Bonnyai Tünde – Kiss Adrienn –
Margitics József

Létfontosságú információs rendszerek biztonsága – kihívások különleges jogrend idején

Jelen tanulmány kiindulási alapjául egy olyan szélsőséges helyzet szolgál, amelyre korábban nem volt példa. Olyan szituációt vizsgálunk, amely váratlanul, kényszerből hozott döntések eredményeként, rövid időn belül alakult ki, ugyanakkor egyes szereplők tekintetében hosszú távú következményekkel járhat. 2020 egy különleges év, nemcsak Magyarország, de az egész világ viszonylatában. Meg kellett tenni olyan dolgokat, amelyekre az emberiség ebben a formában nem volt felkészülve. Bizonyos mértékben váratlanul háttérbe szorultak a 21. század már-már klasszikusnak tekintett kihívásai, és szembekerültünk az ismeretlen okozta félelmekkel. A Covid-19 világjárványt okozott, számos társadalmi, politikai, gazdasági, élettani, technológiai és ideológiai következményt is generálva.

A tanulmány szerzőiként arra vállalkoztunk, hogy ebből a számosságból kiemeljünk egy Magyarország tekintetében specifikumként értelmezhető döntéssorozatot, és annak az érintettekre gyakorolt hatásait vizsgáljuk, jogalkotói és jogalkalmazói szemszögből. A magyar kormány különleges jogrendbeli intézkedései okán kiemelt figyelem irányult – elsősorban a védekezés kulcsfontosságú szereplőiként – az úgynevezett létfontosságú vállalatokra annak érdekében, hogy az általuk biztosított szolgáltatások rendelkezésre állása minden körülmények között biztosítható legyen. Ez az intézkedés a megelőzés szemléletének egy rendkívül előremutató megnyilvánulása, ugyanakkor okkal vet fel olyan kérdéseket, amelyek a normál időszaki jogszabályi környezetben foglaltak megvalósíthatóságára irányulnak.

Helyzetkép – 2020

Adott egy szélsőséges időszak, számos akadályozó tényező, ismeretlen körülmény és egy cél: az életben (egészségben) maradás. Hosszasan lehetne fejtegetni és sorolni, hogy tulajdonképpen mitől is függenek a 21. századi ember hétköznapi életkörülményei, mi az az alapvető ellátási igény, amely nélkül nem tud létezni. Úgy tűnik, hogy a 2020-as év megtanítja a modern kor gyermekét arra, ebben bizony vannak korlátok, amelyeken nem feltétlenül tudunk, vagy nem feltétlenül szabad átlépni. Meg kell tenni azonban a biztonságunk megteremtése és fokozása érdekében olyan intézkedéseket, amelyek a korlátok között is a javunkat szolgálják. A járványok azóta léteznek a Földön, amióta az ember, de az orvostudomány fejlődésének köszönhetően az utóbbi évtizedekben nem kellett olyan körülményekkel szembenéznie a fejlett civilizációnak, amelyek felborították volna a rutinszerű hétköznapok folytonosságát. 2020 tavaszán mégis szembesülnünk kellett azzal, hogy az életünket a megszokottól merőben eltérő működési rendre állítsuk át. A biztonság általános

https://doi.org/10.36250/00925_11

értelmezésében minden területen – de a kiberbiztonság kapcsán kiemelten – az egyik legfontosabb cél és követelmény a rendelkezésre állás biztosítása, alternatívák keresése az üzletmenet-folytonosság fenntarthatósága érdekében, minimumszintek megállapítása, helyreállítási képességek kialakítása stb. Átvitt értelemben ez történt (történik) 2020-ban az életvitelszerű körülményeinkkel is.

Jelen tanulmány ennek egy egészen kis szeletét veszi górcső alá hazánk viszonylatában, és olyan érintetti kört vizsgál, amely által néhány régi és jelentős számú új szereplő jelent meg a biztonság egy speciális palettáján. Bevezetésként azonban mindenképpen szükséges néhány gondolat a kiindulási alapokról ahhoz, hogy a későbbiekben az összefüggések, kérdések és válaszok egyértelműen megállapíthatók legyenek. Mielőtt rátértünk a kialakult helyzetet leíró mérföldkövekre, illetve az emiatt létrehozott sajátos halmazra, a létfontosságú vállalatokra, illetve azok elektronikus információs rendszereinek biztonságára, fontos tisztázni a „létfontosságú" szó jelentését, illetve azokat a kapcsolódó normál időszaki kifejezéseket, amelyekre a különleges jogrendben támaszkodott a jogalkotó.

Kijelenthetjük, hogy a magyar terminológiai rendszerben a létfontosságú jelzőt olyan rendszerekre, struktúrákra, szolgáltatásokra használjuk, amelyek a társadalom, a nemzetgazdaság, az államigazgatás működésének fenntartásában nélkülözhetetlen szerepet töltenek be. Nemzetközi viszonylatban ezeket *kritikus infrastruktúraként* azonosítják, a hazai jogszabályok a *létfontosságú rendszerek és rendszerelemek* kifejezést alkalmazzák ugyanerre. Jelentésbeli különbség nincs a két kifejezés között, de a hazai terminológia talán hangsúlyosabban fejezi ki a jelentőségüket. E rendszerek védelme kiemelt fontosságú, biztonságorientált tevékenység, amelynek kereteit a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) határozza meg. Legkifejezőbb példaként az energiaellátás, az egészségügyi ellátórendszer, az ivóvízhálózat, illetve a távközlési szolgáltatások említhetők.

Tanulmányunk másik terminológiai pillérét pedig az úgynevezett *információs infrastruktúrák* adják, amelyek a vizsgált időszakban rendkívül kiemelkedő szerepet töltöttek be, szinte mindenhol a világban. A járvány okozta távolságtartás, a korlátozó intézkedések „bezártak" minket a klasszikusan értelmezett négy fal közé, így a társadalom jelentős százalékának csupán az információs rendszereken (ebben a kontextusban elsősorban informatikai eszközök, okoseszközök, internetszolgáltatás) keresztül volt kapcsolata a külvilággal. A digitális oktatás és a *home office* bevezetése soha nem látott mértékben növelte meg az internetszolgáltatók forgalmát, az ehhez szükséges eszközigényt és ezzel együtt a kiberbiztonsági kockázatokat és fenyegetettséget is, amire egy későbbi fejezetben térünk vissza. Az információs rendszerek okán kapcsolódik szorosan ide a nemzetközi színtéren *kritikus információs infrastruktúrákként* definiált rendszerek halmaza. A magyar jogi környezetben – a vizsgált időszakban – erre vonatkozóan két fogalom is szerepelt, ami kissé nehezítette az értelmezést. A már említett Lrtv. végrehajtási rendelete, a 65/2013. (III. 8.) Korm. rendelet (továbbiakban: Lrtv. vhr.) szerint *létfontosságú*

információs rendszernek és létesítménynek kellett tekinteni „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszereit, eszközeit és módszereit, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek".[1] Ez a megfogalmazás tulajdonképpen azt jelentette, hogy valamennyi fizikai és virtuális létezésű rendszer/eszköz, amely létfontosságú rendszerelemként azért lett kijelölve, mert információt biztosít vagy informatikai rendszerként funkcionál, az egyben létfontosságú információs rendszer/létesítmény is. A fogalom második fele pedig arra utal, hogy szintén létfontosságú információs rendszernek/létesítménynek kell tekinteni az összes olyan fizikai és virtuális elemet, amely egy létfontosságúként kijelölt rendszerelem működésének alapfeltételeül szolgál. Ez a meghatározás a kezdetektől fogva része a kormányrendeletnek, így három hónappal előbb lépett hatályba, mint a magyar kibertér biztonságának szavatolását célzó, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) és az abban foglalt másik definíció, amely ehhez képest szűkebb értelmezést ad. Az Ibtv. értelmező rendelkezései szerint ugyanis *létfontosságú információs rendszerelemnek* csak a kijelölt létfontosságú rendszerek azon elektronikus információs létesítményeit, eszközeit vagy szolgáltatásait tekintjük, amelyek „működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené".[2] Itt szükséges megemlíteni, hogy a jogalkotó a vizsgált időszakban szerzett – és a korábbi évek – tapasztalatai alapján 2020 júliusában számos módosítást eszközölt a vonatkozó jogszabályokban, aminek eredményeként a kettős definíciós háttér megszűnt, így 2020. július 31-étől[3] csak az Ibtv. szerinti értelmezés hatályos.

A további fejezetekben ismertetett körülmények, döntések, intézkedések okán merült fel a kérdés, hogy a különleges jogrendi időszakban létfontosságú vállalatokként kijelölt szereplők – amelyekre a kijelölésük okán vonatkozott valamennyi normál időszaki szabályozásból fakadó kötelezettség – létfontosságú információs rendszerelemei kapcsán milyen formában teljesülhetnek a kiberbiztonság alapvető követelményei.

[1] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 1. § 3. 2020. április 8-i hatály szerint.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 1. § (1) bekezdés 33. 2019. július 27-i hatály szerint.

[3] Az Lrtv. vhr. módosítása értelmében a korábbi 1. § 3. pontban foglaltakat hatályon kívül helyezték, helyükre új rendelkezések kerültek. Lásd 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 1. § 3. 2020. július 31-i hatály szerint.

Világjárvány és annak egyes következményei hazánkban

2019 decemberében a nemzetközi sajtó egyre fokozottabb figyelmet fordított a közép-kínai Hupej tartományban található Vuhan városában észlelt, emberi megbetegedést okozó koronavírus terjedésére. 2019. december 31-én a Vuhan Városi Egészségügyi Bizottság arról számolt be, hogy a koronavírusok családjába tartozó új típusú vírust, Covid-19 *(coronavirus disease)* azonosítottak városukban. 2020. január 10-én az Egészségügyi Világszervezet az esetre reagálva útmutató csomagot adott ki a vírussal kapcsolatban, amelyben minden ország részére tanácsokat fogalmazott meg a Covid-19 betegséget okozó vírus potenciális eseteinek felderítésére, tesztelésére és kezelésére. 2020. január 13-án megerősítették a Thaiföldön azonosított első fertőzést, egy nappal később pedig az Egészségügyi Világszervezet sajtótájékoztatóján elhangzott, hogy előfordulhat a vírus szélesebb körű terjedése. 2020. január 22–23-án az Egészségügyi Világszervezet vezetője egy bizottságot hívott össze annak értékelésére, hogy a kitörés nemzetközileg aggodalomra okot adhat-e.[4]

Mindezek alapján a legtöbb országban megkezdődött valamilyen szinten a potenciális járványra történő felkészülési intézkedések megfogalmazása. Hazánkban másnap jelent meg a 2020. évi 3. számú Hivatalos Értesítő, amelyben figyelemre méltó a honvédelmi miniszter 2/2020. (I. 24.) utasítása. Az ügyeletes minisztériumi felső vezetői feladatok ellátásáról és jelentési kötelezettségi körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről szóló utasításban szerepel, hogy az 1324/2011. (IX. 22.) Korm. határozat szerinti biztonsági ügyelet feladatait a Magyar Honvédség Központi Ügyelete – alapfeladatai ellátása mellett – látja el. Az utasításban a biztonsági kihívást jelentő helyzetekről készülő jelentések megtételével kapcsolatos részletszabályokat dolgozták ki. A Kormányügyelet tájékoztatásának körébe tartozó biztonsági kihívást jelentő helyzetek felsorolását áttekintve pedig számos olyan pont figyelhető meg, amely párhuzamba hozható a Covid-19 veszélyeinek azonosításával, illetve azok kockázatainak tervezett elemzésével és értékelésével, így például:

- a különleges jogrend kihirdetésére okot adó események bekövetkezése;
- a fővárosi, megyei védelmi bizottságok rendkívüli üléseinek összehívását szükségessé tevő események bekövetkezése;
- a honvédelmi célból fokozott védelmet igénylő kritikusinfrastruktúra-elemek közvetlen veszélyeztetettségét vagy károsodását kiváltó események;
- a honvédelmi rendszerre bármilyen hatást gyakorló elemi csapás, ipari szerencsétlenség, illetve más katasztrófa jellegű esemény;
- minden egyéb, a honvédelmi rendszert érintő olyan előre nem látott veszély vagy bekövetkezett esemény, amely a kormányzati kommunikáció szempontjából releváns.[5]

[4] WHO: *Listings of WHO's response to COVID-19* (2020. június 29.).

[5] 2/2020. (I. 24.) HM utasítás az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és jelentési kötelezettségi körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről.

Kijelenthető, hogy a Covid-19 betegséget okozó vírussal kapcsolatos – jelentős – előzetes aggodalmak és a hozzájuk kapcsolódó rendelkezések a hazai jogalkotásban a fent említett honvédelmi miniszteri utasításban figyelhetők meg először.

Egy héttel később, 2020. január 31-én ennél sokkal konkrétabb és célirányosabb intézkedésként megjelent a Kormány 1012/2020. (I. 31.) határozata a Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzs felállításáról. A határozatban a Kormány áttekintette a Kínai Népköztársaság területéről indult koronavírus-járvány kapcsán kialakult helyzetet, és megállapította, hogy Magyarország polgárainak védelme érdekében elengedhetetlen a járványügyi helyzet folyamatos figyelemmel kísérése, a szükség szerinti intézkedések hatékony megszervezése és az állami szervek kapcsolódó tevékenységeinek összehangolása. Az operatív törzs vezetője a belügyminiszter lett, a törzs tevékenységét a média útján már a lakosság is nyomon követhette a kezdetektől.[6] Az elkövetkezendő hetekben a járvány terjedése nemzetközi szinten erősödött. Ennek érdekében számos országban megelőző védelmi és korlátozó intézkedéseket alkalmaztak, majd több állam – így Magyarország is – különleges jogrendet vezetett be.

Hazánkban március elején azonosították az első fertőzöttet, majd fokozatosan növekedni kezdett az azonosított koronavírus-fertőzöttek száma. Magyarország Kormánya 2020. március 11-én az Alaptörvény 53. cikke szerinti felhatalmazás alapján és a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 44. §-ában foglalt „tömeges megbetegedést okozó humánjárvány vagy járványveszély, valamint állatjárvány" veszélye okán *veszélyhelyzet különleges jogrendi tényállást* hirdetett ki.[7] A veszélyhelyzet kihirdetését megelőzően a hazai járványügyi helyzetre csak az egyedi megbetegedések voltak jellemzők. A veszélyhelyzet kihirdetésének egyik leglényegesebb célja a tömeges megbetegedés elkerülése, valamint az egészségügyi képességek és kapacitások megerősítése volt. Fontos hangsúlyozni, hogy a különleges jogrend bevezetése minden esetben az Alaptörvény szerinti felhatalmazással történik, és lehetőséget teremt a kormányzatnak arra, hogy hatékonyabban, célirányosabban és összességében gyorsabban tegyen meg bizonyos intézkedéseket. A kihirdetett veszélyhelyzet olyan jogi eszközrendszer, amely által a mindenkori kormány rendeleti úton szabályoz, a kialakult és várható helyzet kezelésére vonatkozó intézkedésekre költségvetési tartalékokat fordíthat, jogában áll eltérni a normál időszaki eljárásoktól, és akár alapjogokat is felfüggeszthet annak érdekében, hogy az élet- és vagyonbiztonságot szolgáló döntések végrehajtása zökkenőmentes legyen. A veszélyhelyzetben bevezetett első intézkedés a határellenőrzés szigorításához kapcsolódott. A Kormány a veszélyhelyzetben alkotott rendeletei

[6] 1012/2020. (I. 31.) Korm. határozat a Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzs felállításáról (visszavonva 2020. június 17.).

[7] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

hatályának meghosszabbítására vonatkozó felhatalmazás megadására, illetve a védekezés kereteinek meghatározására megalkotta a koronavírus elleni védekezésről szóló 2020. évi XII. törvényt, amely egy újabb szintet biztosított az ekkorra már világjárványszintű helyzet kezelésére.[8]

Mindezzel a Kormány a koronavírus-humánjárványból fakadó következmények elhárítása érdekében sarkalatos törvényben meghatározott rendkívüli intézkedéseket vezetett be, illetve ehhez kapcsolódóan rendeleti úton részletszabályokat alkotott. A veszélyhelyzet ideje alatt az élet és az anyagi javak, valamint a nemzetgazdasági kapacitások védelmének, az alapvető szolgáltatások biztosítása folyamatosságának érdekében a létfontosságú rendszerek és rendszerelemek[9] kategóriájába tartozó szolgáltatások, eszközök, létesítmények, rendszerek, rendszerelemek megóvásával és védelmével kapcsolatos intézkedések különösen nagy hangsúlyt kaptak. Azon szolgáltatások védelmére és folyamatos biztosítására áldoztak kiemelt figyelmet, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, így a járványügyi helyzetben különösen az egészségügyre, a lakosság személy- és vagyonbiztonságára, illetve a gazdasági és szociális közszolgáltatások ellátására.

A járványügyi védekezés sajátosságai – létfontosságú vállalatok

A védekezési intézkedések egyik legfontosabb pillérei a 2020. március 14-én felállított és egy héttel később kiegészített akciócsoportok.[10] Jelen tanulmányban kifejezetten a „Létfontosságú Magyar Vállalatok Biztonságáért Felelős Akciócsoport" (továbbiakban: Akciócsoport) tevékenységével, főként a működése keretében azonosított vállalatok jogszabályi kötelezettségével foglalkozunk.

A honvédelmi miniszter vezetésével létrejött Akciócsoport két fő tevékenységeként határozták meg az ország működéséhez szükséges létfontosságú állami és nem állami gazdasági társaságok azonosítását, illetve a felügyelet esetleges átvételéhez szükséges előkészületek megtételét. A Kormány 1109/2020. (III. 18.)

[8] 2020. évi XII. törvény a koronavírus elleni védekezésről (hatályon kívül helyezve: 2020. 06. 18.).

[9] A vizsgált időszakban hatályos Lrtv. szerint: a meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen 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. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 1. § *f)* pont 2020. január 1-jei hatály szerint.

[10] Oktatási; Mobil Járványkórház Létrehozásáért Felelős; Létfontosságú Magyar Vállalatok Biztonságáért Felelős; Kommunikációs; Rendkívüli Jogrendi Szabályozásért Felelős; Pénzügyi; Gazdasági Újraindítási; Koronavírus Kutató; Határellenőrzési; Önkéntesség Akciócsoport. 1101/2020. (III. 14.) Korm. határozat a koronavírus elleni védekezés kapcsán szükséges további intézkedésekről.

Korm. határozatában az ország működéséhez szükséges létfontosságú állami és nem állami gazdasági társaságok működőképességének fenntartása érdekében létrehozta a honvédelmi irányító törzset. Ennek feladata lett az érintett állami és nem állami gazdasági társaságok, a Kormány, a Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzs és a Létfontosságú Magyar Vállalatok Biztonságáért Felelős Akciócsoport közötti hatékony kommunikáció és együttműködés elősegítése. A kormányhatározat értelmében a honvédelmi törzs tagjait a honvédelmi és a belügyminiszter közösen állapította meg.[11]

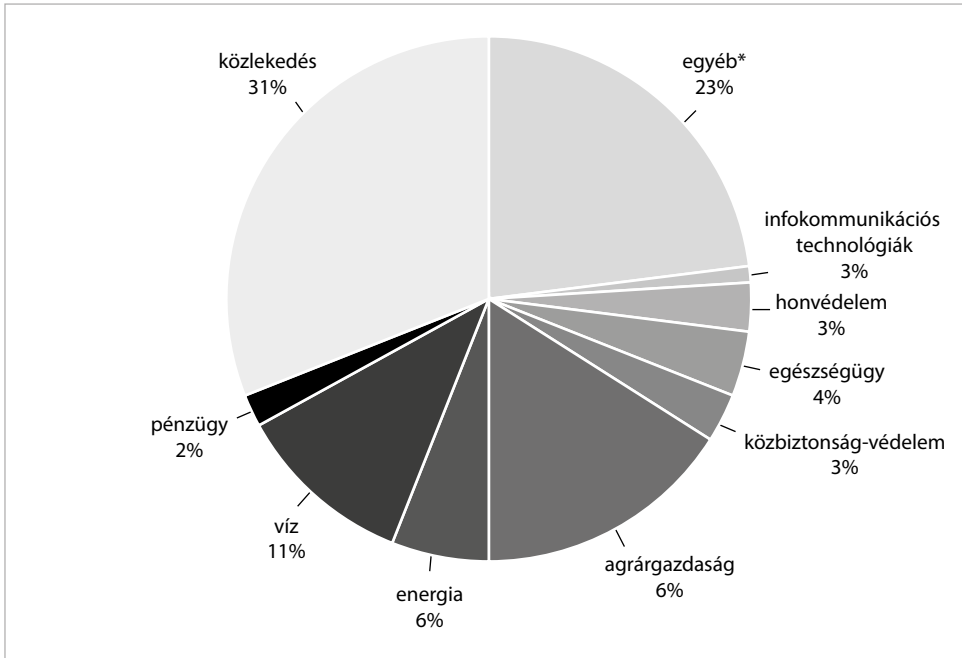
A létfontosságú vállalatok kiválasztásánál nem beszélhetünk véletlenszerűségről, a különböző rendszerek azonosítására önálló – normál időszaki – jogszabályok léteztek. Korábban már említettük, hogy az Lrtv. határozza meg a nemzeti létfontosságú rendszerelemek kijelölésére vonatkozó alapvető szabályokat, illetve az Lrtv. vhr. szabályozza részletesen a lehetséges létfontosságú rendszerelemek azonosítási folyamatát. Ebben az időszakban azonban, amikor kihirdetett veszélyhelyzetben kellett megállapítani, hogy egy adott vállalat létfontosságúnak tekintendő-e, az erre a feladatra létrehozott Akciócsoport és a honvédelmi irányító törzs mérte fel és bírálta el részben hivatalból, részben pedig a vállalatok önkéntes jelentkezéséből kifolyólag a potenciális jelölteket. Mindehhez a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról szóló 86/2020. (IV. 5.) Korm. rendelet adott felhatalmazást és jogi keretet.

A normál időszakban hatályos jogszabályi környezet szerint egy vállalat létfontosságú a nemzet számára, ha az adott szektorba tartozó szolgáltatás leállása veszélyeztetné a gazdaság működőképességét, az emberek ellátását, egészségét vagy életét. Viszont egy létfontosságú vállalatnak nem feltétlenül kritikus minden eleme, ezért fontos pontosan meghatározni azokat az elemeket, amelyek védelemre szorulnak. 2020. március 18-án jelentették be, hogy akár több száz olyan vállalat is van Magyarországon, amely a különleges jogrendben kiemelt figyelmet érdemel és védelmet igényel. Az Akciócsoport első körben 71 vállalatot jelölt ki létfontosságú magyar vállalatként, amelyek pontos listáját a Honvédelmi Minisztérium hozta nyilvánosságra. Végül összesen 142 cég kapta meg a létfontosságú vállalat címkét a vizsgált időszakban, ezek Lrtv. szerinti ágazati megoszlását mutatja az 1. ábra.

A tanulmány szempontjából fontos megjegyezni, hogy a 142 létfontosságú vállalat közül 29 esetében már korábban, a normál időszaki szabályozás szerint kijelölt létfontosságú rendszerelemről beszélünk, így új elemként 113 érintett került a szabályozás alá.

Összességében megállapítható, hogy az Akciócsoport tevékenysége során az Lrtv.-vel összhangban határozta meg a Covid-19 miatt kihirdetett veszélyhelyzet révén létfontosságúvá minősített magyar vállalatok körét.

[11] 1109/2020. (III. 18.) Korm. határozat az ország működéséhez szükséges létfontosságú állami és nem állami gazdasági társaságok veszélyhelyzeti feladatellátásának szakmai támogatásáról.



*Az „egyéb" kategóriába tartozó 23% olyan vállalatok, amelyek az Lrtv. szerinti ágazati besorolásba nem illeszkedtek, de kiemelt jelentőségük indokolta a létfontosságúvá történő kijelölésüket.

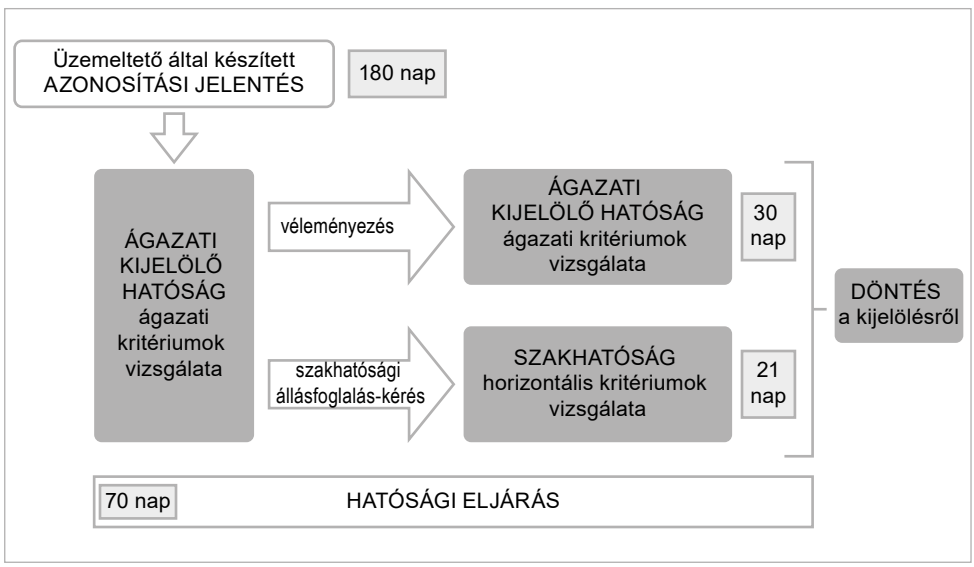
1. ábra Létfontosságú vállalatok aránya az egyes ágazatokban

Forrás: Bonnyai Tünde szerkesztése a Nemzeti Kibervédelmi Intézet adatai alapján

A törekvés, amely szerint az olyan szolgáltatásokat biztosító vállalatokat, amelyek vagy a koronavírus-járványhoz köthető képességeket szolgálnak ki, vagy a lakosság alapvető ellátásával állnak összefüggésben, kormányzati szintű védelem alá kell vonni, rendkívül proaktív, és mind gazdasági, mind társadalmi szempontból felelősségteljes. Ugyanakkor felmerül a kérdés, hogy okozhat-e, és ha igen, akkor mekkora problémát, hogy publikussá tették a Magyarország szempontjából – ilyen speciális helyzetben – létfontosságúnak tekintett létesítmények listáját. Elmondható, hogy a korábbiakban nem volt még hasonló lista, amely e témában tartalmazott volna tételeket, így a veszélyhelyzet ideje alatt nyilvánosságra hozott létfontosságú vállalatokat tartalmazó felsorolás több szempontból fokozott kockázatot hordoz. Nem pusztán azért, mert az ország szempontjából fontosnak tekintendők az adott cégek, és rájuk irányították a figyelmet. Kockázatot jelent önmagában az, hogy a korlátozásokat szükségessé tevő pandémiás időszakban számos cégnél lehetőség volt a távoli munkavégzésre, és mivel a vállalatoknak rendkívül rövid idő alatt kellett átállniuk a megszokottól eltérő munkavégzési környezetre, a legtöbb cég elsősorban az üzletmenetfolytonosságra koncentrált, míg az információbiztonsági kockázatok kiküszöbölése feltételezhetően háttérbe szorult.

A létfontosságú „címke" következményei egy vállalat életében

A vizsgált időszakban hatályos Lrtv.-t alapul véve normál esetben a nemzeti létfontosságú rendszerelemek üzemeltetőinek kijelölési eljárását a törvény mellékleteiben meghatározott ágazatokhoz való tartozás szerint, a vonatkozó ágazati rendeletekben kijelölt illetékes hatóságok hivatalból folytatták le, amelynek keretében az azonosítási jelentésben foglalt ágazati és horizontális kritériumok vizsgálata alapján, a közigazgatási hatósági eljárás szabályainak megfelelően hoztak döntést a kijelölésről. Döntésüket kijelölő határozat formájában közölték az érintettekkel, amelyekben meghatározták az üzemeltetői biztonsági terv kidolgozásának határidejét, illetve a rendszerelem védelmével összefüggő egyéb feltételeket is. Ez az eljárási metódus a törvény szerint legfeljebb 70 napot vett igénybe. A folyamatot a 2. ábra szemlélteti.

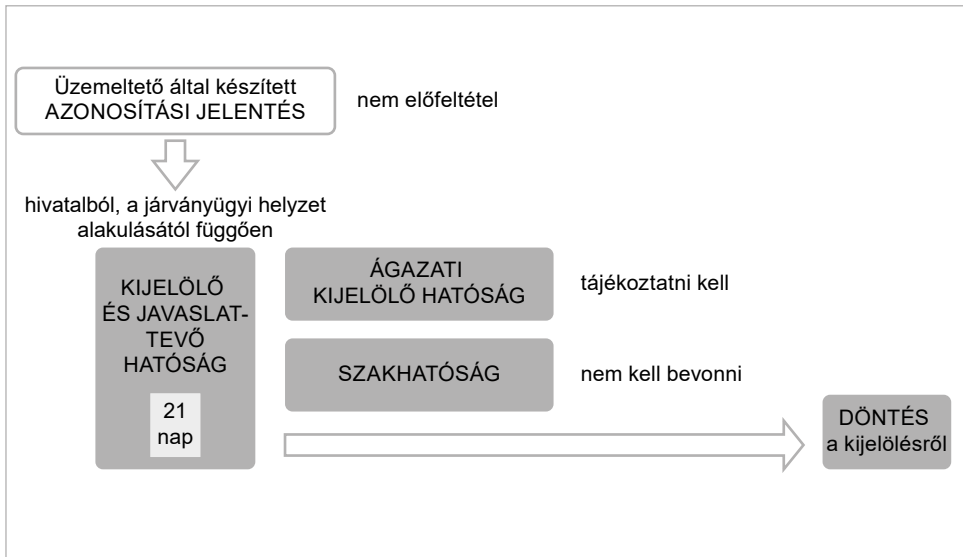


2. ábra Létfontosságú kijelölés normál időszakban
Forrás: Bonnyai Tünde szerkesztése a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról; 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről alapján (2020. július 1-je előtti hatály szerint)

A veszélyhelyzet időszakában jellemző sajátos körülmények okán sokkal gyorsabb döntéshozatali mechanizmusok váltak szükségessé, az eljárások ezért a 86/2020. (IV. 5.) Korm. rendelet 4. § (1) bekezdésének[12] alkalmazásával indulhattak meg,

[12] „A veszélyhelyzet ideje alatt a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény és a végrehajtására kiadott rendeletek tekintetében a honvédelmi

lefolytatásukért a honvédelmi miniszter felelt, a döntés meghozatalára pedig – azonosítási jelentés, így ágazati és horizontális kritériumvizsgálat nélkül – összesen két nap állt rendelkezésre.[13] Az eljárást a 3. ábra szemlélteti.



3. ábra Létfontosságú kijelölés veszélyhelyzet idején

Forrás: Bonnyai Tünde szerkesztése a 86/2020. (IV. 5.) Korm. rendelet a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról (hatályon kívül helyezve: 2020. június 18.) alapján

Arra azonban sem a normál időszaki, sem a különleges jogrendi szabályozás nem tért ki, hogy pandémiás időszak miatt létfontosságúvá kijelölt vállalatok a veszélyhelyzet megszűnését követően milyen „minőségükben" működnek majd tovább.

A kötelezettségek jellege, illetve teljesítésük keretrendszere viszont semmiben nem változott; az ily módon kijelölt nemzeti létfontosságú rendszerelemeknek értelemszerűen ugyanúgy meg kellett felelniük az előírásoknak, mintha normál időszakban jelölték volna ki őket. Ez azt jelentette, hogy a kijelölt létfontosságú vállalatok azzal szembesültek, hogy a kialakult – fokozódó járványügyi – helyzetben betöltött különleges szerepük mellett a kijelölő határozatukban definiált kötelezettségeket is a megadott határidőkön belül teljesíteniük kell. E fejezetrészben azokat az előírásokat és kötelezettségeket mutatjuk be, amelyek az érintett vállalatok egészét általánosságban érintették, mindezt a vizsgált időszakban hatályos jogszabályi állapot szerint.

miniszter a kijelölő hatóság." 86/2020. (IV. 5.) Korm. rendelet a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról 4. § (1) bekezdés *b)* pont.

[13] 86/2020. (IV. 5.) Korm. rendelet a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról 4. § (5) bekezdés.

Az Lrtv. alapján kijelölt létfontosságú rendszerek biztonságának szavatolhatósága érdekében rendkívül fontos kötelezettségek előírása volt szükséges a jogszabályi háttér megalkotásakor, ami az elmúlt évek tapasztalatai folytán a legtöbb esetben tovább szigorodott. Azon túl, hogy az Lrtv. megállapítja minden létfontosságú rendszert üzemeltető számára a biztonsági összekötő személy kinevezését és az üzemeltetői biztonsági terv elkészítését,[14] az Ibtv. további elvárásokat támaszt feléjük. Egyrészt biztosítani kell a kijelölt rendszerelem létfontosságú információs rendszerelemei tekintetében a bizalmasság, sértetlenség, rendelkezésre állás hármas követelményrendszerét, amely az érintett rendszerek zárt, teljes körű, folytonos és kockázatokkal arányos védelmét feltételezi. Mindennek érdekében a kijelölt üzemeltetőknek relatíve rövid időn, 60 napon belül alkalmazniuk kell egy – speciális végzettséggel rendelkező – információs rendszerek biztonságának felügyeletéért felelős személyt, és 90 napon belül készíteniük kell egy informatikai biztonsági szabályzatot.[15] Másrészt a kijelöléstől számított egy éven belül el kell készíteniük rendszereik biztonsági osztályba és szervezetük biztonsági szintbe sorolását.[16]

A különleges jogrend fennállásának ideiglenessége okán[17] – a határidőkből kiindulva – ki kell emelni ezek közül a személyügyi és a dokumentumok készítésére vonatkozó kötelezettséget.

Az üzemeltetői biztonsági terv és az informatikai biztonsági szabályzat tartalmi elemeit figyelembe véve a dokumentumok összeállítása komplex és speciális szaktudást igénylő feladat, elkészítésük – az eddigi normál időszaki tapasztalatok alapján – akár jelentős költségekkel is járhat. Az üzemeltetői biztonsági terv kötelező tartalmi elemeit az Lrtv. vhr. vonatkozó melléklete[18] konkrétan fel is sorolja, ez jól példázza készítésének átfogó jellegét. A tervet ugyanis – a teljesség igénye nélkül – az alábbi részletekbe menő információhalmazként kell értelmezni:

- szervezet, tevékenység, irányítási rendszer bemutatása (szervezeti struktúra és az üzemvezetés, személyzet, elvárt/normális működési paraméterek);
- kijelölt rendszerelem azonosítása és értékelése adott ágazati és horizontális kritériumok alapján;

[14] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 6. § (7) és 6. § (1) bekezdés. 2020. január 1-jei hatály szerint.

[15] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 11. § (1) bekezdés *c)* és *f)* pont, illetve 26. § (6) bekezdés *c)* pont. 2019. július 27-i hatály szerint.

[16] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 7. §, illetve 26. § (6) bekezdés *c)* pont. 2019. július 27-i hatály szerint.

[17] Magyarországon eddig a vörösiszap-katasztrófa miatt volt kihirdetve a leghosszabb időtartamú veszélyhelyzet, de az sem haladta meg a 270 napot, így okkal lehetett számolni azzal, hogy a kiváltó okok enyhülésével a járvány miatti veszélyhelyzet meg fog szűnni.

[18] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról 2. melléklet. 2020. április 8-i hatály szerint.

- környezeti sajátosságok (működést biztosító közműszolgáltatások és egyéb szolgáltatók, a kijelölt rendszerelem környezetében található és a működésére befolyással bíró veszélyes üzemek, gyárak, erőművek);
- belső audit és vezetőségi átvizsgálás rendszere;
- a kijelölt rendszerelem bemutatása (felépítés, tevékenységek, folyamatleírások, informatikai rendszerek, tájékoztatási rendszerek, felügyeleti szervek).

Ezen felül a terv kiemelkedően fontos része – és a fentiek alapján azok mélyreható ismerete függvényében – a működéssel összefüggő kockázatok azonosítása és értékelése, felvázolva a kockázati listát, a kijelölt rendszerelem interdependens kapcsolódásait és az azokból adódó kockázatok azonosítását. Ez alapján az üzemeltetőnek a feltárt kockázatok kezelésére vonatkozó szabványokat, eljárásokat, intézkedéseket is be kell mutatnia. A felsorolást áttekintve meg kell állapítani, hogy kimondottan nehéz például olyan ágazati és horizontális kritériumokat értékelni, amelyeket azonosítási jelentés hiányában a kijelölés során eleve nem vizsgáltak. Az 1. ábrán vázolt ágazati megoszlás alapján pedig különösen nagy kihívást jelenthet az egyéb kategóriába sorolt létesítmények ágazati kritériumainak értékelése, ugyanis azok nem sorolhatók az Lrtv. szerinti ágazatok közé, így ágazati kormányrendeleti szabályozással nem rendelkeznek. Ebből adódóan ágazati kritériumrendszerük sincs, ami az üzemeltetői biztonsági tervben vizsgálható lenne.

A vállalatok üzemeltetőinek gondoskodniuk kell továbbá a biztonsági összekötő személy (továbbiakban: SLO),[19] illetve az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: EIR-felelős) foglalkoztatásáról is. Mindkettő csak büntetlen előéletű lehet, az SLO-nak az Lrtv. vhr.-ben foglalt és az adott ágazati kormányrendeletnek megfelelő szakirányú végzettséggel, míg az EIR-felelősnek a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel kell rendelkeznie. A veszélyhelyzet alatt kijelölt létfontosságú vállalatoknak e személyzeti kérdések komoly kihívásokat jelenthettek, akár saját humán erőforrásból próbálták megoldani, akár új munkaerő alkalmazásával szándékoztak eleget tenni a követelménynek. Mindkét esetben fennáll a lehetősége annak, hogy a vállalat részéről az alkalmazás többletköltséggel jár. Fontos hangsúlyozni ehhez kapcsolódóan, hogy az Lrtv. kijelenti:[20] a kijelölt vállalatokat terhelik az üzemeltetői biztonsági terv elkészítésének, módosításának, a biztonsági összekötő személy foglalkoztatásának költségei.

A körülmények vizsgálatához hozzátartozik az is, hogy mind az Lrtv., mind az Ibtv. lehetővé teszi az illetékes hatóságok számára, hogy a törvények személyi hatálya alá tartozó szervezetek mulasztása esetén szankciókat alkalmazzon – ezek konkrét bírságok formájában is materializálódhatnak, amennyiben a hatóságok

[19] A rövidítés a biztonsági összekötő személy angol terminológiájából ered: *security liaison officer.*

[20] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 7. §. 2020. január 1-jei hatály szerint.

azt indokoltnak találják. Figyelemmel arra, hogy nem egészen 100 napon keresztül állt fenn kihirdetett veszélyhelyzet hazánkban, a hatóságoknak ebben az időszakban nyilvánvalóan nem volt alkalmuk élni a bírságtételek alkalmazásának lehetőségével.

Fenyegetések a kibertérben, a koronavírussal összefüggésben

Az éremnek mindig két oldala van; ez jellemzi az eddigiekben bemutatott helyzetet is. A pandémia ugyanis nemcsak sajátos védekezési szabályokat és intézkedéseket – így a létfontosságú vállalatok feltérképezését – tett szükségessé, hanem olyan kihívásokkal is szembeállított bennünket, amelyek a kibertérben jelentkeztek.

Világszinten elmondható, hogy a járvány felerősödése után a NATO által is hadszíntérként értelmezett kibertérben egyre gyakrabban jelentek meg kifejezetten a koronavírussal kapcsolatos, arra hivatkozó különböző típusú támadások. Ezek a kezdetekben az emberek félelmére, a fennálló új helyzetre és a szervezetlenségre alapozva vették célba az embereket, majd az idő múlásával megfigyelhető volt, hogy egyes szervezetek/szervezettípusok is célponttá váltak.

Az Interpol szerinti legjellemzőbb kiberfenyegetéseket a 4. ábra mutatja be. A koronavírus-járvány kezdete óta a legnagyobb gyakorisággal az online csalások,[21] a kártékony programok,[22] az adatgyűjtésre szánt kártevő programok,[23] a rosszindulatú domainek,[24] a félretájékoztatást megcélzó támadási formák,[25] illetve az adathalász-tevékenységek[26] fordultak elő.

Európában főként a rosszindulatú domainek, az adathalászat, a kritikus infrastruktúrákat célzó kártékony programok, illetve az adatgyűjtésre szánt kártevő programok voltak a „legnépszerűbbek". Az említett káros programok egy kritikus információs infrastruktúrával rendelkező vállalatnak és az ezzel közvetetten érintett külső környezetnek akár nagyobb problémákat, sérüléseket is okozhatnak a megfelelő odafigyelés és felkészülés hiányában.

[21] A Covid-19-re hivatkozva vagy ezt a jelenséget megemlítve haszonszerzési céllal tévesztettek meg embereket.

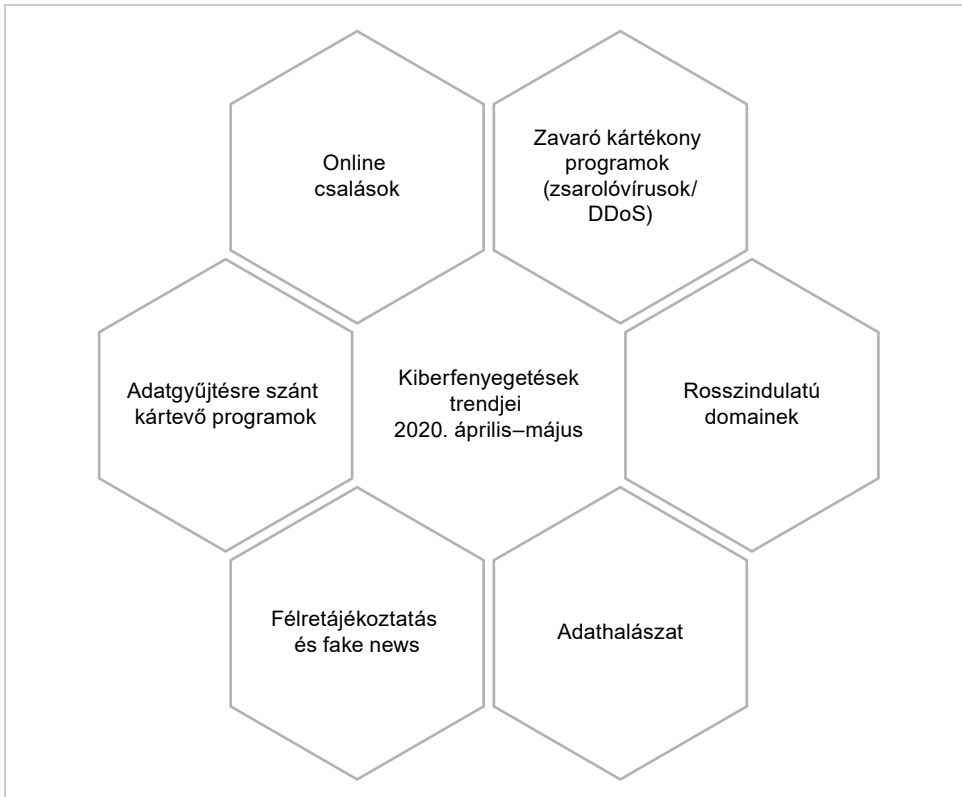
[22] Rosszindulatú programok, amelyek főleg a kritikus infrastruktúrák ellen irányultak, és az üzleti tevékenységek leállását, működésük kiesését okozták.

[23] Különböző távoli elérésű programok, mint például trójai vagy egyéb kémprogramok, amelyeket információk, adatok kicsalásának céljából alkalmaztak.

[24] A koronavírushoz kapcsolódó kulcsszavakkal létrehozott domainnevek: adatok, pénz és egyéb értékek ellopásának célzatával létrehozott oldalak.

[25] Bizonytalanságot és bizonyos szintű káoszt képes elindítani egy támadás, amely direkt módon félrevezető.

[26] Támadó e-mailek vagy adott platformok, amelyek a koronavírus jelenségét adott szövegkörnyezetben alkalmazva csaltak ki az emberekből személyes adatokat.



4. ábra Kiberfenyegetések trendje
Forrás: Kiss Adrienn szerkesztése Interpol: Cybercrime: Interpol report shows alarming rate of cyberattacks during COVID–19. *Interpol,* 2020. augusztus 4. alapján

Kimondottan hazai viszonylatban például arra hívta fel a figyelmet a Nemzetbiztonsági Szakszolgálat égisze alatt működő Nemzeti Kibervédelmi Intézet, hogy a nyitott RDP-portok[27] rendkívüli sérülékenységre adnak okot. A nemzeti CSIRT *(Computer Security Incident Response Team)*[28] kimutatásai szerint már 2020 első negyedévében megfigyelhető volt az internet irányából szabadon elérhető RDP-portok számának látványos emelkedése. Az erőteljes növekedés egyik fő oka lehetett, hogy a járványügyi helyzet súlyosbodásával egyre több szervezet biztosított otthoni munkavégzési lehetőséget a dolgozók számára, amelyet azonban a bevezetésre rendelkezésre álló időkeret

[27] A Microsoft által fejlesztett olyan protokoll, amely grafikus felületet biztosít a felhasználóknak és az adminisztrátoroknak annak érdekében, hogy hálózati kapcsolaton keresztül csatlakozzanak egy másik számítógéphez. Alapesetben a TCP3389 porton üzemel, és a biztonsági kockázatok lehető legalacsonyabb szintre csökkentése érdekében megfelelően kell konfigurálni.
[28] Magyarország nemzeti szintű eseménykezelési feladatokat ellátó szerve, a nemzeti CSIRT a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet szervezeti keretei között működik.

szűkössége miatt nem minden esetben sikerült kellően biztonságosan beállítani.[29] Egy szervezet szempontjából a nem kellő körültekintéssel konfigurált RDP-elérés olyan biztonsági kockázatokat hordoz, amelyek révén akár a szervezet teljes működése is megbénítható. A napi szintű feladatellátás ellehetetlenítése pedig – például egy létfontosságúként megjelölt vállalat esetében – súlyos szolgáltatáskieséssel is járhat. Emellett Magyarországon is előfordult olyan káros csatolmányokat terjesztő kampány júniusban, amely a Nemzeti Népegészségügyi Központ, illetve Müller Cecília országos tisztifőorvos asszony nevében küldött levelekkel egy űrlap letöltésére próbálta rávenni a levél címzettjét,[30] de adathalász – személyes és bankkártyaadatok megadására kérő – kampány is zajlott, szintén a Nemzeti Népegészségügyi Központ arculati elemeit felhasználó e-mailek formájában.[31]

Ezek alapján a létfontosságú vállalatokként nevesített szervezeteknek a jogszabályi kötelezettségeken túl számolniuk kellett azzal is, hogy a működésükben bármikor bekövetkezhet valamilyen formában biztonsági incidens. Ahogy már említettük, emiatt kimondottan aggályos, hogy teljes publicitást kapott az Akciócsoport által vizsgált cégek listája.

A támadások fajtájából azt a következtetést vonhatjuk le, hogy a legtöbb esetben az üzemeltetők és az adott munkavállalók információbiztonsági tudatosságával relatíve könnyen ki lehetett védeni az efféle ártó szándékú cselekmények következményeit, de joggal merülhet fel a kérdés, hogy a korábban az Ibtv. hatálya alá nem tartozó, kiberbiztonsággal kapcsolatos követelményekkel nem szembesülő, a rendszerbe „frissen" bekerülő cégek esetében milyen mértékű és hatékonyságú tudatosságról, védekezőképességről beszélhetünk.

Létfontosságú vállalatok – hatósági felügyelet és eseménykezelés

A létfontosságú rendszerek védelmével kapcsolatos feladatkör rendkívül összetett a normál időszaki szabályozás szerint is. Számos felelős hatóság közös munkájának eredménye, hogy a kijelölt elemek megfeleljenek a jogszabályi előírásoknak. Ezt a rendszertant tovább bonyolította a veszélyhelyzeti intézkedésekkel bevezetett, korábban már említett, központosított döntéshozatali eljárás, amely a létfontosságú vállalatok kijelölését a honvédelmi miniszterhez telepítette. Az eljárás – a célnak megfelelően – egyszerűsödött, ugyanakkor a szakmai szempontok érvényesítésére már nem maradt lehetőség, mivel az ágazati kijelölő hatóságok – a szakmai kritériumok vizsgálatának letéteményesei – nem vettek részt a kijelölésekben.

[29] Nemzeti Kibervédelmi Intézet: Riasztás: nyitott RDP port biztonsági kockázatai.

[30] Nemzeti Kibervédelmi Intézet: Riasztás a Nemzeti Népegészségügyi Központ nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban.

[31] Nemzeti Kibervédelmi Intézet: Riasztás a Nemzeti Népegészségügyi Központ arculati elemeit felhasználó adathalász levelekkel kapcsolatban.

Tekintettel arra, hogy az ideiglenesen bevezetett szabályok nem tértek ki arra, hogy a veszélyhelyzet visszavonását követően milyen módon kívánja a jogalkotó „visszaállítani a normál időszaki állapotot", számos joghézag alakult ki. Egyrészt nem volt egyértelmű, hogy ki gyakorol szakmai felügyeletet a kijelölt elem felett, különösen azok esetében, amelyek az Lrtv. szerinti ágazatokba nem voltak besorolhatók. Másrészt felmerült a kérdés, hogy a különleges jogrendi szabályok közé bekerült – szintén a honvédelmi miniszter felelősségi körébe delegált – ellenőrzést koordináló szervi tevékenységet miként kell értelmezni a jelenben és hosszú távon, főleg azért, mert ezt előre elkészített, éves terv alapján, valamennyi érintett hatóság bevonásával kell végezni. Harmadrészt semmilyen rendelkezés nem tisztázta, hogy a veszélyhelyzet idején kijelölt létfontosságú rendszerelemek megkapják-e az úgynevezett „honvédelmi" jelzőt, ez ugyanis alapjaiban befolyásolja az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság, illetve az eseménykezelő szerv kilétét.[32] A normál időszaki és a veszélyhelyzet időszakában feladat- és hatáskörrel rendelkező szereplőket az 1. táblázat foglalja össze.

A különleges jogrendi szabályozás kialakításakor – feltételezhetően – az volt a kiindulási alap, hogy egyedül a honvédelmi ágazat (normál időszaki) szabályozásában ismerünk olyan kijelölési megoldást, amely szerint honvédelmi érdekből egy másik ágazatban található rendszerelem is kijelölhető létfontosságúnak. Ennek lefolytatása korábban az érintett ágazat kijelölő hatóságának a felelőssége volt, a kijelölésre a honvédelmi ágazati kijelölő hatóság „csupán" javaslatot tehetett. Az Lrtv. 2020. január 1-jén hatályba lépett módosításával mindezt törvényi szintre emelte a jogalkotó, és a honvédelmi ágazat kijelölő hatóságának kizárólagosságával lehetővé tette, hogy a honvédelmi ágazat kijelölő hatósága más, „nem honvédelmi ágazatba tartozó rendszerelemet – az érintett ágazati kijelölő hatóság véleményének bekérését követően – honvédelmi érdekből, kormányrendeletben meghatározott honvédelmi kritériumok alapján nemzeti létfontosságú rendszerelemmé kijelölhet".[33]

[32] A honvédelmi létfontosságú rendszerelemek vonatkozásában külön nyilvántartó hatóság és ellenőrzést koordináló szerv működik a Honvédelmi Minisztériumban a 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről 3. § (1) bekezdésének megfelelően. A honvédelmi célú elektronikus információs rendszerek hatósági felügyeletét a 187/2015. (VII. 15.) 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 24. § (1) bekezdése szerint, míg eseménykezelési feladatait a 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 szóló 6. § (1) bekezdése alapján a Katonai Nemzetbiztonsági Szolgálat látja el.

[33] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 2. § (5) bekezdés. 2020. január 1-jei hatály szerint.

1. táblázat Feladat- és hatáskörök megoszlása

	Normál időszak*		Járványügyi veszélyhelyzet**	
Funkció	**Felelős szerv**	**Feladat**	**Normál időszaki felelős szerv feladata**	**Veszély-helyzetben eljáró szerv**
Ágazati kijelölő hatóság	Ágazati kormány-rendeletben nevesített szerv	Szakmai felelősség a kijelölés során, szakmai felügyelet a működés kapcsán	Kijelölés megindításáról és a kijelölő döntésről tájékoztatást kap	Honvédelmi miniszter
Ágazati javaslattevő hatóság	Ágazati kormány-rendeletben nevesített szerv	Szakmai felelősség a kijelölés során	–	Honvédelmi miniszter
Nyilvántartó hatóság	BM Országos Katasztrófavédelmi Főigazgatóság	Kijelölt – nem honvédelmi – létfontosságú rendszerelemek adatainak nyilvántartása	Kijelölő döntésről tájékoztatást kap	Honvédelmi miniszter
Ellenőrzést koordináló szerv	BM Országos Katasztrófavédelmi Főigazgatóság	Kijelölt – nem honvédelmi – létfontosságú rendszerelemek koordinált ellenőrzése	–	Honvédelmi miniszter
Elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság	BM Országos Katasztrófavédelmi Főigazgatóság	Kijelölt – nem honvédelmi – létfontosságú rendszer-elemek esetében az információbiztonsági követelmények teljesülésének ellenőrzése	Információbiztonsági követelmények teljesülésének ellenőrzése	(BM Országos Katasztrófavédelmi Főigazgatóság)
Eseménykezelő szerv	NBSZ Nemzeti Kibervédelmi Intézet	Kijelölt – nem honvédelmi – létfontosságú rendszer-elemek esetében a biztonsági incidensek kezelése	Biztonsági incidensek kezelése	(NBSZ Nemzeti Kibervédelmi Intézet)

Forrás: Bonnyai Tünde szerkesztése a releváns jogszabályok 2020. július 1-je előtti hatálya alapján

Ez a gondolatmenet a veszélyhelyzetben meghozandó gyors, hatékony és célorientált döntések érdekében megfelelő alapnak bizonyul, ugyanakkor számos részletszabály viszonylatában további jogalkotási tevékenységre lett volna szükség. Tisztázni kellett volna a kijelöléssel járó kötelezettségek listáját és azok

időbeliségét, illetve a számos kivételszabállyal tarkított rendszerben felelős hatóságok és szervek körét egyaránt. A normál időszaki szabályozásban eleve érzékelhető egy joghézag a honvédelmi célú elektronikus információs rendszerek tekintetében. A honvédelmi ágazat által kijelölt ágazaton kívüli létfontosságú rendszerelemekről ugyanis nem derül ki, hogy a működésüket biztosító elektronikus információs rendszerek honvédelmi célúak-e, vagy sem. Ez ismét hatásköri vitákat eredményezhet.

Meg kell állapítani, hogy okkal merült fel a kérdés: ki és milyen felhatalmazás alapján, milyen hatáskörrel lett volna felelős egy kiberbiztonsági incidens kapcsán a vizsgált időszakban.

Tapasztalatok és következtetések

A tanulmány bevezetőjében is határozottan utaltunk arra, hogy a vizsgált időszak rendkívül sok szempontból unikális és gyors döntés meghozatalát tette szükségessé. Szélsőséges helyzet alakult ki, amelyben az élet- és egészségvédelmi intézkedések elsődlegessége megkérdőjelezhetetlen. A világszerte elterjedt járvány minden nemzetet olyan korlátozásokra ösztökélt, amelyekre eddig, ebben a formában nem volt példa. Nem volt tehát *best practice,* nem voltak bevett eljárások, nem volt „nagykönyvben megírt" módszertan. Egy közös cél volt: garantálni a lakosság élet- és vagyonbiztonságát, alapvető ellátását és a nemzetgazdaság működését.

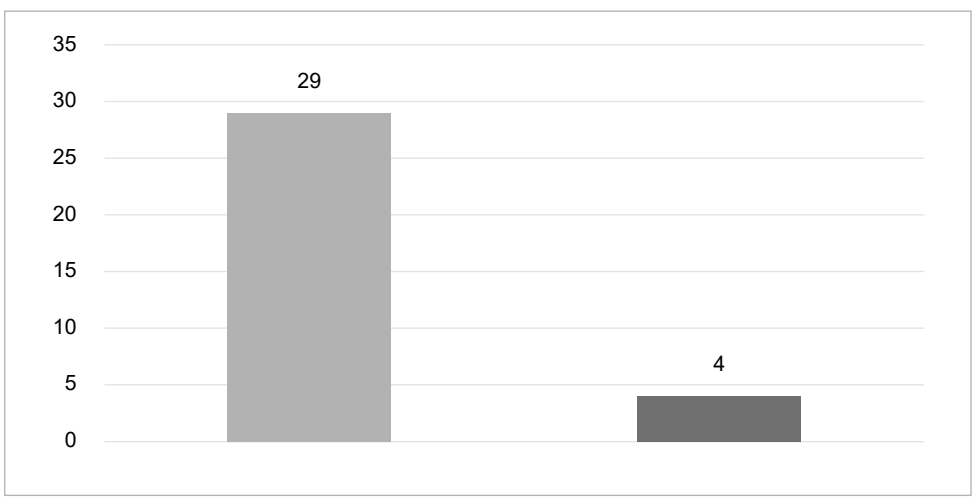
E sajátos körülmények között született meg az úgynevezett létfontosságú vállalatok egyedi halmaza, az előbbiekben ismertetett metódus eredményeként. Ennek során 142 vállalat napi rutinja íródott felül bizonyos szempontok mentén azzal, hogy váratlanul egyfajta állami felügyelet alá kerültek. A kiválasztott vállalatok üzletmenet-folytonosságának garantálhatósága érdekében nemcsak a kijelölésekről, hanem a legfelsőbb szintű vezetés támogatásáról is gondoskodott a már említett honvédelmi irányító törzs. Az országos operatív törzsnek közvetlenül jelentő irányító törzs felügyelete alatt tevékenykedtek az úgynevezett honvédelmi irányítócsoportok, amelyek nyomon követték és koordinálták a vállalati munkát. Az irányítócsoportok kirendelésének fő célja a fizikai biztonság szavatolása és a működőképesség feltételeinek biztosítása volt.[34]

A bemutatott következmények alapján azonban több kérdés is felmerült, nemcsak a veszélyhelyzeti működés kapcsán, hanem az azt követő, újbóli normál időszaki üzletmenet tekintetében is. A váratlanul kialakított döntéshozatali mechanizmus ugyanis lehetővé tette a létfontosságú vállalatok – a körülmények okán nagyon is szükséges – gyors kijelölését, ugyanakkor rendkívül erőteljesen

[34] Honvédelem.hu/MTI: Benkő Tibor: csütörtök reggel jelennek meg az érintett vállalatoknál a honvédelmi irányító csoportok. *Honvedelem.hu,* 2020. március 18.

háttérbe szorította a szakmai szempontokat. A szabályozási környezet és így az érintettek akkor még egyáltalán nem voltak felkészülve egy ilyen markáns módszertanváltásra. A korábbi évek során kialakított és jól bejáratott mechanizmusok, a normál időszakban illetékes hatóságoknál rendelkezésre álló tapasztalat figyelmen kívül hagyása összességében kevésbé hatékony eredményt hozott. A Kormány javaslatára az Országgyűlés 2020. június 20-án megszüntette a veszélyhelyzetet, így a különleges jogrendi időszakban hozott intézkedések felülvizsgálatát meg kellett kezdeni. A vonatkozó kormányrendelet értelmében az Akciócsoport (a jogszabály szövege szerint a honvédelmi miniszter mint kijelölő hatóság) 60 napot kapott arra, hogy a létfontosságú vállalatok körét – az ágazatilag illetékes kijelölő hatóság bevonásával – megvizsgálja, és megállapítsa, mely cégek esetében szükséges a létfontosságúvá történt kijelölés fenntartása.[35]

A 142 vállalat közül 101 esetében – vagyis több mint 70%-ban – visszavonták a kijelölést, de ezek közül 21 továbbra is létfontosságú rendszerelemként működik, figyelemmel a normál időszakban korábban megtörtént ágazati kijelölésére. Ez alapján 80 olyan szervezet van, amely megkezdte a jogszabályi követelményeknek történő megfelelést, de a kijelölés visszavonása által annak teljesítésére már nem kötelezett. Ideiglenes kijelölésük által lényegében átlagosan 94 napig tartoztak a törvény hatálya alá. Az újonnan létfontosságúként kijelölt 113 elem közül végül 33 esetében tartották fenn a kijelölést, az 5. ábrán látható ágazati megoszlás szerint.



5. ábra Tartósan létfontosságúvá kijelölt vállalatok ágazati megoszlása
Forrás: Bonnyai Tünde szerkesztése a Nemzeti Kibervédelmi Intézet adatai alapján

[35] 86/2020. (IV. 5.) Korm. rendelet a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról 8. § (2) bekezdés.

Ahogy már említettük, a veszélyhelyzet időszakában történt kijelölések kapcsán az ideiglenességnek a kezdetektől fogva egyértelműnek kellett lennie. Ha ezt párhuzamba állítjuk a létfontosságú rendszerek védelmének alapvető célkitűzésével – amely szerint szakmai alapokon nyugvó, társadalmi szükségleteket kiszolgáló, illetve gazdasági érdekeket is figyelembe vevő szempontok alapján történik a mindennapi életünk fenntartásához szükséges szolgáltatásokat nyújtó szereplők azonosítása, kijelölése, majd védelme –, akkor jogosan kérdezhetjük, hogy ez a célkitűzés milyen módon érvényesíthető a veszélyhelyzeti kijelölések tekintetében, akár fenntartott, akár visszavont kijelölésről beszélünk.

Szintén fontos körülmény, hogy a veszélyhelyzet időszakában olyan hatósági feladatot kapott a honvédelmi miniszter által irányított Akciócsoport, amelynek ellátásához egy alapvetően szűk ügyfélkörrel, illetve relatíve kis tapasztalattal rendelkező szervezeti egység (Honvédelmi Minisztérium illetékes főosztálya) tudott támogatást nyújtani. Mindehhez hozzátartozik az a nem elhanyagolható tényező is, hogy a 142 vállalat között számos meghatározó piaci szereplőt is találunk, amelyek vezetése kevésbé szokott a klasszikus államigazgatási és különösen a honvédelmi típusú irányítási módszerekhez. Érdemes lenne figyelembe venni a jövőben, hogy a normál időszakban felelősséggel bíró hatóságok az elmúlt években jelentős tapasztalatot szereztek a kijelölt elemekkel történő kapcsolattartás terén is – különösen a „civil cégek" kapcsán. Ez a tapasztalat azt mutatja, hogy ehhez az ügyfélkörhöz merőben más megközelítést, mentalitást és módszereket kell alkalmazni úgy, hogy a jogkövető magatartásra való hajlandóság értelemszerűen ne csorbuljon. A veszélyhelyzet – jellegéből adódóan – természetesen egészen más irányítási/vezetési körülményeket teremtett, amelyeknek minden érintett eleget kívánt tenni, de mindezek alapján célszerű lenne megvizsgálni és megfontolni a most szerzett tapasztalatok és a meglévő tudás ötvözeteként, hogy a létfontosságú rendszerek biztonságának szavatolásáért felelős struktúrában – jogrendtől függetlenül – kiemelt szerepet kapjon a kapcsolattartás és bizalomépítés. Ehhez alapvetően a jogi keretek között is alkalmazható rugalmasság, partnerség, támogató és fejlesztő mentalitás szükséges.

A kijelölések tekintetében – ügyféloldalról – pedig jogosan merül fel a kérdés, hogy azok a cégek, amelyek megkezdték a kötelezettségek teljesítését a jogszabályoknak való megfelelés érdekében, de kijelölésük visszavonásával már nem vonatkoznak rájuk a jogszabályok, mihez kezdjenek a „félbemaradt" megoldásaikkal. Hasznos lehet-e számukra az elmúlt hónapokban szerezett vállalati tapasztalat például egy saját üzletmenet-folytonossági terv készítése vagy egy hasonló élethelyzetre történő felkészülésre irányuló belső folyamat kialakítása során? Az viszont nyilvánvalóvá válhatott számukra, hogy a kártékony programok nagyobb számú megjelenésével, a veszélyhelyzet idején szerzett tapasztalatok alapján a létfontosságú vállalatok üzemeltetőinek láthatóan nagy a felelőssége olyan tekintetben, hogy folyamatos kockázatelemzést végezzenek, és a munkavállalókat időről időre információbiztonsági tudatosítás keretében oktassák.

Mindezektől függetlenül ki kell hangsúlyozni, hogy a veszélyhelyzeti időszak intézkedései, azok végrehajtásának körülményei, lehetőségei, a szerzett tapasztalatok – előnyökkel és hátrányokkal együtt – a jövőben mindenképpen visszaforgathatók a folyamatok fejlesztése érdekében. A témakört érintő, 2020 júliusában bekövetkezett jogszabályváltozások egy része már ezen alapul. Az eddigi hiátus megszűnt azzal, hogy az Lrtv. kiegészült a 6/A. alcímmel, amely konkrétan nevesíti a különleges jogrendben bevezethető rendkívüli intézkedéseket. Mindez előremutató tény, hisz veszélyhelyzet akár „a kritikus infrastruktúrák olyan mértékű működési zavara" miatt is kihirdethető, amelynek „következtében a lakosság alapvető ellátása több napon keresztül, vagy több megyét érintően akadályozott" – jelenti ki a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló törvény.[36]

Az új szakasz egyértelműsíti, hogy különleges jogrend idején a létfontosságú rendszerek kijelölését illetően külön megállapítható az eljáró hatóság, megváltoztatható az eljárás időtartama és a végrehajtás szabályrendszere, illetve korlátozható az eljárásban részt vevők száma is. Nevesíti továbbá annak lehetőségét, hogy az adott kijelölt rendszer vonatkozásában a mindenkori kormány a tevékenység koordinálására kijelöljön egy kormánytagot, illetve kormányzati összekötő szakembert delegáljon, akiknek külön megállapítható a feladat- és hatáskörük. Fontos rendelkezés továbbá, hogy a bevezetett intézkedések a különleges jogrend megszűnését követő 60 napon belül kötelezően felülvizsgálandók, az illetékes ágazati kijelölő hatóságok bevonásával.[37] Ez a rendelkezéshalmaz minden olyan esetre megteremti a jogalapot, amely a normál működéstől eltér. Szakmai szempontból előremutató, hogy centralizált eljárási rend vezethető be, amely a különleges jogrendre okot adó körülmények teljes körű figyelembevétele mellett fókuszálhat a szükséges kijelölések végrehajtására. Ugyanakkor a cikkünkben bemutatott jogszabályi kötelezettségek oldaláról vizsgálva továbbra is hiányos, mert nem tér ki az érintettekre vonatkozó elvárások megváltoztatásának lehetőségére. Okkal feltételezhetjük, hogy ennek elmaradása a különleges jogrendi jogalkotás során ismét háttérbe szorul. Ahhoz, hogy ezek a részletszabályok is megalkothatók legyenek, nélkülözhetetlen a normál időszakban történő előzetes felkészülés, ami feltételezi, hogy a különleges jogrendben kialakításra kerülő struktúra központi szervnél legyen (célszerűen minisztériumnál), országos hatáskört kapjon, de kellő rugalmassággal, szükséges hatékonysággal működhessen, széles körű ismeretekkel és tapasztalattal rendelkező állományt vonultasson fel, amely képes a „civil attitűdhöz" alkalmazkodva is eredményeket elérni.

[36] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról 44. § *cd)* pont.

[37] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről 13/A. §. 2020. július 1-jei hatály szerint.

Felhasznált irodalom

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1100128.tv

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Online: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

2020. évi XII. törvény a koronavírus elleni védekezésről (hatályon kívül helyezve: 2020. 06. 18.). Online: https://net.jogtar.hu/jogszabaly?docid=a2000012.tv

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1300065.kor

187/2015. (VII. 15.) 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. Online: https://net.jogtar.hu/jogszabaly?docid=a1500187.kor

359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről. Online: https://net.jogtar.hu/jogszabaly?docid=a1500359.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. Online: https://net.jogtar.hu/jogszabaly?docid=a1800271.kor

86/2020. (IV. 5.) Korm. rendelet a veszélyhelyzet során alkalmazandó egyes honvédelmi tárgyú szabályokról (hatályon kívül helyezve: 2020. 06. 18.). Online: https://magyarkozlony.hu/dokumentumok/a67ce792810ae64f0fa5758c88c5876a95204b4e/letoltes

1012/2020. (I. 31.) Korm. határozat a Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzs felállításáról (visszavonva 2020. június 17.). Online: https://net.jogtar.hu/jogszabaly?docid=A20H1012.KOR

1101/2020. (III. 14.) Korm. határozat a koronavírus elleni védekezés kapcsán szükséges további intézkedésekről. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1101.KOR&dbnum=1

1109/2020. (III. 18.) Korm. határozat az ország működéséhez szükséges létfontosságú állami és nem állami gazdasági társaságok veszélyhelyzeti feladat-ellátásának szakmai támogatásáról. Online: https://net.jogtar.hu/jogszabaly?docid=a20h1109.kor

2/2020. (I. 24.) HM utasítás az ügyeletes minisztériumi felsővezetői feladatok ellátásáról és jelentési kötelezettségi körébe tartozó biztonsági kihívást jelentő helyzetek jegyzékéről. Online: http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2020/2.pdf

Honvédelem.hu/MTI: Benkő Tibor: csütörtök reggel jelennek meg az érintett vállalatoknál a honvédelmi irányító csoportok. *Honvedelem.hu,* 2020. március 18. Online: https://honvedelem.hu/hirek/hazai-hirek/benko-tibor-csutortok-reggel-jelennek-meg-az-erintett-vallalatoknal-a-honvedelmi-iranyito-csoportok.html

Honvédelmi Minisztérium: Hetvenegy vállalatnál kezdték el a munkát a Honvédelmi Irányító Törzsek. *Honvedelem.hu,* 2020. március 19. Online: https://honvedelem.hu/hirek/hazai-hirek/hetvenegy-vallalatnal-kezdtek-el-a-munkat-a-honvedelmi-iranyito-torzsek.html

Interpol: Cybercrime: Interpol report shows alarming rate of cyberattacks during COVID–19. *Interpol,* 2020. augusztus 4. Online: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Nemzeti Kibervédelmi Intézet: *Riasztás a Nemzeti Népegészségügyi Központ arculati elemeit felhasználó adathalász levelekkel kapcsolatban*. Online: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nemzeti-nepegeszsegugyi-kozpont-arculati-elemeit-felhasznalo-adathalasz-levelekkel-kapcsolatban

Nemzeti Kibervédelmi Intézet: *Riasztás a Nemzeti Népegészségügyi Központ nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban*. Online: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-a-nemzeti-nepegeszsegugyi-kozpont-neveben-kuldott-karos-csatolmanyt-tartalmazo-levellel-kapcsolatban

Nemzeti Kibervédelmi Intézet: *Riasztás: nyitott RDP port biztonsági kockázatai*. Online: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-nyitott-rdp-port-biztonsagi-kockazatai

WHO: *Listings of WHO's response to COVID-19* (2020. június 29.). Online: https://who.int/news-room/detail/29-06-2020-covidtimeline