részére is lehetőséget kínálnak, hogy saját eszközeikkel csatlakozzanak az erre kialakított – az éles rendszerektől leválasztott – hálózatokra. Számukra az ügyfelekénél is részletesebb tájékoztatást javasolt adni arról, hogy tevékenységük milyen mértékben engedélyezett és a szolgáltatás igénybevételével milyen viselkedési szabályokat várunk el tőlük. Javasolt külön engedélyhez kötni a használatot és rendszeres időközönként felülvizsgálni, hogy az engedély megadásakor fennálló körülmények megváltoztak-e?

Saját eszközökre történő hivatalos alkalmazások telepítése, illetve saját eszközök használata alapesetben tiltott: csak külön engedély birtokában és pontosan meghatározott biztonsági előírások betartása esetén javasolt. Az otthoni munkavégzés – ha nem az hivatal erre rendszeresített – estlegesen hordozható – eszközein keresztül, hanem saját infrastruktúra segítségével történik – mindig kiemelt kockázatúnak minősül és ezzel arányos védelmi intézkedéseket igényel. Az engedély mindig adott időszakra adható, felülvizsgálata – esetleg meghosszabbítása – ismételt eljárásban – az engedély kiadására meghatalmazott ellenjegyzésével történhet.

4.2.1.4.1.1. Az OCS Inventory

Többen már a *Digitális Jólét Program* pályázat[64] keretében találkozhattunk az OCS Inventory NG[65] programmal, amely nagy segítségünkre lehet eszközleltáraink elkészítésében (is). Már egy néhány számítógépet magában foglaló hálózat esetében sem tudjuk az operációs rendszerek aktuális verzióját és telepített frissítéseit nyomon követni, képzeljük el, hogy egy több telephelyen üzemelő hivatal milyen kihívásokkal néz szembe, ha az NKI riasztását, amelyben a szokásos keddi Microsoft javításokra hívja fel a figyelmet – köztük 3-t kritikusnak minősítve – kénytelen kezelni? Egyenként vizsgálja majd, hogy az adott frissítés érinti-e az adott telephelyen üzemelő eszközeiket?

Ennek a helyzetnek a kezelésére is többféle megoldás is kínálkozik. A hagyományos – kézi leltározás csak kisebb elemszámú eszköz esetében jelent megoldást, nagyobb állomány, vagy földrajzilag távol elhelyezkedő konfigurációk esetében ezt a feladat olyan segédprogramok segítségével oldható meg, amelyek képesek automatikusan – rendszeres időközönként – vagy konkrét lekérdezést elindítva információt szolgáltatni. Ismertek olyan vállalkozások, amelyek korábban egyedi vírusvédelmi rendszereket telepítettek, majd ezt továbbfejlesztve központi felületet implementáltak termékeikbe, melyekből a számunkra szükséges adatok is kinyerhetőek. Hálózati operációs rendszerek is kínálnak olyan beépített vagy harmadik gyártó által telepíthető szolgáltatásokat, melyek segítségével a megfelelő nyilvántartás összeállítható. Aktív hálózati eszközöket gyártó- és fejlesztő cégek is kínálnak olyan szolgáltatásokat, amelyek erre a feladatra is alkalmasak – széles a paletta, amelyen kikereshető a hatékony, de az elérhető erőforrásainkkal arányos megoldás.

64 https://djp.palyazat.kifu.gov.hu/ginop331/

65 https://ocsinventory-ng.org/?lang=en

Az OCS Inventory NG -t azért emeltem ki ezek közül, mert nyílt forrású és az előző bekezdésben leírtakra visszautalva: gyűlt már kellő mennyiségű hazai tapasztalat az alkalmazásával/használatával kapcsolatban! Ahogy a jogosultságkezelések kialakításában referenciaként javasoltuk az ASP keretrendszerét figyelembe venni, úgy az eszköz- és szoftver leltárak összeállításakor is érdemes megvizsgálni, hogy egy jelenleg is működő rendszer milyen tanulságokkal szolgálhat számunkra. *(További eszközök használatáról a Jegyző és Közigazgatás 2018. évi 5. számában olvashatunk cikket – referenciaként említve Hosszúpályi önkormányzatát, ahol az OCS Inventory – az IBIR kiépítésének részeként – 2017 óta üzemel.)*

Az OCS Inventory NG hazai pályafutása töretlen – nemrégiben egy másik ágazatban – az egészségügyi szektorban – is történtek lépések alkalmazására és bevezetésére. (Egyes intézmények már nemcsak a leltárfunkciókat tesztelték, de központi telepítési és mobilplatform-kezelő szolgáltatásait is sikerrel kipróbálták.)

4.2.1.4.2. Helyiségleltár és zónabesorolás

Ha az eszközök, licenszek és szoftverelemek nyilvántartása már kellő részletezettséggel rendelkezésre áll a megfelelő védelem kialakításához azokat a helyiségeket is biztonsági zónába szükséges sorolni, amelyekben ezek a berendezések megtalálhatóak.

Az elektronikus ügyintézés jelenlegi elterjedtségét megelőzően a *személyes* ügyintézés volt jellemző a hivatalokban. Ideális esetben az épület ügyfélforgalom számára biztosított részei a nyitvatartási időben szabadon elérhetőek – az ügyintézők megfelelő védelemmel ellátott munkahelyeken fogadhatják az érkezőket. Kialakításuk olyan, hogy a még a vétlen károkozás is a minimálisra korlátozódik: nincsenek kusza kábelek a földön, amelyben elbotolhatnak az arra járók, a berendezések kellően biztosítottak – zárható szekrényben elhelyezettek és/vagy hozzáférhetőségük egyéb eszközökkel korlátozott. A bejáratnál szolgálatot adó személyzet tájékoztatja az érdeklődőket és az épület egyéb – ügyfélforgalom elől elzárt – részei megfelelően biztosítottak. Ezt a területet *1-es biztonsági zónaként* jelöljük – ide a fent ismertetett feltételekkel kíséret nélkül léphetnek be és tartózkodhatnak az ügyfelek.

A *2-es biztonsági zónába* azok a munkahelyek tartoznak, ahol munkavállalóink a munkájuk elvégzéséhez szükséges eszközöket és anyagaikat tartják. Ezeket az irodákat munkaidőben használjuk – nyilvántartást vezetünk azokról, akik jogosultak felvenni a kulcsaikat – rögzítjük annak megtörténtét és záráskor a kulcs leadását/visszavételét is. Erre a területre ügyfél az adott ügyintéző – vagy megbízottja – kíséretében léphet be és nem maradhat felügyelet nélkül. Belső eljárásrendben szabályozott, hogy ezekről az esetekről szükséges-e nyilvántartást vezetni és azok milyen részletezettségűek.

A *3-as biztonsági zónák* azok a területek, ahová előzetes bejelentkezés és az adott helységbe belépési jogosultsággal rendelkező személy kíséretében engedjük be azokat, akiknek erre felhatalmazásuk van. Ilyen helyiség például a szerverszoba – itt biztosan kötelező olyan nyilvántartást vezetni, amelyen az oda belépő személyek adatait rögzítjük. (Egyes értelmezések szerint az ASP -s munkahelyek is ilyen védelem alá eső helyiségeket igényelnek.)

A törvényben és a végrehajtási rendeletben a *fizikai védelmi intézkedések* között sorolják fel azokat az előírásokat, amelyek egyes helyiségek besorolását teszik szükségessé. A fentiekben mintaként felsorolt zónabesorolás csak *javaslat* – a felhőtárhelyeken megosztott adatokat például sorolhatjuk a *0 -s zónába*, hiszen semmilyen értékelhető hatásunk nincs az ottani környezetre; a páncélterem leírására pedig, ahová két külön személy által őrzött egyedi kulccsal juthatunk be létrehozhatunk egy új szintet: a *4 -s zónát.*

Lényeges, hogy az IT-biztonsági rendszer fizikai határai megfelelően kerüljenek leírásra és pontos nyilvántartás álljon rendelkezésre a helyiségekről, amelyek – zónabesorolásuktól függően – megfelelő védelmi intézkedésekkel biztosítottak. Az eszközleltárban legyen megjelölve, hogy az adott berendezés melyik helyiségben található és oda kiknek van joga belépni, ott tartózkodni és munkát végezni, milyen feltételekhez kötött a belépés olyan személyek számára, akiknek nem biztosított állandó belépő.

4.2.1.5. Szerződött partnerek

Korábban minden önkormányzatnak volt tanúsított ISO 9001-es minőségirányítási rendszere. Ebben a rendszerben a beszállítókat évente értékeltük és minősítettük: megfelelő színvonalon szolgáltatnak-e – hosszabbítunk-e velük szerződést? Az IT-biztonsági rendszerben azért vesszük nyilvántartásba a beszállítókat, mert az Ibtv. kötelez bennünket erre. (11.§ k.) pont: *„ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek”,* illetve az l.) pont: *„ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek”.)* Hogyan tudjuk azokat a partnereinket szerződéses kötelezettségeik teljesítésére rávenni, akikkel még az IT-biztonsági rendszer bevezetését megelőzően kerültünk kapcsolatba? Ha a szerződés megkötésekor még nem volt hatályban az Ibtv. hivatkozhatunk arra, hogy a szerződéskori állapothoz képest lényeges körülmény változott, amely körülmény nem róható fel nekünk - rajtunk kívül eső okból vagyunk kénytelenek módosítani azt, vagy elállni tőle. Az új szerződések esetén viszont már a hivataloknál rendszeresített „*Beszerzési eljárásrend*” -ben rögzítjük, hogy azokat az IT-biztonsági követelményeket, amelyek ránk is vonatkoznak szerződéses kötelemként partnereink is biztosítsák. Ha partnerünk nem találkozott még az Ibtv. -vel, de más IT-biztonsági szabvány szerint tanúsított – ilyen például az ISO 27001-s szabványcsalád – van lehetőségünk vizsgálni, hogy az ott kialakított biztonsági szintek megfelelőek-e az általunk elvártaknak? Olyan szervezettel szerződni kritikus szolgáltatások igénybevételére, amelynek nincs tanúsítása kiemelt kockázatként kezelendő és a szerződés megkötésekor a kockázatokkal arányos védelmi intézkedések előírása indokolt.

4.2.1.6. Rendszer és szolgáltatás beszerzés

A hivatalok többsége, ha olyan eszközök/szolgáltatások beszerzését tervezi, amelyek várható bekerülési értéke meghaladja a közbeszerzési értékhatárt, erre szakosodott irodák közreműködését veszik igénybe az ügylet lebonyolításához. Kisebb számban vannak azok a hivatalok, amelyek erre saját szakértőt, vagy pályázati osztályt/csoportot tartanak fenn. A közbeszerzési kiírásokban opció, de az európai uniós forrásokból finanszírozott pályázatoknál kötelező elem az IT-biztonsági szempontok megjelenítése. Ne indítsunk úgy beszerzést, hogy az IT-biztonsági szempontok nem kerülnek be a kiírásba. Sok gondtól óvhatjuk meg magunkat, ha a „*Beszerzési eljárásrend*” kellő alapossággal átgondolt és tartalmazza mindazokat az elvárásokat, amelyeket az IBF-nek ellenőriznie és véleményeznie kell. Az Ibtv. végrehajtási rendelete az „*Adminisztratív védelmi intézkedések*” 3.1.3-s pontjához tartozó 8 alpontban sorolja fel, hogy milyen követelményeket vizsgálunk a *„Rendszer és szolgáltatás beszerzése”* során.

4.2.1.6.1. Konfigurációkezelés

Az ASP pályázat során eszközök beszerzésére is nyílt lehetőségük a hivataloknak. A kiírásban nem konkrét gyártók termékeit sorolták fel, hanem azokat a minimumkövetelményeket, amelyeknek megfelelve bármelyik beszállító alkalmas termékeiből kiválaszthatták a számukra megfelelőt. Ezek a követelmények – illetve ezeknek a követelményeknek megfelelő eszközök – amelyeket a pályázati elszámoláshoz kötelezően csatolni kellett – sok hivatalnál az első *„Alapkonfiguráció”* leírása volt, amelyet a „*Konfigurációkezelés*” nyilvántartásába rögzíteni lehetett. Ez a fejezet a „*Logikai Védelmi Intézkedések*” közé sorolt és a 3.3.6. pont rendelkezik a felépítéséről. Az első ezek közül a *„Konfigurációkezelési eljárásrend”*. Az ASP -s pályázathoz hasonlóan ez a szabályzat leírja, hogy a szervezetnél milyen minimumkövetelmények határozhatóak meg az adott eszközök tekintetében, melyeket információs rendszereink alapkonfigurációiként írhatunk elő. Éves felülvizsgálata és aktualizálása, illetve változások esetén a korábbi verziók megőrzése és eltárolása is kötelező.

A hivatalok jelentős részénél nem állnak készen ilyen részletezettségű nyilvántartások folyamatos kezelésére. A rendszer kiépítésekor rögzítésre kerültek az alapkonfigurációk, de már az éves felülvizsgálatok is csak az újonnan beszerzett termékek paramétereinek rögzítésében merülnek ki. A *„Mentés, archiválás és visszaállítási tesztek”* fejezetben visszautalunk arra, hogy az alapkonfigurációk rögzítése miért lenne fontos egy esetleges katasztrófahelyzet elhárításában?

4.2.1.7. Szervezet szintbe (SZVI), rendszerek osztályba (OVI) sorolása

Az Ibtv. „*Értelmező rendelkezések”* – fogalmi meghatározásai között találjuk a definíciót - *biztonsági szintbe sorolás: „a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;”*

A hivatalok a hatóság jelenleg elfogadott gyakorlata szerint a hivatalok a 3-s biztonsági szinthez rendelt követelmények teljesítését ez év júniusáig valósítják meg. A jelenlegi ellenőrzések során azt tapasztaltuk, hogy a vizsgálatok a 2 -s védelmi szinthez kapcsolódó követelményeket kérik számon és az ehhez kapcsolódó védelmi intézkedések bemutatását kérik.

Az NKI honlapjáról[66] letölthető SZVI-tábla és kitöltési útmutató hasznos segítség a jogszabályban előírt kötelezettségek teljesítéséhez – jelenleg a 2.10 -s verziónál tartunk.

Az önkormányzati szektorban nem gyakori, de egyes kormányhivataloknál már előfordult, hogy az IBF élt a jogszabály által biztosított lehetőséggel és a teljes szervezetre *alacsonyabb* biztonsági szintet határozott meg, mint amelyet megadott az adott szervezet egy szervezeti egységére. A hatóság elfogadta az indoklását és az új besorolást.

Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, az 1. szint eléréséhez szükséges intézkedéseket a 10. § (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő tíz éven belül meg kell valósítani.A magasabb biztonsági szint elérésére - minden egyes szintet érintően, a következő magasabb szintre lépéshez - két év áll rendelkezésére. A szintbesorolást 3 évente, szükség esetén – az elektronikus információs rendszer biztonságát érintő változás esetén, illetve új elektronikus információs rendszer bevezetésekor- soron kívül, dokumentált módon felül kell vizsgálni. (Ilyen jellegű változásnak ítélték egyes hivatalok a választásokat követően a frissen megválasztott polgármester által kinevezett új jegyző beiktatását is.)

A „*biztonsági osztályba sorolás”* az Ibtv. *„Értelmező rendelkezések”* 12. pontjában ilyen definíciót kapott: „*a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása”*.

Az OVI tábla és a kitöltési segédlet szintén az NKI honlapján érhető el – jelenleg a 4.60 -s verziónál járunk. A hatóság részére eddig beküldött űrlapok széles spektrumát foglalják el a különböző értelmezéseknek, melyek az elektronikus információs rendszerek definíciójából fakadnak. Egyeztetések során felmerült, hogy mind a hatóság, mind a hivataloknál kinevezett IBF -ek munkáját megkönnyítené, ha csak azokról a rendszerekről kerülne beküldésre OVI tábla, amelyek megfelelnek az EIR definíciójának. Az ASP szakrendszerei például nem a hivatal üzemeltetésében vannak, besorolásukat sem ő végezte el – ezeket a Magyar Államkincstár határozta meg. A hivatal alkalmazáskatalógusában természetesen nyilvántartjuk és a MÁK ajánlásai szerinti védelmi intézkedéseknek megfelelően kezeljük a hozzáférési pontokat, az ASP klienseket, munkahelyeket.

Azokat a szakrendszereket viszont, amelyeket az ASP keretében „váltottak” le sok helyen még üzemben tartják – új adatokat már nem töltenek fel, de a korábbi nyilvántartásokból még indítanak lekérdezéseket – ezekről a rendszerekről készült biztosan készült OVI tábla és azt a hatóság részére megküldte az érintett hivatal képviselője. (Javasolt megvizsgálni, hogy ezekre az adatokra ebben a formában a továbbiakban is szükség lesz-e: szigorúan értelmezve a jogszabályt ilyen rendszerek *üzemeltetése* a szervezet biztonsági szintjét 4-s besorolásúra emelheti.)

66 https://nki.gov.hu/hatosag/tartalom/urlapok/

4.2.1.8. Naplózás, naplóelemzés

A „*Jogosultságok, szerepkörök, hatókörök*" fejezetben korábban említettük már, hogy *„Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről"* – röviden: GDPR – egyik alapelve az *elszámoltathatóság,* amely alapelvet a megfelelő jogosultságok *ellenőrzésével* és a rendszeren végzett változtatások vagy változtatási kísérletek *rögzítésével* valósíthatjuk meg. Ebben lesznek segítségünkre a naplókezeléssel kapcsolatos szabályok és eljárásrendek.

A hivataloknál kialakított infrastruktúra organikusan fejlődött: az IT-berendezések nem stratégiában rögzített elvek szerint – tervezett módon – kerültek beszerzésre, hanem *igényvezérelten* – az adott feladatok ellátásához éppen szükséges eszközök megvásárlásával. Találkoztunk olyan településsel, ahol azért volt értékelhető szerverpark üzemben, mert egy korábban önkormányzati tulajdonban lévő szolgáltató megszűntette a tevékenységét így az eszközeire már nem volt szükség. (A rajtuk fellehető hálózati operációs rendszerek támogatási időszaka még éppen belül volt a gyártó által garantált határidőn, de a telepítéshez használt adathordozókról már nem lehetett volna újratelepíteni egy másik eszközre.) Naplóbejegyzésekről csak akkor és annyiban értesültek a kezelők, ha az a rendszer kritikus állapotát jelezte, vagy hibaüzenetként jelentkezett. Ezek kezelése sem volt eljárásrendben rögzítve – jó esetben értesítésre került a rendszergazda, aki az adott megyében több településsel is szerződésben volt, de abban nem szerepelt olyan elem, amely a hibabejelentéstől számított meghatározott határidőt tartalmazott volna, amelyen belül biztosan reagálnia kell. Ebben az esetben az IT-biztonsági rendszer kiépítésének egyik feltétele volt, hogy találjunk olyan szakembert, aki heti rendszerességgel megjelenik a helyszínen és legalább a kötelező frissítéseket telepíti, a mentések lefutását ellenőrzi és a kritikus hibaüzeneteket/naplóbejegyzéseket lekezeli.

Tapasztalataink szerint általában is igaz, hogy a naplóállományok jellemzően az adott eszközön tárolódnak, központi naplószerverek nincsenek üzemben, azokat nem vizsgálják és elemzik – mentésükről külön nem gondoskodnak.

Az IT-biztonsági rendszer kiépítése során sikerült a rendszerek üzemeltetőinek figyelmét felhívni a naplóbejegyzések fontosságára és azok rögzítésre kerültek a naplóállományok nyilvántartásában – havi rendszerességgel mentésre kerülnek és megőrzési idejüket az adatvédelmi tisztviselő felülvizsgálta. Elemzésükre csak olyan esetekben kerül sor, amikor valamely incidens kivizsgálása során a nyomrögzítéshez, vagy az események visszajátszásához szükségesek.

Több alkalommal megtörtént, hogy a naplóállományok a rendszerrel azonos partícióra kerültek és elfoglalták a rendelkezésre álló területet – ellehetetlenítve a további üzemszerű működést. A hiba sürgős elhárítást követően sem került sor az esemény elemzésére, amelynek következtében az néhány hónapon belül megismétlődött.

A konfigurációkezelés fejezetben megfogalmazott zárógondolat itt is analóg: jelenleg a hivatalok többségében nincs erőforrás a naplóállományok megfelelő kezelésére és elemzésére.

4.2.1.9. Mentés, archiválás és a visszaállítási tesztek

A 2015. évi 41-s BM rendeletben az adminisztratív védelmi intézkedések között vannak rögzítve a mentésekkel, megbízhatósági és sértetlenségi tesztekkel, helyreállítással és alternatív tárolási helyszínekkel kapcsolatos követelménypontok.

2017. decemberében került kihirdetésre a 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról. A jogszabály 2018 januárjában lépett hatályba. A rendelet megjelenése és annak hatálybalépése között nem volt sok idő a felkészülésre. Azok a települések, akiknél az IT-biztonsági rendszer kiépítése már olyan fázisban volt, hogy a mentési és archiválási eljárásrend kialakításra került csak a megfelelő titkosítási algoritmust kellett megtalálni és az elégséges méretű merevlemezeket biztosítani, hogy a jogszabályban

előírt kötelezettséget teljesíteni lehessen. Akiknél még nem jutott idáig az IBIR bevezetést vezénylő szakember ott előre kellett hozni ennek az eljárásrendnek a testre szabását.

A rendelet célja – olyan kormányzati fenntartású és üzemeltetésű központi tárhelyet biztosítani a hivataloknak, ahonnan katasztrófa esetén igényelhetőek az újratelepítéshez szükséges állományok – nem volt ördögtől való, csak az előkészítés volt kicsit „sietős".

A rendelet által előírt „*Archiválási szabályzat*" elkészítéséhez mintát is kínált a jogalkotó – ezek alapján az IT-biztonsági rendszerben kialakított mentési eljárásrendet csak ki kellett egészíteni ezekkel az elemekkel és már kész is volt a mentési terv, amelyhez ezen a biztonsági szinten (3-s) még nem voltak előírva a visszaállítási tesztek…

Sok hivatal nem rendelkezik olyan tartalék eszközökkel, amelyek alkalmasak lennének a visszaállítási tesztek lefuttatására. A stratégiákban rögzített közép- és hosszú távú tervek közé javasolt felvenni, hogy a megvalósításra keressen forrást a hivatal – rövid távon pedig legalább mérje fel, hogy ez milyen módszerekkel valósítható meg és milyen költséget jelenthet?

4.2.2. Az IBF szerepe, feladatai és kinevezése

4.2.2.1. Az IBF kiválasztása

Az IBF kinevezésének jogszabályi feltételei jól meghatározottak: az Ibtv. 13.§ *„(8) A szervezetnél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel."* (Külön jogszabály[67] rendelkezik arról, hogy ezek a képzettségek milyen módon szerezhetőek meg, mely egyéb képzésekkel egyenértékűek, illetve hány év gyakorlati idő beszámításával teljesíthetőek.)

A szükséges képzettségek mellett a büntetlen előéletet nemcsak a kinevezést *megelőzően*, de a megbízás időtartama *alatt* is ellenőrizheti a szervezet – ennek szintén adottak a jogszabályokban rögzített feltételei: Ibtv. 13.§ *„(9) pont - A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni. A szervezet az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja."*

Ha találunk is olyan személyt, aki a fentiekben megfogalmazott feltételeknek megfelel még mindig felvetődik a kérdés: szervezeten belül találjunk – neveljünk ki – alkalmas kollégát, akit alkalmazotti jogviszonyban foglalkoztatunk, vagy keressünk inkább olyan társaságot, akinek IT-biztonsági profiljában fellelhető ilyen típusú szolgáltatás? Nincs egyértelmű válasz a kérdésre: a tapasztalatok azt mutatják, hogy mindkét megoldás működőképes lehet. Minden az adott szervezet IT-biztonsági felkészültsége/érettsége – és a vezetői elköteleződés mértékétől függ. Fontos még megjegyezni, hogy az önkormányzati szektorban az alkalmazott bérezési rendszer nem teszi igazán vonzóvá ezt a beosztást a piaci bérezéssel szemben.

Az IBF-nek mindezeken túl olyan emberi tulajdonságokkal is rendelkeznie kell, amely alkalmassá teszi őt a szinte lehetetlen – néha egymásnak ellentmondó – feladatok ellátására. Minden olyan eseményért felelősséggel tartozik, amely a szervezeten belül az IT-biztonsággal kapcsolatba hozható: észleli a fenyegetéseket és a kockázatokat; naprakészen ismeri a terület jogi és technikai vonatkozásait; szót ért mind a felhasználókkal, mind az IT-infrastruktúrát üzemeltető és fejlesztő kollégákkal;

[67] 26/2013. (X. 21.) KIM rendelet - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.

oktató, tanácsadó és auditor is egyszerre; ezeken felül a számonkérésre is alkalmas kompetenciákkal bíró személyiségvonásokkal rendelkezik. Az IT-biztonság az egyik leggyorsabban fejlődő terület – napi munkájának ellátása mellett folyamatosan képezi magát, hogy a szervezet, amelyik megbízta ezzel a feladattal biztonságban tudja az erőforrásait: adatait, üzleti folyamatait és mindazokat, akik ennek működését élvezik és biztosítják.

4.2.2.2. Az IBF bejelentése és elhelyezkedése a szervezeti hierarchiában

Ha sikerül kiválasztani a megfelelő jelöltet, aki minden feltételnek megfelel – büntetlen előéletű, képzettsége és tapasztalata a jogszabályban előírt – rátermett a feladatára és a hatóság előzetesen jóváhagyta/véleményezte a személyét – a bejelentést a hatóság erre kialakított elektronikus felületén tehetjük meg. A regisztráció folyamatáról az NKI weboldalán itt tájékozódhatunk:

https://nki.gov.hu/hatosag/tartalom/ugyfajtak/elektronikus-informacios-rendszer-biztonsagaert-felelos-szemely-nyilvantartasba-vetele-regisztracio/

Az Ibtv. törvény előkészítése során az *összeférhetetlenségi* szabályokat még markánsan meg kívánták jeleníteni a közreműködő szakértők. Ezirányú törekvéseik az egyeztetések során „elvesztek” – maradt a józan megfontolás: olyan hierarchia kialakítása célszerű, amelyben elkerülhető, hogy az IBF ellenőrzése alá vont területek vezetői utasítási jogkörrel rendelkezzenek felette.

A jogszabály csak annyira kötelez a 13.§ első pontjában, hogy: *„(1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.”*

Követendő gyakorlatnak tekinthető a GDPR iránymutatásai szerint kinevezett adatvédelmi tisztviselő (DPO) jogállása köré épített védelem. (GDPR törzsszöveg, 38. cikk – Az adatvédelmi tisztviselő jogállása - (3) bekezdés *„Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.*”) Működésük feltételei láthatóan már az uniós rendelet törzsszövegében is megjelentek – az adatvédelmi munkacsoport pedig további iránymutatásokat tett közzé, amelyeket a magyar hatóság a honlapján is elérhetővé tett[68].

Az eddig összegyűjtött tapasztalatok alapján a kialakult jó gyakorlat ebben a szektorban főként azokon a településeken, ahol az IT-biztonsági feladatokra csak részmunkaidőben lehetne státuszt biztosítani: külső megbízással foglalkoztatni megfelelő kompetenciával bíró személyt. Nagyobb szervezetek is gyakran választanak külsős IBF -et, mert a megfelelő kompetenciákkal rendelkező szakemberek száma véges, képzési és járulékos költségei magasak és a szervezettől kellő távolságot tartva jobb rálátással rendelkezhet, pártatlansága és függetlensége is könnyebben biztosítható.

[68] https://www.naih.hu/files/WP243_rev01_hu.pdf

4.2.2.3. További IT-biztonsági szereplők

Az IT-biztonsági rendszer kialakításában üzemeltetésében és felügyeletében résztvevők: az elektronikus információs rendszer vezetője (EIV), az információbiztonsági felelős (IBF), az IT-biztonsági rendszer üzemeltetésében résztvevő személy és az információbiztonsági felügyelő. Külön fejezetet érdemel még az adatvédelmi tisztviselő (DPO) is.

4.2.2.3.1.EIRÜRSZ – az elektronikus információbiztonsági rendszer üzemeltetésében résztvevő személy

Az EIV -hez hasonlóan ezt a személyt – vagy személyeket – is az éves kötelező továbbképzésekre kötelezik – egyéb feltételekhez nem kötik az alkalmazását. Olyan szervezeteknél fordul elő, ahol az IT-biztonsági rendszer üzemeltetésének operatív feladatai már meghaladják egy személy erőforrásait/kapacitását.

4.2.2.3.2. IBFE – az Információbiztonsági felügyelő

Különös szereplője ez a személy az IT-biztonsági területnek: különleges jogosítványokkal bír és az Ibtv. 16. § -nak 3. bekezdésében írja le mely esetben dönt a hatóság a kirendeléséről: *„Ha a szervezet költségvetési szerv, és a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be”.* Természetesen a kirendelést megelőzően felszólítja a szervezetet, hogy tegyen eleget kötelezettségeinek és a törvény 2019 -ben elfogadott módosításában már a bírság kiszabásának és a kirendelés okán felmerülő költségek megtérítésének lehetősége is a jogkövető magatartást kikényszerítő eszközök közé került.

Ismereteink szerint a törvény elfogadása óta információbiztonsági felügyelő kinevezésére még nem került sor.

4.2.2.3.3. DPO – Az adatvédelmi tisztviselő

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) – ismertebb nevén a GDPR – egy lényeges új szerepkört hozott létre és azoknál a szervezeteknél, ahol a személyes adatok védelmét az addigi jogszabályok mellett további garanciákkal is szükségesnek ítélték biztosítani kötelezően megbízást is kell adni ilyen személynek. (Az önkormányzatok már korábban is rendelkeztek ilyen *jellegű* feladatok ellátására nevesített személlyel – ő volt a „*belső adatvédelmi felelős*”.) A GDPR rendelkezéseit nem kellett a hazai jogrendbe átültetni: a benne foglaltak a tagállamokban közvetlenül hatályosultak. A törvényalkotó - élve a rendeletben biztosított jogával - egyes területeket részleteiben is kibontott és a kapcsolódó irányelveknek megfelelően ültetett át a 2011. évi adatvédelmi törvénybe – továbbiakban: Infotv[69]. Kinevezéséhez nincsenek kötve az IBF -nél előírt kötelező végzettségek – az ajánlásokban a „rátermettséget” és a hazai, illetve nemzetközi adatvédelmi jogszabályokban való jártasságot, annak szakértői ismeretét említik meg, emelik ki. A rendelet kötelező alkalmazását megelőzően és az Infotv. kapcsolódó módosításainak elfogadásának időszakában nem volt teljesen világos, hogy a DPO elláthat-e IT-biztonsági felelősi beosztást is, de mára már tisztázódni látszik, hogy a két terület eltérő kompetenciákat és szemléletet kíván, amelyek feloldása egyszemélyi kinevezettek esetében összeférhetetlenségi kérdéseket vethet fel. Ismereteim szerint egységes állásfoglalást a NAIH még nem tett közzé nyilvánosan elérhető anyagai között.

[69] https://net.jogtar.hu/jogszabaly?docid=a1100112.tv

Az adatvédelmi tisztviselők támaszkodnak az IT-biztonsági rendszer egyes elemeire, de szemléletmódjuk alapvetően különbözik az IT-üzemeltetéssel, fejlesztéssel és biztonsággal foglalkozó szakemberekétől. A fókusz esetükben a személyes adatokra, azok kezelésével kapcsolatos folyamatokra irányul. Sok hivatalnál nem is igazán tudtak különbséget tenni a két funkció – IBF és DPO – között – ráadásul korábban még a hatóságok rövidített nevei is csak egy betűben különböztek egymástól: NAIH és NEIH. Biztonsági események vizsgálata során már annak észlelésekor javasolt bevonni az adatvédelmi tisztviselőt, hogy az adatvédelmi vonatkozások tekintetében időben eljárhasson és ha szükséges a rá ruházott kötelezettségeit teljesíteni tudja. (72 órája van, hogy a hatóságot értesítse, ha olyan súlyú adatvédelmi incidenst fedez fel, mely a természetes személyek jogaira és szabadságaira nézve magas kockázattal járhat.) És fordítva: az adatvédelmi incidensek esetenként (például: szándékos támadások, visszaélések) „tartalmaznak" olyan biztonsági eseményre utaló nyomokat, amelyek kivizsgálásához IT-biztonsági kompetencia szükséges – a hivataloknál például az IBF. Az adatvédelmi incidensek hatóság felé történő bejelentésének kötelező tartalmi eleme, hogy bemutassa: milyen IT-biztonsági intézkedések történtek eddig az incidens megszűntetése érdekében és melyek azok, amelyeket a hasonló esetek elkerüléséért fognak alkalmazni a jövőben.

A fentiekből leszűrhető: a DPO értékes és hasznos tagja a szervezet IT-biztonsági szereplőinek – az együttműködés mindkét fél számára gyümölcsöző lehet – egymásrautaltságuk felismerése segíthet ennek kiépítésében!

4.3. Üzemeltetés

4.3.1. Oktatás

A „*Felvételi eljárás(ok) rendje*" fejezetben utaltunk rá, hogy a *belépéskor* kötelező oktatás munkakörönként különböző szinteket jelenthet – jelenleg a kétszintű – rendszergazdai és felhasználói – az elterjedt. A rendszergazdák mélységében kell ismerjék a rendszert és betekintésük van az IBSZ teljes struktúrájára – értik és alkalmazzák az abban leírtakat. A felhasználók az IBSZ kivonatát kapják csak kézhez – a viselkedési és felelősségi szabályokra koncentrál az oktatás – a tesztkérdések is ilyen szinten kerülnek összeállításra.

Jogviszony megváltozása esetén – új munkakör felvételekor – is szükséges lehet az ismeretek felelevenítése és előfordulhat, hogy a felhasználó az új munkakörében másféle hozzáférésekkel bír majd, amelyhez más típusú felelősségek tartoznak. Ennek ismertetésére szintén az oktatás kínál megoldást.

Az NKI heti rendszerességgel küldi ki hírlevelét, amelyben tájékoztatást nyújt az esetleges adathalász kampányokról, vagy egyéb rosszindulatú tevékenységekről. Érdemes ébren tartani a felhasználóink figyelmét és figyelmeztetni őket a lehetséges veszélyekre – ezt a tevékenységet is az oktatási tevékenységekhez sorolhatjuk.

Ha nem érkezett időben a figyelmeztetés és olyan biztonsági esemény következik be, amelynek tanulságait meg kívánjuk osztani az állománnyal érdemes rendkívüli alkalmat szervezni, amelyben felhívhatjuk az érintetti kör figyelmét mire érdemes ügyelni a jövőben. Ezek az alkalmak szintén bekerülhetnek az oktatási tervbe és nyilvántartásba.

Éves kötelező továbbképzésre kötelezett az IBF – érdemes a felhasználókat is legalább ilyen rendszerességgel összehívni és felelevenníteni a korábban már ismertetett alapelveket kiegészítve az év közben tapasztaltakkal. Az NKI médiaközpontjából[70] letölthető videók kifejezetten jó színvonalúak és olyan területeket mutatnak be, amelyek személyesen is megérinthetik a felhasználóinkat – érdemes használni őket.

[70] https://nki.gov.hu/it-biztonsag/mediatar/

4.3.2. Változásjelentések

A rendszer üzemeltetése során javasolt legalább havi rendszerességgel összegyűjteni azokat az elemeket, amelyek az IT-biztonsági rendszer működésének bizonyítékaként is értelmezhetőek. A normál üzemmenet során meg kell jelenjenek ezek a szempontok is, mert fontos, hogy a nyilvántartások aktuálisak, a valóságot hűen tükrözőek legyenek. .

Az *új belépők* nyilvántartása nemcsak a megfelelő jogosultságok kiosztása miatt fontos, hanem az oktatás és a nyilatkozatok ellenjegyzése miatt is. A viselkedési szabályok megismerése és annak elfogadása *alapvető* érdeke a szervezet minden felelős beosztásban dolgozó tagja részére.

A *kilépők* havi jelentésben történő rögzítése szintén olyan adat, amely áttekinthetővé teszi a nyilvántartást.

Havi rendszerességgel javasolt elkészítetni a jelentést az ütemezett/eseti javítások és karbantartások megtörténtéről: az ütemezett karbantartások megelőzhetik a meghibásodásokat – az eseti javításokról szóló jelentések pedig lényeges információkkal bírnak az adott berendezések állapotáról, meghibásodási gyakoriságáról.

Javasolt, hogy a felhasználói szabályokat sértő cselekményeket is kerüljenek nyilvántartásba – azok felderítésének időpontjával és az esetleges következmények ismertetésével együtt.

A naplóállományok elemzésére tapasztalataink alapján nagyobbrészt a biztonsági események bekövetkeztekor kerül sor. Megelőző védelmi intézkedésként ebben a szektorban a rendelkezésre álló erőforrások elosztásakor nem kerül fókusz erre a területre. Csak a normál üzemmenettől jelentősen eltérő értékek esetén kap értesítést a rendszer felügyeletével megbízott személy és csak kivételes esetekben volt megfigyelhető központi naplókezelés. Javasolt az esetleges eltérések rögzítésén túl a naplóállományok ellenőrzése – a normál üzemmenet során is.

4.3.3. Biztonsági események és incidensek

Az Ibtv. a *biztonsági eseményeket* az értelmező rendelkezések részben az alapfogalmak között a 9. pontban így írja le: *„nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;”.* Ez a megfogalmazás az *incidens* általánosan elfogadott jelentésétől azért különbözik, mert az Ibtv. kodifikációs eljárása során idegen szónak tekintették azt. Ennek következtében van most lehetőségünk megkülönböztetni ezeket a fogalmakat az IT-biztonsági terminológiában az adatvédelmi szóhasználattól, amely a saját rendelkezéseiben következetesen *adatvédelmi incidensként* használja azt. Az adatvédelmi tisztviselő (DPO) hogyan definiálja a „nem várt” eseményeket? GDPR törzsszöveg, 4. cikk 12. pont - „*adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;”.* Ezek a definíciók analógok az IT-biztonság alapfogalmaival: *bizalmasság*, *sértetlenség*, *rendelkezésre állás*.

Az önkormányzati szektorban azt tapasztalható, hogy az IT-biztonsági rendszer bevezetését megelőzően nem voltak biztonsági események – nyilvántartásba véve… Az ilyen jellegű incidenseket azért „titkolták” el, vagy próbálták házon belül megoldani, mert annak beismerése, hogy a hivatalban bármiféle rendellenes működés mutatkozhat ellenkezett a korábban megszokott beidegződésekkel. Ennek feloldására a biztonsági események nyilvántartásába kötelező jelleggel felvetettük az NKI riasztásait, amelyek így nem helyi kompetenciaként kerültek rögzítésre, hanem központilag elrendelve, amely a hivatal hierarchikusan felépített szervezeti rendszerének viszonyaira adaptálva könnyebben

elfogadtatható volt. A másik érv, amellyel sikerült „érzékenyítenünk” az érintetteket a tájékoztatással elérhető figyelmeztetés – segítségnyújtás – lehetősége volt, amellyel – ha időben értesülnek a lehetséges károkozókról – megelőzhetőek a súlyosabb adatvesztések, kiesések. Saját hibáink és tapasztalataink *edukációs* jelleggel történő megosztására nagyobb hajlandóság tapasztalható.

Az incidensek kezelésére felállítandó „operatív csapat” – mai szóhasználattal: törzs – összeállításakor szintén találkoztunk megkérdőjelezhető hozzáállással… Volt település, ahol a hivatal törvényességének őre nem szeretett volna felkerülni az értesítendők listájára. Megtörtént eset: egy megyei kormányhivatal vezetője a helyi sajtóból értesült arról, hogy szervezete egyik gépéről kéretlen üzeneteket küldenek. Ő a hivatalába beérkezve kifejezetten kérte, hogy a továbbiakban az elsők között értesítsék a hasonló esetekről. Megítélésem szerint egyébként ez utóbbi hozzáállás a felelős vezetői magatartás.

Az Ibtv. 19. § (4) bekezdésében *egyértelműen utal* arra, hogy: *„A 2. §-ban meghatározott szervek a tudomásukra jutott biztonsági események adatait kötelesek haladéktalanul az (1) bekezdés szerinti eseménykezelő központ részére továbbítani.”*

Az önkormányzatok és hivatalaik számára a bejelentés megtételére ezen a linken nyílik lehetőség: https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/

Az események megelőzése, felderítése, esetleges bekövetkezésekor a további hibás működés megszűntetése, a károk elhárítása, a működés helyreállítása és az eseményeket követően a felelősök előtalálása – a friss élmény hatása alatt – még meg szokott történni, de az értékelés és az okok felkutatását követő biztonsági elemzés és a kockázatok újraértékelése - sok esetben - elmarad, illetve olyan hosszú idő után kerül rá sor, amely megnehezíti – talán el is lehetetleníti az érdemi munkát. Megítélésünk szerint épp ez az a lépés, amely a rendszer védelmi képességeit emelni lenne képes: szomorú látni, hogy a napi üzemeltetési feladatok sokasága épp ezektől a lehetőségektől fosztja meg a szervezeteket! (Más ágazatban volt „szerencsénk” egy olyan incidenst vizsgálni, amelynek hatására a korábban a mentések előállítására rendelkezésre álló idősáv a többszörösére nőtt. Az okok kiderítését megelőzően sajnos nem kerültek rögzítésre azok a „nyomok”, amelyek alapján visszakövethető lett volna mi történt – a gyors hibajavításnak áldozatául estek a későbbi elemzésre lehetőséget kínáló állományok. Ebben a helyzetben a probléma ismételt előfordulásának valószínűsége magasabb – az értékelés során nem lehetett megfelelő – bizonyítékokkal alátámasztott - védelmi intézkedéseket foganatosítani.)

5. JOGSZABÁLYTÁR

5.1. Magyar jogszabályok

- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=99700047.tv
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
  https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
  Elérhetőség: https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 2003. évi C. törvény az elektronikus hírközlésről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- 2009. évi CLV. törvény a minősített adat védelméről
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- 2021. évi XCI. törvény a nemzeti adatvagyonról
  https://net.jogtar.hu/jogszabaly?docid=a2100091.tv
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról;
  https://net.jogtar.hu/jogszabaly?docid=a1100038.kor
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- 1035/2012. (II. 21.) Korm. határozata - Magyarország Nemzeti Biztonsági Stratégiájáról
  https://net.jogtar.hu/getpdf?docid=A13H1139.KOR&targetdate=&printTitle=1139/2013.+%28III.+21.%29+Korm.+hat%C3%A1rozat&getdoc=1
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158

- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól Hatályon kívül helyezte: 2015. évi CCXXII. törvény 121. § (1) b).
  https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV
- 26/2013. (X. 21.) KIM rendelet - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
  https://net.jogtar.hu/jogszabaly?docid=a1300026.kim
- 65/2013. (III. 8.) Korm. rendelet - A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
  https://net.jogtar.hu/jogszabaly?docid=a1300065.kor
- 360/2013. (X. 11.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről Hatályon kívül helyezte: 374/2020. (VII. 30.) Korm. rendelet 22. §
  https://net.jogtar.hu/jogszabaly?docid=a1300360.kor
- 512/2013. (XII. 29) Korm. rendelet az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII. 13.) Korm. rendelet módosításáról
  https://net.jogtar.hu/jogszabaly?docid=a1300512.kor
- 540/2013. (XII. 30) Korm. rendelet a létfontosságú agrárgazdasági rendszerelemek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1300540.KOR
- 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=a1300541.kor
- 2015. évi CCXXII. törvény - Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1500222.tv
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
  https://net.jogtar.hu/jogszabaly?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
  Hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
  https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR
- 39/2016. (XII. 21.) EMMI rendelet az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról
  https://net.jogtar.hu/jogszabaly?docid=a1600039.emm

- 386/2016. (XII. 2.) Korm. rendelet az egészségbiztosítási szervekről https://net.jogtar.hu/jogszabaly?docid=a1600386.kor
- 257/2016. (VIII. 31.) Korm. rendelet - Az önkormányzati ASP rendszerről https://net.jogtar.hu/jogszabaly?docid=a1600257.kor
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- 148/2018. (VIII. 13.) Korm. rendelet az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet és az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet módosításáról https://net.jogtar.hu/getpdf?docid=a1600257.kor&targetdate=&printTitle=257/2016.+%28VIII.+31.%29+Korm.+rendelet
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR
- 271/2018. (XII. 20. Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról http://njt.hu/cgi_bin/njt_doc.cgi?docid=212067.363096

5.2. Európai Uniós jogi aktusok

- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU
- Számítástechnikai bűnözésről szóló Egyezmény (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU

- A Tanács következtetései a kiberdiplomáciáról (2015)
  http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf
- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról
  http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017):
  http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

6. FOGALOMTÁR

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [1]
- **Adatbiztonság***:* Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat**: Más néven phishing, amelynek lényege abban rejlik, hogy az adathalászok a felhasználókat valamilyen elektronikus csatornán keresztül – például e-mailben, azonnali üzenetben, vagy éppen szalagcímhirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó***:* Az a személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó***:* Minden olyan anyagi eszköz, amely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését. Így adathordozó a pendrive, a DVD, CD, SSD-kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés***:* Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok 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 (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]
- **Adatkezelő***:* Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem***:* A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[5]
- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megvál-

toztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot, nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]

- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, a titoktartási kötelezettség alóli felmentés, a megismerési engedély kiadása. [5]
- **Adatokat érintő beavatkozás:** információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is. [6]
- **Adatkifürkészés**: digitális adatok információs rendszeren belüli, oda irányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel. [6]
- **Advanced persistent threat (APT)**: Magas szintű, tartós vagy más (és az anyagban is használt) néven célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [7]
- **Aktív kiberbiztonság (Active Cyber Defence Cycle** – ACDC): Aktív kiberbiztonsági intézkedések gyűjtőfogalma. Az aktív kiberbiztonság négy nagyobb tevékenységből áll, ezek a fenyegetéselemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; és a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [9]
- **Application Programming Interface**: Alkalmazásprogramozási interfész, amely hozzáférést biztosít egy adott szoftver vagy eszköz utasításkészletéhez. [10]
- **ASP-szolgáltatás**: Az alkalmazásszolgáltató (Application Service Provider – ASP) központon keresztül olyan hardver- és szoftver-infrastruktúra, arra épülő keret- és szolgáltatási rendszer jön létre, amely által az önkormányzatok szakrendszeri és egyéb szolgáltatásokat vehetnek igénybe egymással integrált módon. [11]
- **Authentikáció**: Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [12]
- **Automatizált informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [13]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindu-

latú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [14]

- **Betörésdetektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a mintaalapú betörésdetektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörésdetektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [15]
- **Big Data**: A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [16]
- **Biometrikus azonosítás**: Olyan eszközök és eljárások összessége, amelyek a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, tenyér vénamintáinak azonosítása, gépelési minta alapú azonosítás. [17]
- **Bizalmasság elve***:* Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható, vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény***:* Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése***:* Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály***:* Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás***:* A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint***:* A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás***:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonságtudatosság**: A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét, és figyel az őt esetlegesen érintő fenyegetésekre. [18]
- **Black hat hacker**: Ide tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább az etikus és az etikátlan hackerek között húzható meg. [19]
- **Bot-eszközök**: automatizált rendszerek, amelyek valamilyen tevékenységet hajtanak végre emberi beavatkozás nélkül. [20]
- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, amelyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen használnak. Egy számítógépes vírushoz képest a fenyegetés "megalkotója" ebben az esetben

nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [15]

- **CIA**: Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [5]
- **Cleartext jelszavak**: Titkosítatlanul, szöveges formátumban tárol jelszavak. [20]
- **Cloud computing**: („számítástechnikai felhő", „felhőalapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azokat nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhőalapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhőalapú informatikaalapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail) vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját – főleg marketing- – céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhőalapú szolgáltatástól szabadulni. [2]
- **CMS (Content Management System):** Más néven tartalomkezelő rendszer, olyan komplex webes környezet, ami lehetővé teszi, hogy tartalmainkat – webfejlesztő szakemberek segítsége nélkül – saját magunk, webes felületeken keresztül módosítsuk. [10]
- **CRM (Customer Relationship Manager)**: Olyan eszközök összessége, amelyek segítik a potenciális és meglévő ügyfelekkel való együttműködést, beleértve az ügyfélszerzéssel, marketinggel, értékesítéssel és ügyfélszolgálattal kapcsolatos tevékenységeket. [10]
- **Dead drop**: Az alkalmazott módszer lényege, hogy a kereskedő valamilyen nyilvánosan elérhető rejtekhelyen elrejti az árut, majd a rejtekhelyről értesíti a vásárlót, aki a rejtekhelyen felszedi a megvásárolt terméket. A dead drop módszer előnye, hogy teljesen aszinkron, azaz az értékesítő (vagy közvetítő) és a vásárló nem tartózkodik egy időben az átadási ponton, nem lehet a csomagokat követni vagy feltartóztatni, a vásárlónak nem kell kontakt vagy más személyes adatot megadnia a kézbesítéshez (pl. cím, postafiók stb.), így a kereskedőnek nem is kell ezeket az adatokat tárolnia és megvédenie, nem tudnak egymásra vagy egymás ellen vallani. [20]
- **Domain Name System (DNS):** Azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az *internetre* vagy egy *magánhálózatra* kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott *tartománynevekhez* (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le", „oldja fel", melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [22]
- **DNS-szerver**: A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [22]
- **Elektronikus információbiztonság**: Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és

megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. [3]

- **Elektronikus információs rendszer**:
  a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
  b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
  c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.
  Egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök - így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók -, eljárások - így különösen szabályozás, szoftver és kapcsolódó folyamatok -, valamint az ezeket kezelő személyek együttesét. [1]
- **Elektronikus információs rendszer biztonsága**: Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elektronikus hírközlő hálózat**: Átviteli rendszerek és – ahol ez értelmezhető – a hálózatban jelek irányítására szolgáló berendezések, továbbá más erőforrások – beleértve a nem aktív hálózati elemeket is –, amelyek jelek továbbítását teszik lehetővé meghatározott végpontok között vezetéken, rádiós, optikai vagy egyéb elektromágneses úton, beleértve a műholdas hálózatokat, a helyhez kötött és a mobil földfelszíni hálózatokat, az energiaellátó kábelrendszereket, olyan mértékben, amennyiben azt a jelek továbbítására használják, a műsorszórásra használt hálózatokat és a kábeltelevíziós hálózatokat, tekintet nélkül a továbbított információ fajtájára.[23]
- **Elosztott szolgáltatásmegtagadásos támadás***:* Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **ENISA (Európai Uniós Kiberbiztonsági Ügynökség):** az EU elsőszámú kiberbiztonsággal foglalkozó intézménye, a kiberbiztonsággal kapcsolatos tanácsadásért felelős ügynökség, amely információs és tudásközpontként működik. [21]
- **EPCIP (European Programme for Critical Infrastructure Protection):** a kritikus infrastruktúrák védelmére irányuló európai program, amelynek célkitűzése, hogy javítsa a létfontosságú infrastruktúrák védelmét az Európai Unióban. [21]
- **Ethernet**: A DEC, az Intel és a Xerox cégek által kidolgozott alapsávú LAN-ra vonatkozó specifikáció. Az Ethernet-hálózatok az ütközések feloldására a CSMA/CD-t használják. Számos kábeltípuson (csavart érpár, optika stb.) működik legalább 10 Mbps sebességgel). [22]
- **Europol:** Európai Rendőrségi Hivatal, amelynek fő feladata segítséget nyújtani az EU-s tagállamok bűnüldöző hatóságainak a terrorizmus elleni fellépésben, illetve a súlyos nemzetközi bűncselekmények felderítésében. [21]
- **Eseménykezelő Szakterület (Event Detection Team):** Intézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hi-

szen alapvetően passzív adatforgalom-ellenőrzésről és annak elemzéséről van szó. A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján azonosíthatjuk a támadók által felhasznált internetes erőforrások címeit, másrészt – különböző elemző algoritmusok segítségével – felfedezhetjük a behatolási módszerek alkalmazási trendjeinek aktuális alakulását, valamint következtetéseket vonhatunk le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről. [21]

- **Exploit**: Olyan forráskódban terjesztett 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.[10]
- **Fenyegetés***:* Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Folytonos védelem**: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Fluxus**: A fluxus a felületet metsző mágneses erővonalak mennyisége. [21]
- **Fuzzing**: Egy leginkábban automatizált módon végrehajtott szoftvertesztelési technika, amelynek során érvénytelen, véletlenszerű, illetve nem várt adatokat adunk meg a program bemeneteként, majd a kimenetet megvizsgálva próbáljuk megtalálni a sérülékeny pontokat. Ezzel a technikával főkent overflow, illetve DoS jellegű sérülékenységeket kereshetünk hatékonyan, miközben a szoftver kivételkezeléséről és robosztusságáról is képet kaphatunk. [10]
- **Gateway**: Átjáró, konverter eszköz, különböző protokollon kommunikáló eszközök között. [22]
- **GDPR**: A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Hacker**: Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus**: Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, hogy elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadásokat, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk, bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [24]
- **Hálózat**: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hálózati és információs rendszer:** elektronikus hírközlő hálózat, vagy minden olyan eszköz vagy egymással összekapcsolt eszközök csoportja, amelyek digitális adatokat dolgoznak fel, valamint a tárolt, kezelt, visszakeresett vagy továbbított digitális adatok. [6]

- **Hardver**: Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt, vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okos eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, amelyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [25]
- **Hash függvények**: Olyan, elsősorban informatikában használt egyirányú eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adat neve *hash* érték. [10]
- **Hitelesség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Honeypot (csapdarendszer)**: Elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapdarendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapdarendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapdarendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [26]
- **IKT-szolgáltatás**: Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [21]
- **IKT-termék:** Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [21]
- **Illetéktelen személy**: Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ**: 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. [1]
- **Információbiztonság***:* Olyan tevékenység vagy állapot, amelynek középpontjában a bizalmasság, a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [25]
- **Informatikai biztonság**: Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika**: A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia**: Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **Internet of Things (Iot)**: A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra és azok internetszerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni", és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [27]

- **iOS**: Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja**: A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Kémprogramok** (**spyware**): A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, amelyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [14]
- **Kiberbiztonság**: A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez. [1]
- **Kiberfenyegetés**: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat. [21]
- **Kibervédelem**: A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér-képességek megőrzését. [1]
- **Kiberbűnözés***:* **Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amely rendkívül adaptív tulajdonsággal jellemezhető, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket.**
- **Kiberhadviselés***:* Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [28]
- **Kiberkémkedés***:* Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [29]
- **Kihívás:** Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást, és kihatással lehetnek egy adott régió hatalmi viszonyaira. [30]
- **Kockázat***:* A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Kombólista:** olyan gyűjtemény, amelynek a forrása nem ismert. Általában a kombólisták értéke meglehetősen csekély, több terabyte méretben érhetők el különféle oldalakon vagy szolgáltatásokban, például a Collections adatszivárgás jelentős része kombólista, csupán felhasználónevet és jelszót tartalmaz, amelyekről a legtöbb esetben nem lehet tudni, hogy honnan származnak, azaz hova lehet belépni ezekkel az adatokkal. [20]
- **Korai Figyelmeztető Rendszer (Early Warning System – EWS):** Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának az ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. [26]
- **Közigazgatás**: Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.

- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [21]
- **Kritikus infrastruktúra**: azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotórészei, amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszú távon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére. [14]
- **Kritikus sérülékenység**: Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [13]
- **Kvantumkriptográfia (Quantum cryptography):** Olyan technikák összessége, amelyekkel egy adott fizikai rendszer kvantummechanikai tulajdonságainak mérése révén –
- beleértve a kifejezetten a kvantumoptika, kvantumtérelmélet vagy kvantum-elektrodinamika által meghatározott fizikai tulajdonságokat is – közös „rejtjelezési" kulcs hozható létre. [31]
- **Létfontosságú információs rendszerelem**: Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené. [1]
- **Létfontosságú rendszerelem**: az Lrtv. 1. mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, - és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. [32]
- **Malware**: Az angol malicious software (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [14]
- **MFP (Multi-Functional Printer):** Olyan multifunkcós nyomtató, amely fénymásolóként, szkennerként, nyomtatóként és néha faxként is működik, miközben gyakran hálózatra csatlakoztatható. [10]
- **Minősített adat**: A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. A „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]

- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- **NEIH**: Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt, vagy más módon tudomására jutott biztonsági rések elhárítását, és ellenőrzi a helyreállító intézkedés eredményességét. [15]
- **Nemzeti adatvagyon**: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége.[33]
- **Nemzeti Kibervédelmi Intézet**: A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [15]
- **P2P: peer-to-peer** Olyan kommunikáció, ahol a szereplők kitüntetett csomópont vagy központi szerver nélkül, közvetlenül egymással kommunikálnak [20]
- **PDCA:** Plan-Do-Check-Act = Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás.
- **Port kopogtatás (port knocking):** Olyan módszer, amely segítségével megfelelő sorrendben próbálunk, előre meghatározott portokon keresztül kommunikálni, aminek hatására más portok is elérhetővé válnak. [10]
- **Ransomware***:* Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejé-ben visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [34]
- **Rendelkezésre állás elve**: Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Scareware**: Ál-vírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek, vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg nem akarják meggyőzni a felhasználót a „teljes verzió" megvásárlásáról), és semmilyen, vagy legalábbis minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [18]
- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy

az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]

- **Sérülékenység**: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]
- **Sérülékenységvizsgálat**: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.[5]
- **Social engineering***:* Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. [18]
- **SPF (Sender Policy Framework):** Egy olyan DNS rekord, amit annak igazolására használnak, hogy az email feladója, valóban a domén jogos tulajdonosa-e, illetve, hogy abból az IP-címtartományból történik-e az üzenet feladása, amelyből adott domén esetében ez lehetséges. [10]
- **Súlyos biztonsági esemény**: Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [15]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik (európai használatban: CSIRT [Computer Security Incident Response Team], amerikai használatban: CERT [Computer Emergency Response Team]). [35]
- **Számítógépes féreg***:* Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Személyes adat**: Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [36]
- **Szolgáltatásmegtagadásos támadás***:* Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **SQL injection**: Más néven SQL-befecskendezés. Ez egy olyan exploit, amely azokat az adatbázis-lekérdező programokat használja ki, ahol nem tesztelték le alaposan a lekérdezések metódusát. Az SQL injection parancsokat küld a webszerverhez kapcsolt SQL-adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor az űrlap mezőkbe – mint például a felhasználónév – közvetlen parancs adható meg az SQL-szervernek. Így például a támadó a megfelelő parancs megadásával kinyerheti az adott oldal összes felhasználójának nevét vagy egyéb kritikusabb táblák információit is. [22]
- **TCP/IP** = A TCP/IP betűszó az angol Transmission Control Protocol/Internet Protocol (átviteli vezérlő protokoll/internetprotokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről. [22]
- **Teljes körű védelem**: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **TOR (The Onion Router)**: Ezen hálózat azzal biztosítja a felhasználók anonimitását, hogy hagymaszerűen felépülő, többrétegű titkosítást alkalmaz. Ez biztosítja, hogy maga a kommu-

nikáció, sőt az egyes adatcsomagok útvonala hétköznapi eszközökkel nem fejthető vissza. A hálózatot TOR-klienst futtató gépek alkotják, ezek lehetnek node-ok vagy ún. TOR-exitek. [10]

- **Trójai progam***:* Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat, vagy akár adatállományokat törölnek. [14]
- **Tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [37]
- **UAV (Unnamed Aerial Vehicles):** Ember nélküli légi járművek. [38]
- Üzletmenet-folytonosság **tervezése**: Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. Ang.: Business Continuity Planning (rövidítve: BCP). [5]
- **Védelmi intézkedések**: Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Vezeték nélküli személyi hálózat (WPAN)**: A vezeték nélküli személyi hálózat célja tipikusan egy adott felhasználó közvetlen környezetében, néhány méteres távolságon belül levő intelligens eszközök összekötése egy rádiós interfész segítségével. [39]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve azáltal, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD-kártya, merevlemez, MP3- és videólejátszó, mobiltelefon stb.), vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölhetik vagy módosíthatják, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nemcsak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [14]
- **Virtuális magánhálózat (VPN):** Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Wardriving**: Eredetileg a nyílt, vagy gyengén védett WE- titkosítást használó wifi-hálózatok felkutatását jelentette, és GPS-adatokat is rögzítettek a hálózati paraméterekkel egy időben, hogy később adatbázisokban rögzítve az adatokat másokkal is megoszthassák az információkat. Manapság sokszor összemossák a piggybacking fogalmával, pedig a fontos különbség a kettő között, hogy az egyiknél publikus információkat gyűjtünk, a másiknál pedig engedély nélkül csatlakozunk is a hálózathoz, és adatforgalmat bonyolítunk rajta. [10]
- **Webalkalmazás tűzfalak (WAF):** olyan eszközök, melyek webalapú, illetve adatbázis-alapú támadások elleni védelmet nyújtanak azáltal, hogy mind a klienstől érkező, mind a kimenő forgalmat adott szabályok szerint elemzik, és a szabályokra való illeszkedés alapján blokkolják, átengedik, vagy módosítják. [10]

- **XSS:** A rövidítés a cross side scripting kifejezéssel oldható fel. Magyarul oldalakon keresztül végrehajtott közvetett szkripthívás. A támadók célja, hogy egy kártékony szkriptet futtassanak le a célgépen. Létezik perzisztens és nem perzisztens fajtája. Ez utóbbi alkalmával a kártékony kód az URL-be kerül beillesztésre, amely rákattintás esetén lefut és elvégzi a felhasználó által nem kívánt tevékenységet. Az értő szemnek valószínűleg feltűnik, hogy a „script" kifejezést, vagy például a javas scriptre utaló „.js" kifejezés el van bújtatva az URL-ben. Tipikusan phishing-támadásoknál alkalmazható jól. A perzisztens változat során magán a webszerveren helyezik el a szkriptet, amely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor-elhelyezésre például a nem megfelelő beviteli védelemmel ellátott blogoldalak bejegyzései adnak lehetőséget. [22]
- **Wireless evil twin támadás**: A felhasználó számítógépének wifi-beállításai módosulnak úgy, hogy a támadó által üzemeltetett wi-fi-hálózathoz kapcsolódjon. Így minden hálózati kommunikációt rögzíteni képes a támadó, amelyből később bármilyen adatot kinyerhet. [22]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

6.1. A fogalmak forrásjegyzéke

[1] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár*. Forrás: https://www.naih.hu/adatvedelmi-szotar.html (Utolsó letöltés: 2020. 09. 03.)

[3] Muha L. – Krasznay Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem, Budapest.

[4] *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*

[5] Muha L. (2004): Fogalmak és definíciók. In *Az informatikai biztonság kézikönyve.* URL: http://lmuha.hu/defins.html (Utolsó letöltés: 2020. 09. 08.)

[6] Molnár A. (2019): Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[7] Sági G. (2017): Informatikai rendszer támadási folyamata. *Műszaki Katonai Közlöny,* URL: http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (Utolsó letöltés: 2020. 09. 08.)

[8] Tikos A. (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[9] Rédecsi M. – Tóth G.: (2013) *Android*. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (Utolsó letöltés: 2020. 09. 11.)

[10] Arányi G. (2020): Sérülékenységvizsgálatok tapasztalatai a hazai kibertérben. In *Kibertéri fenyegetések.* Dialóg Campus Kiadó, Budapest.

[11] Jerabek Gy. (2020*):* Információbiztonság az önkormányzati szektorban. In *Az Ibtv. gyakorlata.* Dialóg Campus Kiadó, Budapest.

[12] Gyurák G. (2015): *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.

[13] *A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet.*

[14] Haig Zs. – Kovács L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. URL: http://hdl.handle.net/11410/285 (Utolsó letöltés: 2020. 09. 11.)

[15] Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In *Cél-*

zott támadások. Dialóg Campus Kiadó, Budapest.

[16] *A Big Data a hivatalos statisztikában*. 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (Utolsó letöltés: 2020. 09. 08.)

[17] Mátrai J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (Utolsó letöltés: 2020. 09. 08.)

[18] Oroszi E. (2008): *Social Engineering.* Budapesti Corvinus Egyetem, Budapest.

[19] Sági G. (2018): Célzott támadási modellek és műszaki védelem lehetőségek. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[20] Kocsis T. (2020): Történetek a Darknet mélyéről – Adatszivárgási esettanulmányok. In *Kibertéri fenyegetések.* Dialóg Campus Kiadó, Budapest.

[21] Bonnyai T. (2019): Kritikus információs infrastruktúra védelem. In *Kritikus információs infrastruktúrák védelme*. Dialóg Campus Kiadó, Budapest.

[22] Kaczur G. (2018): Spearphishing. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[23] *2003. évi C. törvény. az elektronikus hírközlésről.*

[24] Carabott, E. (2011): *Hacking Motivations – Hactivism*, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (Utolsó letöltés: 2020. 08. 22.)

[25] Solymos Á. (2018): Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[26] Marsi T. (2019): Incidenskezelés kritikus infrastruktúrák esetén. In *Kritikus információs infrastruktúrák védelme.* Dialóg Campus Kiadó, Budapest.

[27] Kóbor Á. (2014): *Mi az a „dolgok internete”?* URL: https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (Utolsó letöltés: 2020. 09. 03.)

[28] Cser O. (2018): Célzott támadás a pénzügyi szektor ellen. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[29] Krasznay Cs. (2012): A polgárok védelme egy kiberkonfliktusban. *Hadmérnök*, 2012/4, URL: http://hadmernok.hu/2012_4_krasznay.pdf (Utolsó letöltés: 2020. 09. 11.)

[30] Resperger I. (2002): Kockázatok, kihívások és fenyegetések a XXI. században. ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.

[31] Tóth K. (2020): Az egészségügyi információs rendszerek információbiztonsága, In *Az Ibtv gyakorlata.* Dialóg Campus Kiadó, Budapest.

[32] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.*

[33] *2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.*

[34] Yaqoob, I. – Ahmed, E. – Imran, M. (2017): *The rise of ransomware and emerging security challenges in the Internet of Things.* Computer Networks, 6 September (2017), URL: https://doi.org/10.1016/j.comnet.2017.09.003 (Utolsó letöltés: 2020. 09. 11.)

[35] Bodó A. – Zámbó N.: A közreműködők kötelezettségei a célzott támadások elhárításában az ibtv. szerint. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[36] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.*

[37] Gyaraki R. (2018): Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban. In *Célzott támadások.* Dialóg Campus Kiadó, Budapest.

[38] Bódi A. (2020): Információbiztonság a közlekedés, mint létfontosságú rendszerelem esetén. In *Az Ibtv. gyakorlata.* Dialóg Campus Kiadó, Budapest.

[39] Haddad, R. (2019): Okoseszközök a kritikus információs infrastruktúrákban. In *Kritikus információs infrastruktúrák védelme*. Dialóg Campus Kiadó, Budapest.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Dorogi Katalin

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-496-2 (PDF)