Bonnyai Tünde – Danyek Miklós –
Görgey Péter – Kriskó Edina –
Molnár Anna – Tikos Anita

# KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019

Nemzeti Közszolgálati Egyetem, Budapest

# KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

## Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019


**Szerkesztő:**
Deák Veronika

**Szerzők:**
Dr. Bonnyai Tünde
Dr. Danyek Miklós
Görgey Péter
Dr. Kriskó Edina
Molnár Anna
Tikos Anita

**Szakmai lektor:**
Dr. Muha Lajos (kivéve: 3. fejezet)
A 3. fejezet szakmai lektora: Vereckei Béla Ferenc



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

**Felelős Kiadó:**
Prof. Dr. Kis Norbert Rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

# TARTALOM

# 1. TIKOS ANITA: A MAGYAR KIBERVÉDELEMMEL KAPCSOLATOS SZABÁLYOZÁS AKTUÁLIS KÉRDÉSEI

## 1.1. A kibervédelmi szabályozás változásához vezető út

Az Európai Unió már a 2000-es évek elején felismerte a kibertér jövőbeli szerepét és fontosságát az egységes piac és gazdaság versenyképességének fenntartásában és növelésében, melyhez elengedhetetlen a kiberbiztonság megteremtésé. A kibertér, az előnyei mellett komoly fenyegetéseket és kockázatokat is hordoz magában, melyeket a határon átnyúló természete miatt közösségi szinten fel kell mérni, majd pedig ki kell dolgozni a megfelelő védelmi mechanizmusokat EU-s és nemzeti szinten egyaránt. Ezen felismerésnek köszönhetően az Európai Unió is a napirendjére tűzte a kiberbiztonság megteremtésének és fejlesztésének kérdéskörét, melynek érdekében a politikai célkitűzések megfogalmazásán túl létrehozta a tagállamokat segítő és jó gyakorlatokat összegyűjtő Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (továbbiakban: ENISA), valamint az EU-s intézmények eseménykezelő központját a CERT-EU-t.

Ezzel párhuzamosan számos szakterületen fogalmazott meg az EU további információbiztonsági vagy kibertérhez kapcsolódó intézkedéseket, mint például a kiberbűnüldözésre, gyermekvédelemre, nemzetközi kiberbiztonsági együttműködésekre vonatkozóan.

Szektorspecifikus információbiztonsági elvárások és feladatok (főként eseménykezelés szintjén) is megfogalmazásra kerültek már néhány jelentősebb, a kibertér fenyegetéseinek jobban kitett szektorokban, mint például az energiaszektor, pénzügyi szektor, távközlési szektor stb.

Az EU a 2010-es évek elején arra a következtetésre jutott, hogy ezen szabályok ugyan fontos előrelépést jelentenek, de nem nyújtanak EU-szerte azonos, elégséges és megfelelő megoldást a kibertérben megjelenő fenyegetésekre vonatkozóan, mivel a tagállamok felkészültségi szintje (szabályozás, intézményrendszer, szolgáltatások stb.) továbbra is jelentős eltéréseket mutat.

Ezért az Unió egy egységes kiberbiztonsági politika létrehozását tűzte ki célul, mely a bűnüldözés és gyermekvédelem megerősítését, a nemzetközi együttműködések hangsúlyozását és támogatását, valamint az Uniószerte egységes szabályozási, fogalmi és intézményi alapok kidolgozását tűzte ki célul. Ezen politika egyik sarokpontja a 2013-ban elfogadott EU kiberbiztonsági stratégia[1] volt. Az EU kiberbiztonsági politikájának másik – jelen témánk szempontjából legfontosabb – elemének pedig a 2016-ban elfogadott Hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvet (továbbiakban: NIS irányelv) tekintjük.

Az irányelv egyik jelentősége, hogy az első átfogó, komplex EU-s szintű kiberbiztonsági jogszabály, mely minden tagállam számára kötelező intézkedéseket és minimum információbiztonsági szabályokat fogalmaz meg tíz kiemelkedő fontosságú szektorra vonatkozóan. Az irányelv jelentőségének másik fontos eleme, hogy kötelező és részletesen szabályozott EU-s szintű stratégiai és ope-

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

ratív együttműködési mechanizmusok (szakértői csoportok) létrehozását írja elő, melyben minden tagállam felelős szervezetének kötelező részt venni.

Az elmúlt években az irányelv rendelkezéseinek a nemzeti jogba történő átültetése jelentette az egyik legfőbb kihívást Magyarország és a többi EU-s tagállam számára. Jelenleg pedig az előírások és jogszabályok gyakorlati alkalmazása és végrehajtása jelenti a fő feladatot az irányelv hatálya alá eső, valamint az irányelv végrehajtásában és alkalmazásában feladatot ellátó intézmények számára.

## 1.2. A hálózati és információs rendszerek biztonságáról szóló irányelv

Az irányelv javaslat több mint 3 év alatt jutott át az EU-s jogalkotási folyamat útvesztőin, majd végleges formáját elérve 2016. július 19-én megjelent az Európai Unió hivatalos lapjában az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről címmel.

Ahogy az előző fejezetben már előrevetítettem, a NIS irányelv az első olyan, kötelező erejű, közösségi szintű szabályozás az információbiztonság területén, mely geopolitikai alapon határoz meg minimumszabályokat és kötelező együttműködési mechanizmusokat a szakosított intézmények, valamint az irányelv hatálya alá eső piaci szereplők, szolgáltatók számára. Fontos megjegyezni, hogy már az irányelv előtt is megfigyelhető volt egyes területeken (szektoronként vagy regionális szinten) az információbiztonsággal foglalkozó intézmények (pl.: eseménykezelő központok és hatóságok) közötti együttműködés, de ezek az együttműködési formák mindeddig önkéntesen és bizalmi alapon valósultak meg.

Az irányelv célja, hogy megteremtse a gyors és hatékony európai szintű kiberbiztonsági együttműködés és (incidenskezelés és -elemzés szintű) reagáló képesség alapjait, mely remélhetőleg hatékonyan alkalmazható lesz valamennyi lényeges biztonsági esemény és kockázat kezelésére. Annak érdekében, hogy egy ilyen hatékony és gyors együttműködési mechanizmus létrehozható legyen, a legkiemelkedőbb szektorokban meg kell teremteni a hálózati és információs rendszerek biztonságának általános védelmének alapjait Uniószerte. Ezért az irányelv ezen szektorokra vonatkozóan megfogalmazza a legfontosabb védelmi szempontokat és minimumelvárásokat, valamint az EU-s együttműködési mechanizmusok megfelelő működéséhez szükséges nemzeti szakosított szervezeteket és azok minimum feladatait, képességeit.

Ennek megfelelően az irányelv rendelkezései között elkülöníthetünk nemzeti szinten végrehajtandó és közösségi szinten végrehajtandó feladatokat, előírásokat. Jelen tananyag szempontjából a nemzeti szintű intézkedésekre vonatkozó előírások lesznek a relevánsak, de mindenképp fontosnak tartom előtte röviden bemutatni az EU-s szintű feladatokat is, hiszen a nemzeti szintű feladatok fő célja, hogy lehetővé tegyék az EU-s szintű együttműködési formák hatékony megvalósítását.

### *1.2.1. Az irányelv rendelkezéseiből adódó közösségi szinten végrehajtandó feladatok*

Az irányelv II. fejezete foglalkozik az EU-s szintű együttműködés létrehozásának kérdéskörével. Az EU-s tagállamok közötti bizalom erősítésnek, stratégiai együttműködés támogatásának, illetve a hálózati és információs rendszerek magas szintű biztonságának elősegítése és megteremtése érdekében az irányelv létrehozza a nemzeti hatóságok együttműködését biztosító Együttműködési Csoportot.

Az együttműködési csoport az alábbi feladatok ellátásáért felel:[2]

- stratégiai **iránymutatást nyújt** a számítógép-biztonsági eseményekre reagáló csoportok (továbbiakban: CSIRT) hálózatának,
- **megosztja a tapasztalatait** és a jó gyakorlatokat a NIS irányelv szerinti biztonsági események bejelentésére vonatkozóan, a képzéssel és tájékoztatással kapcsolatban, a hálózati és információs rendszerekre vonatkozó kutatásával és fejlesztésével kapcsolatban,
- biztosítja a **bevált gyakorlatok** tagállamok közötti cseréjét,
- **megvitatja a tagállamok képességeit**, felkészültségét, melybe bele tartozhatnak a nemzeti stratégiák és a CSIRT-ek hatékonyságának értékelése is (kérés esetén)
- évente **megvizsgálja** az irányelv rendelkezései alapján bejelentett incidensekről szóló összefoglaló jelentéseket,
- másfél évente **jelentést készít** a stratégiai együttműködés terén szerzett tapasztalatairól.

Az EU-s szintű gyors és hatékony operatív együttműködés, incidenskezelés és megelőzés megvalósítása érdekében az irányelv létrehozta a tagállamok kijelölt CSIRT-jeinek együttműködését biztosító CSIRT-ek hálózatát.

A CSIRT-ek hálózata az irányelv 12. cikkében foglaltak szerint az alábbi főbb feladatok ellátásáért felelős:

- **megosztja** a CSIRT-ek szolgáltatásaival, illetve operatív képességeivel kapcsolatos **információkat**,
- **megosztja** a biztonsági eseményekkel kapcsolatos nem bizalmas **információkat**,
- bármely tagállam kérése esetén, **megvitatja** az érintett tagállam joghatósága alá tartozó **biztonsági eseményt**,
- megvitatja és azonosítja az operatív együttműködés további formáit a megadott szempontok figyelembevételével,
- **megvitatja** a gyakorlatokból levont tanulságokat,
- másfél évente **jelentést készít** az operatív együttműködés terén szerzett tapasztalatairól.

Az irányelv rendelkezései kiterjednek a határon átnyúló események hatékony, gyors és koordinált kezelésének kérdéskörére is, melyben a tagállamok érintett intézményei (szektorális szereplők) és szakosított szervei (CSIRT-ek, hatóságok, nemzeti egyedüli kapcsolattartó pont) által követendő eljárás és (egyedüli kapcsolattartó pontok által koordinált nemzeti és EU-s) együttműködés főbb szabályait is lefekteti az irányelv.

Az irányelv rendelkezései szerint minden tagállam kijelöl egy hálózati és információs rendszerek biztonságáért felelős úgynevezett nemzeti egyedüli kapcsolattartó pontot (Single Point of Contact továbbiakban (SPOC)) az irányelv szerinti nemzeti illetékes hatóságok közül. A nemzeti kapcsolattartó pont feladata a nemzeti szintű koordináció biztosítása, abban az esetben, ha egy incidens több hatóságot és/vagy eseménykezelő központot érint. Kiemelt szerepet játszik a kapcsolattartó pont a határon átnyúló incidensek gyors és hatékony kezelésében hiszen, ha egy incidens két vagy több tagállamot érint (vagy akár érinthet) akkor a kapcsolattartó pont feladata, hogy tájékoztassa az érintett tagállamok kapcsolattartó pontjait az incidensről és a rendelkezésére álló információkról. Ezt követően a tagállamoknak már lehetősége nyílik közösen fellépni a támadással szemben az incidens kezelése (technikai segítségnyújtás, riasztások kidolgozása és terjesztése, valamint a nyilvánosság tájékoztatása) érdekében.

[2] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről 11. cikk (3)

### *1.2.2 Az irányelv rendelkezéseiből adódó nemzeti szintű feladatok*

Az irányelv előírásai szerint minden tagállamnak ki kell jelölnie egy vagy több (akár szektoronként egy) információbiztonsági hatóságot, valamint számítógép-biztonsági eseményekre reagáló csoportot (CSIRT). A kijelölésre kerülő CSIRT-eknek rendelkezniük kell az irányelv 1. mellékeltében megfogalmazott képességekkel, szolgáltatásokkal.

Fontos kiemelni, hogy az irányelv hatálya 2 féle szolgáltató típusra terjed ki: az alapvető szolgáltatásokat nyújtó, valamint a digitális szolgáltatásokat nyújtó szolgáltatókra.

Előbbiek olyan intézmények, amelyek kritikus társadalmi és/vagy gazdasági tevékenységekhez nyújtanak olyan szolgáltatást, mely hálózati és információs rendszerektől függ a következő ágazatokban:

- energia
- közlekedés
- banki szolgáltatások
- pénzügyi piaci infrastruktúrák
- egészségügy
- ivóvíz ellátás és -elosztás
- digitális infrastruktúra

Az irányelv hatálya alá eső másik alanyi kör a digitális szolgáltatásokat nyújtó szolgáltatók csoportja, melybe az online piactér, keresőmotorok, felhő szolgáltatók tartoznak.

A NIS irányelv különböző kijelölési szabályokat, biztonsági követelményeket, valamint incidensbejelentési kötelezettségeket fogalmaz meg mind az alapvető, mind a digitális szolgáltatást nyújtókra vonatkozóan.

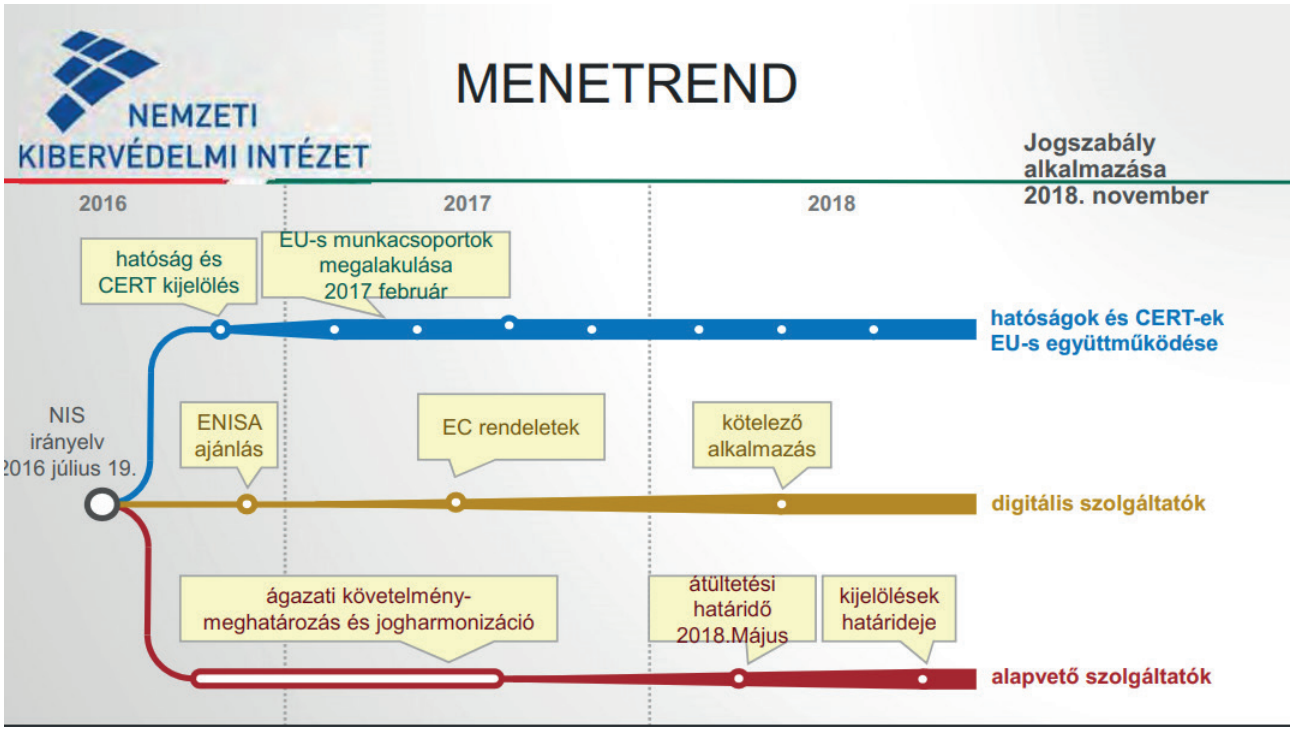
A hálózatbiztonsági irányelv valamennyi tagállam számára előírja, hogy meghatározott kritériumok[3] alapján dolgozzon ki a hálózat és információs rendszerek biztonságára vonatkozó nemzeti stratégiát.

A fent felsorolt szektorokban a tagállamoknak ki kell jelölniük az irányelv által meghatározott szempontok figyelembevételével a hatály alá eső intézményeket. Ezen kijelölés hatékonyságának érdekében a nemzeti szintű sajátosságok (pl.: piac mérete, piaci szereplők sajátosságai, szokásai stb.) figyelembevételével szektoronként pontosítani lehet az irányelv rendelkezéseiben megfogalmazott kijelölési kritériumokat.

Az irányelv átültetésének jelentős része 2016 és 2018 között valósult meg, mely időszakban párhuzamosan megkezdődött a közösségi szintű együttműködési mechanizmusok felállítása, a részletszabályok kidolgozása (végrehajtási aktusok és eljárásrendek útján), valamint a nemzeti jogszabályok harmonizációja.

[3] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről 7. cikk

A folyamat főbb állomásait az alábbi ábra részletekbe menően szemlélteti:




*1. ábra: A NIS irányelv átültetésének menetrendje*
*Forrás: Tikos Anita: Nemzeti Kibervédelmi Intézet bemutatása. Az információbiztonság törvényi szabályozása (2017. február 27.) in: Informatikai Szakbizottság anyagai (*https://eoq.hu/szakb/11/inf170227.pdf *) (letöltve: 2019. július 30.)*

Az irányelv rendelkezéseinek a nemzeti jogba való átültetésére és a felelős szakosított intézmények kijelölésére/létrehozására 21 hónap állt a tagállamok rendelkezésére. Ezt követően további 6 hónapja volt a tagállamoknak, hogy már a nemzeti jogszabályokban megfogalmazott kritériumok alapján elvégezzék a szolgáltatók kijelölését.

A hálózatbiztonsági EU-s előírásoknak irányelv formájában való elfogadása azt a lehetőséget biztosítja a tagállamok számára, hogy az irányelv előírásainak és rendelkezéseinek a nemzeti jogukba való átültetését önmaguk alakíthatják ki, hajthatják végre, kiegészíthetik, szigoríthatják rendelkezéseit vagy akár kiterjeszthetik a hatályát egyéb szektorokra is.

Ennek megfelelően a tagállamok többféle módon is megvalósíthatták a nemzeti jogba való átültetést:

- az addigi nemzeti szintű kiberbiztonsági jogi és szervezetrendszer teljes felülvizsgálatával, a NIS irányelv koncepciójának megfelelő átalakításával, újradefiniálásával,
- az addigi nemzeti szintű kiberbiztonsági jogi és szervezetrendszer kiegészítésével, mely a korábbi rendszert érintetlenül hagyva azon szektorokra és/vagy intézményekre alkalmazza a NIS irányelv előírásait, melyek nem tartoznak a korábbi jogszabályi előírások hatálya alá (pl: nem került kijelölésre, mint kritikus infrastruktúra, de NIS szerint jelentős – alapvető – szolgáltatást nyújt),
- az addigi nemzeti szintű kiberbiztonsági jogszabályi és szervezetrendszeren belül, annak kiegészítéseként valósul meg az irányelv elvárásainak a nemzeti jogrendbe való átültetése,
- végül pedig előfordulhat az úgynevezett hibrid megoldás is, mely során a fenti 3 lehetőség keveredését (szektoronként eltérően) figyelhetjük meg.

### *1.2.3. NIS irányelv átültetésének folyamata Magyarországon*

A továbbiakban részletesen bemutatom, hogy Magyarország mely megoldást választotta az irányelv rendelkezéseinek hazai jogrendbe való átültetésére, illetve, hogy milyen jogszabályi és szervezetrendszerbéli módosításokat és változásokat hajtott végre az irányelv implementációja érdekében.

A NIS irányelv megjelenését követő évben (2017. júliusában) a digitális ökoszisztéma egészét érintő minden polgárra, vállalkozásra és szakterületre kiterjedő Digitális Jólét Program (DJP) az akkori Nemzeti Fejlesztési Minisztériummal (a mai Innovációs és Technológiai Minisztérium) való együttműködésben kidolgozta a DJP2.0[4] elnevezésű stratégiai dokumentumot, mely összesen 26 területre vonatkozóan fogalmaz meg célkitűzéseket, feladatokat és fejlesztési programokat a digitális gazdaságfejlesztés érdekében. Az információbiztonság, kiberbiztonság témakör is helyet kapott a DJP2.0 által lefedett területek között, melynek célkitűzései között szerepel a hazai szabályozás harmonizációja a NIS irányelv rendelkezéseivel, valamint a nemzeti kiberbiztonsági stratégia felülvizsgálata a kibervédelmi képességek fejlesztésének érdekében, melyhez a feladatokat és felelősöket is magába foglaló intézkedési tervet is kell készíteni.

Ezen célkitűzések megfelelően tükrözik, hogy a NIS irányelv rendelkezéseinek átültetésének kérdéskörét Magyarország prioritásként kezelte, illetve az irányelv célkitűzéseivel egybecsengő olyan célokat fogalmazott meg a digitális fejlesztést megcélzó gazdaságfejlesztési program keretében, mint például a stratégia felülvizsgálata, valamint a szervezetfejlesztési célkitűzések (nemzeti CERT létrehozására vonatkozó javaslat).

Az Irányelv rendelkezéseinek a nemzeti jogba való átültetéséhez először fel kell mérni, hogy milyen stratégiai, jogszabályi és intézményi gyakorlattal rendelkezik Magyarország, melyek a magyarországi gyakorlat sajátosságai és ezek mennyire vannak összhangban a NIS irányelv által előírt szabályokkal.

A NIS irányelv szerinti szektorok (a digitális szolgáltatási szektorokat kivéve) legjelentősebb szolgáltatóira már vonatkoznak kiberbiztonsági előírások és jogszabályok kijelölt létfontosságú rendszerelemekként és létesítményekként, hiszen a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezései szerint a kijelölt létesítményeknek és rendszerelemeknek meg kell felelniük az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: L. tv. vagy Ibtv.) és annak végrehajtási rendeleteiben megfogalmazott előírásoknak.

Magyarországon a jogalkotók arra a döntésre jutottak, hogy a fentiek okán nem szükséges a NIS irányelv átültetését új stratégiai, jogszabályi vagy intézményi keretek között megvalósítani, hanem az új előírások nagyrészét a meglévő jogszabályok kiegészítéseként, azoknak kvázi egy új elemeként fogják átültetni a már leszabályozott területeken, mint például a nemzeti hálózat és információbiztonsági stratégia esetében, valamint az alapvető szolgáltatások szektoraira vonatkozóan.

A digitális szolgáltatásokra (online piactér, online keresőprogram és felhőalapú számítástechnikai szolgáltatás) vonatkozóan Magyarország korábban nem fogalmazott meg átfogó kiberbiztonsági elvárásokat, szabályokat, mindössze szektorális előírások és elvárások (például a pénzügyi ágazatban az MNB által megfogalmazott a közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV.1.) számú ajánlás) kerültek megfogalmazásra ezen szolgáltatások alkalmazására vonatkozóan az adott szektor képviselői számára. Ezért a NIS irányelvnek a digitális szolgáltatásokat nyújtókra vonatkozó előírásainak a magyar jogba való átültetése érdekében új jogszabály kerül kidolgozásra.

Az Irányelv átültetésére vonatkozó koncepcionális kérdések (intézményi felelősségek, stratégiai felülvizsgálat, új jogszabály kidolgozása, vagy valamely másik koncepcióba, jogszabályba való beillesztés) eldöntését követően az összes szükséges jogszabályi módosítást és új jogszabály létrehozá-

[4] Digitális Jólét Program 2.0 stratégia: https://digitalisjoletprogram.hu/files/58/f4/58f45e44c4ebd9e53f82f56d5f44c824.pdf

sára vonatkozó kezdeményezést egy úgynevezett implementációs táblában gyűjtik össze az érintett szakterületek képviselői. Ezen tervezet alapján az adott területért felelős döntéshozók végre tudják hajtani a szükséges jogszabályi változtatásokat, fejlesztéseket.

## 1.3. A Nemzeti Kiberbiztonsági Stratégia szabályozás

A korábbi fejezetekben már ismertettem a NIS irányelv főbb célkitűzéseit, melynek egyik fontos eleme, a 7. cikkben megfogalmazott előírás, miszerint a tagállamoknak el kell fogadniuk egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát. Az Irányelv előírásainak megfelelően a létrehozandó stratégiának legalább a NIS irányelv hatálya alá tartozó ágazatokra ki kell terjednie, illetve az alábbi témákat kell érintenie az 7. cikk (1) a.) -g.) pontok alapján:

- nemzeti stratégia céljai és prioritásai,
- a megfogalmazott célok és prioritások végrehajtását segítő szereplők szerepköre és felelőssége,
- köz- és magánszféra együttműködése (PPP) a felkészültség, reagálás és helyreállítás elősegítéséhez szükséges intézkedések,
- a stratégiához kapcsolódó oktatási, képzési vagy tájékoztató programok létrehozása/megnevezése,
- a stratégiához kapcsolódó Kutatási és fejlesztési tervek kijelölése,
- kockázatértékelési terv,
- a stratégia végrehajtásában szerepet játszók szereplők jegyzéke.

Ezen előírásoknak megfelelően Magyarországnak meg kellett vizsgálnia, hogy a hatályos Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III.21.) Korm.határozat megfelel-e az Irányelv előírásainak, valamint a stratégia létrejötte óta a digitális technológia fejlődésének köszönhetően megjelent újabb típusú fenyegetésekre és kihívásokra fogalmaz-e meg célkitűzéseket, intézkedéseket.

A 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégia egy rövid, tömör és alapvető célkitűzéseket megfogalmazó stratégia, melynek a célja, hogy lefektesse az információbiztonság alappilléreit. A stratégiában a kormány rögzíti, hogy Magyarország vállalja a kibertér védelmével kapcsolatosan felmerülő feladatok felelősségteljes ellátását.

A 2013-ban elfogadott kiberbiztonsági stratégia az alábbi célkitűzéseket fogalmazza meg:

- a kormányzati, magán- illetve a tudományos szféra együttműködésének támogatása (Public Private Partnership vagyis PPP),
- nemzetközi együttműködés a globális kibertér szereplőivel (regionális együttműködések, valamint az egyes nemzetközi szervezeteken- EU, NATO, EBESZ, ENSZ- belül megvalósuló együttműködések),
- kiberbiztonsági oktatás és képzés fejlesztése,
- gyermekek védelme,
- tudatosítás,
- kutatás-fejlesztési a nemzetközi gyakorlatnak megfelelően,
- szabályozások kidolgozása,
- szakosított intézmények létrehozása,
- gazdasági szereplők motiválása.

A fenti felsorolásból láthatjuk, hogy a 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégia számos a NIS irányelv szerinti stratégiai területeket, célkitűzéseket is érint, de túlságosan általánosan, felületesen. Ez ilyen formában nem felelne meg a NIS irányelv szerinti követelményeknek. A 2013-as stratégia nem rendelkezik továbbá a végrehajtásba bevont szereplők jegyzékével, ütemtervvel, illetve nem határoz meg a célok elérése érdekében létrehozandó K+F terveket, oktatási programokat.

Magyarország kormányzata végül arra a döntésre jutott, hogy a nemzeti kiberbiztonsági stratégia megújítását, az új kihívásokra vonatkozó célkitűzések megfogalmazását, valamint az EU-s kötelezettségeknek való megfelelést a 2013-as Nemzeti Kiberbiztonsági Stratégiában foglalt értékeket megtartva fogja Magyarország kiberterének biztonságát és védelmét erősíteni.

Ennek megfelelően, a 2013. évi Magyarország Nemzeti Kiberbiztonsági Stratégia változtatások nélkül hatályban maradt, mint a magyar kibertér alappilléreit lefektető legfőbb kiberbiztonsági stratégia. Ennek kiegészítéseként, úgynevezett szektorális stratégiaként 2018 decemberében a kormány elfogadta a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozatot.

A 2018-ban elfogadott szektorális stratégia célja a NIS irányelv előírásainak való megfelelés, illetve a 2013-as nemzeti stratégia elfogadása óta megjelent új kiberbiztonsági kihívásoknak és fejlesztésekre való célkitűzések megfogalmazása. Az ágazati stratégia 56 intézkedést határoz meg a digitális környezet iránti bizalom erősítése, a digitális infrastruktúravédelem, valamint a gazdasági szereplők támogatása érdekében megfogalmazott célkitűzésekre vonatkozóan.

A digitális környezet iránti bizalom erősítésének érdekében a stratégia célul tűzi ki, a szakmai együttműködések erősítését (társadalmi szintű és szakmai együttműködésekben egyaránt) és a párbeszéd kialakítását; a biztonságtudatosság növelését, a kiberbűnüldözés továbbfejlesztését (a rendvédelem és igazságszolgáltatás kiberbűnözés elleni fellépésének és képességeinek fejlesztése útján); a szakmai irányító intézményrendszer (kormányzati felelősségbe tartozó intézmények) fejlesztését a feladataik, hatáskörük és együttműködési szabályaik felülvizsgálata útján.

A hatékony digitális infrastruktúravédelem érdekében a stratégia célkitűzései között szerepel az informatikai fejlesztések minőségmenedzsmentje (ide értve a „security by design” elv érvényesítését); a kormányzati elektronikus szolgáltatások biztonságának növelését; a nemzetközi együttműködés erősítését (beleértve a NIS irányelv szerinti együttműködési fórumokon való aktív részvételt, valamint Magyarország többi globális, regionális és bilaterális kiberbiztonsági együttműködését); az alapvető szolgáltatások, valamint a létfontosságú infrastruktúrák és szolgáltatásaik védelmét (mely a NIS irányelv hatékony végrehajtására és a szabályozás alá eső szektorok szolgáltatóinak szakmai és módszertani támogatására terjed ki). A digitális infrastruktúravédelemre vonatkozó célkitűzések közé tartozik még a kibervédekező, -elhárító, és -reagáló képességek fejlesztése (passzív és aktív eszközök egyaránt).

A gazdasági szereplők támogatása érdekében a stratégia célul tűzte ki, a kutatás-fejlesztés szerepének növelését (K+F stratégia, állami ösztönzés, főbb K+F témák azonosítása, stb.), a Kutatóközpontokkal való együttműködést; hazai digitális innováció támogatását (támogatási konstrukciók kidolgozása és továbbfejlesztése, a folyamatkoordinált és átlátható végrehajtása); valamint a versenyképes hazai tudásbázis létrehozását (oktatás, továbbképzés a társadalom széles körében; kiberversenyek és gyakorlatok a tanulók számára).

A stratégia tartalmazza továbbá a stratégia létrejöttekor hatályos jogszabályok végrehajtásába bevont szereplők jegyzékét, mely összegzi a felhatalmazással rendelkező szervek jogszabály szerinti feladatait, illetve azon információkat, hogy mely szervezetekkel/intézményekkel működnek együtt a jogszabályok végrehajtása során.

Az ágazati stratégia által megfogalmazott intézkedések végrehajtását elősegítő és szabályozó intézkedési terv (meghatározza a végrehajtás ütemezését és az intézkedésekhez kapcsolódó felelősöket) kidolgozását is előírja a 1838/2018. (XII. 28.) számú Kormányhatározat.

## 1.4. Alapvető szolgáltatást nyújtó szolgáltatók szabályozása

A NIS irányelvet ismertető fejezetben leírtaknak megfelelően az irányelv IV. fejezete előírásokat és biztonsági követelményeket fogalmaz meg az úgynevezett alapvető szolgáltatásokat nyújtó intézményekre vonatkozóan, valamint előírja ezen szereplők számára a kötelező incidens bejelentési kötelezettséget (és annak minimum elemeit, tartalmát).

Ahogy a lenti táblázatban is jól látszik, a NIS irányelv által definiált alapvető szolgáltatást nyújtó szolgáltatási ágazatok (és alágazatok) köre nagyrészt megegyezik a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (továbbiakban: Lrtv.) hatálya alá tartozó szektorokkal és alszektorokkal.

| ÁGAZAT | ALÁGAZAT | A NIS IRÁNYELV SZERINTI ÁGAZAT VAGY ALÁGAZAT |
|---|---|---|
| Energia | villamosenergia-rendszer létesítményei | Villamos energia |
| | kőolajipar | Kőolaj |
| | földgázipar | Földgáz |
| Közlekedés | közúti közlekedés | Közúti közlekedés |
| | vasúti közlekedés | Vasúti közlekedés |
| | légi közlekedés | Légi közlekedés |
| | vízi közlekedés | Vízi közlekedés |
| | logisztikai központok | |
| Agrárgazdaság | mezőgazdaság | |
| | élelmiszeripar | |
| | elosztó hálózatok | |
| Egészségügy | aktív fekvőbeteg-ellátás | Egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is) |
| | mentésirányítás | |
| | egészségügyi tartalékok és vérkészletek | |
| | magas biztonsági szintű biológiai laboratóriumok | |
| | gyógyszer-nagykereskedelem | |
| Társadalombiztosítás | társadalombiztosítási ellátások igénybevételéhez kapcsolódó informatikai rendszerek és | |
| Pénzügy | pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei | Pénzügyi piaci infrastruktúrák |
| | bank- és hitelintézeti biztonság | Banki szolgáltatások |
| | készpénzellátás | |
| Infokommunikációs technológiák | internet-infrastruktúra és internet hozzáférés szolgáltatás | Digitális infrastruktúra |
| | vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok | |
| | rádiós távközlés | |
| | űrtávközlés | |
| | műsorszórás | |
| | postai szolgáltatások | |
| | kormányzati informatikai, elektronikus hálózatok | |

| | | |
|---|---|---|
| Víz | ivóvíz-szolgáltatás | Ivóvízellátás és -elosztás |
| | felszíni és felszín alatti vizek minőségének ellenőrzése | |
| | szennyvízelvezetés és -tisztítás | |
| | vízbázisok védelme | |
| | árvízi védművek, gátak | |
| Közbiztonság - Védelem | rendvédelmi szervek infrastruktúrái | |
| Honvédelem | honvédelmi rendszerek és létesítmények | |

*1. táblázat: A NIS irányelv szerinti alapvető szolgáltatási ágazatok (valamint alágazatok) és az Lrtv. hatálya alá tartozó szektorok összevetése, megfeleltetése*
*Forrás: a táblázatot a szerző a 2012. évi CLXVI. törvény 4. mellékelte alapján (a táblázat adatait kivonatolva) készítette*

Az eredeti táblázat elérhető:
https://net.jogtar.hu/jogszabaly?docid=A1200166.TV#lbj7idc0e8 (letöltve: 2019.augusztus 3.)

A kijelölt létfontosságú rendszerek és létesítmények esetében a humán és fizikai védelem biztosításán túl, az informatikai rendszereik védelmének biztosítását is előírja az Lrtv. az üzemeltetők számára, melynek megvalósítása során az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénynek és annak végrehajtási rendeleteinek követelményeinek kell megfelelniük. A jogszabály (Lrtv.) előírja ezen szektorok hatósági felügyeletének (az Országos Katasztrófavédelmi Főigazgatóság által) szükségességét, illetve ezen rendszerek és létesítmények operatív támogatását biztosító eseménykezelőközpont, a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központot (LRLIBEK) létrehozását.

Ezen körülményeket figyelembe véve Magyarországon az a koncepcionális döntés született, hogy a NIS irányelv szerinti alapvető szolgáltatásokra vonatkozó előírásokat és szabályokat a létfontosságú rendszerek és létesítményeket szabályozó keretrendszerbe beillesztve, azt kiegészítve ültetik át a nemzeti jogba, hiszen a jogszabályi előírásoknak és felügyeleti, támogatói intézményi feltételeknek is nagyrészt megfelel.

### *1.4.1. Alapvető szolgáltatást nyújtó intézmények kijelölése*

Ennek megfelelően a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényt kiegészítették a jogalkotók a 2/A §-val, mely az alapvető szolgáltatók kijelölésére és nyilvántartására vonatkozó külön (kiegészítő) szabályokat, feltételeket tartalmazza.

Az új rendelkezések[5] alapján, **alapvető szolgáltatásokat nyújtó szereplőnek azon intézmény jelölhető ki**, mely:

- kijelölt nemzeti létfontosságú rendszerelem üzemeltetője,
- a NIS irányelv II. mellékletében felsorolt ágazatok és alágazatok valamelyikébe sorolható szolgáltatást nyújt
- szolgáltatása elektronikus információs rendszerektől függ
- a szolgáltatását érintő biztonsági esemény jelentős zavart okozna az általa nyújtott szolgáltatás biztosításában

[5] 2012. évi CLXVI. törvényt 2/A §

Az Lrtv. szerinti létfontosságú rendszerelem fogalma pedig magába foglalja azt a követelményt, hogy a rendszerelem elengedhetetlen a létfontosságú társadalmi feladatok ellátásához. A fenti előírások összességében megfelelnek az irányelv által az alapvető szolgáltatásokat nyújtó szereplők azonosítására előírt kritériumoknak[6].

Az intézmény **alapvető szolgáltatást nyújtó szereplővé nyilvánításának folyamata** hatósági eljárás formájában történik, mely a következő lépésekből áll:

- a kijelölt létfontosságú rendszerelemek üzemeltetői megvizsgálják a 2/A. § (2) bekezdés előírásainak való megfelelést. Az erről készült elemzést azonosítási jelentés kiegészítés formájában benyújtja az üzemeltető a kijelölő hatóság részére, abban az esetben, ha a rendszerelem ágazata/alágazata tekintetében megállapítható az előírásoknak való megfelelés.
- az adott szektor ágazati kijelölő hatósága az azonosítási jelentés kiegészítés beérkezését követő 30 napon belül hoz döntést az alapvető szolgáltatóvá történő kijelölésről. A kijelölés elfogadását vagy megerősítését az ágazati kijelölő hatóság nemzeti létfontosságú rendszerelemmé kijelölő határozat formájában teszi hivatalossá.

Az ilyen folyamat során kijelölt alapvető szolgáltatók jegyzékét a nyilvántartó hatóság kezeli és vezeti. A nyilvántartó hatóság az alapvető szolgáltatók jegyzékét 2 évente felülvizsgálja és szükség esetén frissíti, aktualizálja.

Az ágazatspecifikus kijelölési szabályokat, a kijelölőhatóságot és a helyszíni ellenőrzéseket végző szervezetek kijelölését az úgynevezett ágazatspecifikus rendeletek tartalmazzák a létfontosságú rendszerelemek és létesítmények vonatkozásában, de azok az alapvető szolgáltatóvá való kijelölésre vonatkozóan nem fogalmaztak meg további ágazatspecifikus kritériumokat.

A NIS irányelv átültetésének megkezdése idején a NIS ágazatok közül a közlekedés, valamint az infokommunikációs technológiák ágazatokra vonatkozóan még nem volt elfogadott és hatályos ágazatspecifikus rendelet Magyarországon, így ezen szektorokban nem került létfontosságú rendszerelem kijelölésre, melynek következtében alapvető szolgáltatást nyújtó intézményt sem volt lehetőség kijelölni ezen szektorokban.

Az irányelv megfelelő átültetése céljából a fent említett két szektorban is mielőbb ki kellett dolgozni a szükséges szektorális szabályokat. Ennek eleget téve, 2017. szeptember 5-én megjelent az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 249/2017. (IX. 5.) Korm. rendelet, illetve 2019. július 4-én pedig a közlekedési szektorra vonatkozó a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 161/2019. (VII. 4.) Korm. rendelet jelent meg.

Ezen végrehajtási rendeletek esetében is fennáll azon következtetés, hogy az alapvető szolgáltatóvá való kijelölésre vonatkozóan nem fogalmaztak meg további (a létfontosságú rendszerelemtől eltérő) ágazatspecifikus kritériumokat.

A nem kijelölt létfontosságú rendszerelmeknek alapvető szolgáltatást nyújtó szereplőként való azonosítására a nyilvántartó hatóság állásfoglalása[7] szerint a vonatkozó ágazati Korm. rendelet hatálybalépését követő 180 nap áll rendelkezésre. Ezen idő alatt a lehetséges rendszerelem üzemeltetőjének el kell készítenie (és benyújtania az illetékes kijelölő hatóság részére) az azonosítási jelentést, mely a létfontosságú rendszerelem és az alapvető szolgáltatóvá való kijelölés kritériumainak való megfelelésre vonatkozó elemzést egyaránt tartalmaznia kell. Tehát a jogszabályi előírásnak és definíciónak megfelelően mindenképp létfontosságú rendszerelemmé kell válnia az intézménynek ahhoz, hogy alapvető szolgáltatóvá lehessen kinevezni.

---

[6] A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv 5. cikke

[7] OKF Tájékoztató: http://www.katasztrofavedelem.hu/letoltes/iparbiztonsag/szolgaltatok/Tajekoztato_Alapveto_szolgaltatast_nyujtok_reszere.pdf

A jogszabályi[8] előírások szerint a még ki nem jelölt rendszerelem azonosítási jelentésének az alábbiakat kell tartalmaznia:

- rendszerelem megnevezése, az arra vonatkozó kockázatelemzés
- nemzeti vagy európai létfontosságú rendszerelemmé történő kijelölésre vonatkozó javaslat
- az azonosítási jelentés teljességére vonatkozó üzemeltetői nyilatkozat
- azonosítási eljárás kezdő és záró időpontja
- Lrtv. 4. mellékletében szereplő ágazatba vagy alágazatba sorolás (ha lehetséges)
- Lrtv. 2/A. § (2) bekezdésében foglalt kritériumoknak való megfelelésről szóló elemzés

Az újonnan kijelölendő rendszerelemek és szolgáltatások kijelölésére vonatkozó azonosítási jelentés elbírálására 70 napja van a szektorért felelős kijelölő hatóságnak.

### *1.4.2. Kijelölt alapvető szolgáltatókra vonatkozó biztonsági követelmények*

A NIS irányelv 14. és 15. cikke tartalmazza az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó minimum biztonsági követelményeket:

- megfelelő és arányos műszaki és szervezési intézkedéseket dolgozzanak ki a hálózati és információs rendszereik biztonságát fenyegető kockázatok kezelése érdekében
- a kockázatokkal arányos biztonsági szintet biztosítsanak
- biztosítsák az érintett szolgáltatás folytonosságát a biztonsági események megelőzése, valamint hatásuk csökkentése érdekében
- rendelkezzenek biztonsági szabályzatokkal, illetve azok végrehajtását igazoló dokumentumokkal (mely megvalósulhat akár képesített ellenőr általi ellenőrzés útján is).

Az irányelv előírásainak – a jogszabályi sajátosságaiból adódóan - a nemzeti jogba történő átültetése során ezen követelmények pontosíthatók, szigoríthatók vagy részletezhetők a tagállami sajátosságok és igények alapján.

Mivel Magyarországon az alapvető szolgáltatások a kijelölt létfontosságú rendszerelemek keretén belül kerültek átültetésre, így a létfontosságú rendszerelemekre vonatkozó elektronikus információbiztonsági előírások kiegészítésével, pontosításával tehetünk eleget az irányelv követelményeinek. A létfontosságú rendszerelemek elektronikus információs rendszereire vonatkozó biztonsági szabályokat az Ibtv. és a hozzá kapcsolódó, a végrehajtását segítő Korm. rendeletek tartalmazzák. Mivel az Ibtv.-ben és végrehajtási rendeleteiben megfogalmazott követelmények lefedik az Irányelvben szereplő követelményeket, így az irányelv nemzeti jogba történő átültetéséért felelős döntéshozók úgy határoztak, hogy az alapvető szolgáltatást nyújtókra vonatkozó követelmények szigorítása vagy kiegészítése nem szükséges.

**Tehát azon szolgáltatóknak/ intézményeknek, melyek kijelölt alapvető szolgáltatók lesznek nem keletkezik semmilyen biztonsági követelményeknek való megfelelésből adódó többletfeladatuk.**

További, szektorspecifikus útmutatások, biztonsági követelmények és szabványok találhatóak az alapvető szolgáltatásokra vonatkozóan az ENISA és az együttműködési csoport által készített „Az alapvető szolgáltatásokat nyújtókra vonatkozó biztonsági követelmények feltérképezése az egyes

[8] 65/2013. (III. 8.) Korm. rendelet
a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) számú Korm. rendelet 2. § (2)

ágazatok számára[9]" című tanulmányban. A tanulmányban felsorakozatott követelmények és útmutatások segítséget nyújthatnak azon intézményeknek, amelyek több EU-s tagállamra is szeretnék kiterjeszteni a szolgáltatásaikat, hiszen így be tudnak vezetni olyan többletintézkedéseket vagy szabályokat, mely segítségével a többi tagállamban megfogalmazott elvárásoknak, követelményeknek is jobban meg tudnak felelni.

### *1.4.3. Alapvető szolgáltatók incidensbejelentési kötelezettségei*

A NIS irányelv 15. cikke az alapvető szolgáltatásokat nyújtó szereplők számára incidensbejelentési kötelezettséget is megfogalmaz. Az irányelv biztonsági események bejelentésére vonatkozó szabályaival (jelentős hatás fogalmának bevezetése, illetve indokolatlan késedelem nélküli bejelentési kötelezettség) kiegészítette az eseménykezelő központok feladatairól szóló 271/2018. (XII. 20.) Korm. rendeletet.

Az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet 9. § előírja, hogy az alapvető szolgáltatást nyújtó intézmények „indokolatlan késedelem nélkül" bejelentik az adott szektorért felelős eseménykezelő központnak azon biztonsági eseményeket, melyek jelentős hatást gyakorolnak alapvető szolgáltatásuk folytonosságára.

A biztonsági eseményről szóló jelentésnek tartalmaznia kell (a megszokott és már korábban előírt elemeken túl) a szolgáltatás zavara által érintett felhasználókat, az esemény időtartalmát, valamint földrajzi kiterjedését.

Ha az alapvető szolgáltatást végző intézmény egy alapvetőnek nyilvánított szolgáltatását egy digitális szolgáltatást nyújtó intézményre alapozza (kiszervezés keretében), akkor a digitális szolgáltatást nyújtó szereplőt ért biztonsági eseményeket is be kell jelenteni az eseménykezelő központnak, ha az jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

## 1.5. Digitális szolgáltatást nyújtó szolgáltatók szabályozása

Ahogy fentebb már említettem a NIS irányelv szerinti digitális szolgáltatások körébe az online piacteret, online keresőprogramokat, valamint a felhő alapú számítástechnikai szolgáltatásokat soroljuk. Ezen szolgáltatások hálózati és információs rendszereire vonatkozóan Magyarországon a NIS irányelv implementálását megelőzően nem volt előírásokat, követelményeket tartalmazó szabályozás. Így ez egy tejesen új és feltérképezendő területnek számít.

A felhő alapú szolgáltatások alkalmazása jelentősen elterjedt az elmúlt évek során, így azokra vonatkozóan már fogalmaztak meg követelményeket és előírásokat egyes szektorális felügyeleti hatóságok (például a kormányzati szektor intézményeit felügyelő Nemzeti Elektronikus Információbiztonsági Hatóság, illetve a pénzügyi szektor felügyeletéért felelős Magyar Nemzeti Bank). Ezen szabályok inkább csak a szolgáltatást alkalmazni kívánó intézmények számára fogalmaznak meg alkalmazási feltételeket, szabályokat, illetve a hatóságok minimális kötelezettségeket róttak a digitális szolgáltatásokat nyújtókra.

[9] Mapping of OES Security Requirements to Specific Sectors: https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/at_download/fullReport

A NIS szerinti digitális szolgáltatások az elektronikus kereskedelemről, illetve az információs társadalommal kapcsolatos szolgáltatásokról szóló EU-s és nemzeti szabályozások hatálya alá sorolhatók. Ennek megfelelően a fent említett szolgáltatási csoporthoz kapcsolódó főbb szabályokat (pl: szolgáltató és közvetítő szolgáltató felelősségei, elektronikus úton történő szerződéskötés szabályai, elektronikus hirdetésre vonatkozó különös szabályok, információs társadalommal összefüggő szolgáltatásokra vonatkozó különös fogyasztóvédelmi szabályok stb.), illetve a szolgáltatásokra vonatkozó definíciókat az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (továbbiakban: Ekertv.) tartalmazza Magyarországon. Ezért első körben ezen jogszabályt kellett kiegészíteni a NIS irányelv digitális szolgáltatásokra vonatkozó főbb elvárásaival, feladataival.

A NIS irányelv szerinti digitális szolgáltatók körére a magyarországi jogszabályok a bejelentés-köteles szolgáltatást nyújtók fogalmát alkalmazzák, melyet az Ekertv. 2. § (j) pontja vezetett be, definiált. Az **Ekertv**. kiegészült még egy új, a bejelentés-köteles szolgáltatásokra vonatkozó különös szabályok című fejezettel, mely lefekteti az ezen szolgáltatást nyújtókra vonatkozó **főbb alapelveket** az alábbiak szerint:

- 6/A pont előírja, hogy a bejelentés-köteles **szolgáltatásokat nyújtóknak meg kell tenniük a szükséges intézkedéseket** annak érdekében, hogy az általuk használt hálózati és információs rendszerek vonatkozásában megelőzzék az incidensek bekövetkezésének valószínűségét, illetve a mégis bekövetkező incidenseket kezeljék, hatásukat pedig csökkentsék.
- előírja,[10] hogy a Kormány **külön rendeletben fogalmazza meg** a bejelentés-köteles szolgáltatások hálózati és információs rendszereinek **biztonságára vonatkozó szabályokat, követelményeket**.
- a rendeletben előírt **követelmények teljesülését a kijelölt hatóság ellenőrizheti**,
- a bejelentés-köteles szolgáltatóknak a rendeletben meghatározott **biztonsági eseményeket be kell jelenteniük, melynek részletes szabályait és eljárásait külön rendeletbe kell foglalni,**
- lehetővé teszi, hogy **a kijelölt hatóság bírságot szabhasson ki** a bejelentés-köteles szolgáltatás nyújtója számára **mulasztás esetén**.
- követelmények **nem alkalmazandók** azon bejelentés-köteles szolgáltatásokra, melyeket **mikro- és kisvállalkozások** nyújtanak.

A NIS irányelv előírásainál szigorúbb szabályozást dolgozott ki Magyarország, amikor az implementáció során rendeletben előírja, hogy **a bejelentés-köteles szolgáltatást nyújtóknak regisztrálniuk kell magukat a rendelet által kijelölt hatóságnál**, mely nyilvántartást vezet a regisztrált, bejelentett szolgáltatást nyújtókról.

Az Ekertv. 17. § (1a) bekezdésében foglalt felhatalmazásnak megfelelően a Kormány elfogadta a bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendeletet, mely részletes előírásokat és szabályokat tartalmaz:

- a kijelölt hatóság feladataira és hatáskörére,
- a bejelentés-köteles szolgáltatást nyújtó intézmények elektronikus és információs rendszereinek biztonságára vonatkozó főbb követelményekre,
- a jelentős biztonsági eseményekre és azok bejelentésére vonatkozó szabályokra,
- a jogkövetkezményekre, valamint
- a jogszabálysértések esetén kiszabható bírságok és azok mértékére (1. melléklet) vonatkozóan.

[10] Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 6/A §

A 410/2017 (XII.15.) Korm. rendelet 2018. május 10-én lépett hatályba. A Korm. rendelet végrehajtásának első néhány hónapját követően a kormányzat a bejelentés- köteles szolgáltatásokra vonatkozó szabályok és előírások pontosítását és további intézkedésekkel való kiegészítését látta szükségesnek. Az előírások felülvizsgálata során az ezen szolgáltatások felügyeletére kijelölt hatóság (OKF) és eseménykezelő központ (OKF LRLIBEK) módosítására is sor került (a Nemzeti Kibervédelmi Intézet szervezeti egységei kapnak felhatalmazást).

A 410/2017 (XII.15) Korm. rendelet felülvizsgálatát követően 2018. december 20-án a Kormány elfogadta az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018 (XII.20.) számú Korm. rendeletet, mely a 2019. január 1-i hatályba lépésével hatályon kívül helyezi a korábbi, 410/2017. számú Korm. rendeletet.

Az új (270/2018 számú) Korm. rendelet a korábbi rendelkezésekhez képest kiterjesztette annak hatályát a közvetítő szolgáltatókra, valamint további jogszabályi hivatkozásokkal egészült ki. Ennek köszönhetően az Ibtv. és az annak végrehajtását elősegítő jogszabályok előírásaival is gazdagította, egyértelműsítette a rendelet előírásait.

A 270/2018. számú Korm. rendelet **hatálya kiterjed azon intézményekre**, melyek:

- az Ekertv.-ben meghatározott bejelentés-köteles szolgáltatást nyújtó szolgáltatókra (online piactér; felhőalapú számítástechnikai szolgáltatás, keresőszolgáltatás)
  - o melyek nem tartoznak a mikro- és kisvállalkozások körébe,
  - o melyek nem lettek európai vagy nemzeti létfontosságú rendszerelemként kijelölve,
- közvetítő szolgáltatókra (Ekertv. 2. § (l) bekezdés (la)-(le)-ben megfogalmazott definíció szerint).

A fenti leírás és a hivatkozott jogszabályok szerinti szolgáltatás definíciók alapján sem könnyű azonosítani, hogy egy adott szolgáltatás a Korm. rendelet hatálya alá tartozik-e vagy sem. Felmerülhet a kérdés, hogy online piactérnek tekintjük-e azt az esetet, amikor egy cég kizárólag saját termékei/szolgáltatásai számára saját online webshopot működtet, vagy csak azon nagy online webshopok tartoznak a rendelet hatálya alá, melyek bárki számára felületet biztosítanak a termékeik eladására? A felmerülő kérdések megválaszolására jelen tananyag keretében nem vállalkoznék, főként azért, mert a bejelentés-köteles szolgáltatások felügyeletéért felelős hatóság a honlapján (https://nki.gov.hu/hatosag/tartalom/a-bejelentes-koteles-szolgaltatasokrol/) részletesen, jogszabályokkal alátámasztva és azokat gyakorlati szabályokra és magyarázatokra lefordítva pontosítja, hogy mely szolgáltatások minősülnek és melyek nem online piactérnek, felhőalapú számítástechnikai szolgáltatásnak, valamint keresőszolgáltatásnak.

### *1.5.1. A bejelentés-köteles szolgáltatást nyújtó intézmény kötelezettségei*

A bejelentés- köteles szolgáltatást nyújtó intézmények esetében nem szükséges az azonosítási eljárás, hiszen a mikro- és kisvállalkozások, illetve az európai vagy nemzeti létfontosságú rendszerelemek kivétel az összes szolgáltató a jogszabály hatálya alá tartozik. Ezért mindössze egy regisztrációs folyamat teljesítését írja elő a jogszabály (mely meghaladja az EU-s elvárásokat). A regisztrációt a hatóság holnapján, elektronikus úton kell elvégezni a következő adatok megadásával (https://nki.gov.hu/hatosag/tartalom/urlapok/ ) :

- gazdasági társaság neve,
- székhelye,
- cégjegyzékszáma,
- kapcsolattartási adatai,
- szolgáltatás típusa.

A bejelentés-köteles szolgáltatást nyújtó intézmény számára **előírt biztonsági intézkedések:**

- rendelkezzen kockázatelemzéssel a hálózati és információs rendszerek biztonságára vonatkozóan,
- vezessen be és alkalmazzon a kockázatokkal arányos biztonsági intézkedéseket,
- biztosítsa az üzletmenet folytonosságát,
- rendelkezzen azon biztonsági dokumentumokkal (szabályzatok és jegyzőkönyvek stb.) melyek lehetővé teszik a szolgáltató rendszereinek biztonsága érdekében alkalmazott biztonsági intézkedések és elemek ellenőrzését.

### *1.5.2. A bejelentés-köteles szolgáltatást nyújtó intézmény incidens bejelentési kötelezettségei*

A bejelentés- köteles szolgáltatást nyújtó haladéktalanul bejelenti az eseménykezelő központnak azon biztonsági eseményeket, melyek:

- szolgáltatásának elektronikus információs rendszerein következtek be,
- jelentős hatást gyakoroltak az EU-n belül kínált szolgáltatás gyakorlására.

Egy esemény hatásának jelentőségének megállapításához szükséges szempontok és paraméterek az EU-s elvárásokkal azonosak:

» „a digitális szolgáltató által nyújtott szolgáltatás több mint 5 000 000 felhasználóóra erejéig nem érhető el, ahol a „felhasználóóra" kifejezés az esemény által hatvan perces időszak alatt az Unió területén érintett felhasználók számát jelenti;

» az esemény következtében sérül a tárolt, továbbított vagy feldolgozott adatok vagy a digitális szolgáltató hálózati és információs rendszere által nyújtott vagy azon keresztül elérhető, kapcsolódó szolgáltatások sértetlensége, hitelessége vagy bizalmassága, és ez Unió-szerte több mint 100 000 felhasználót érint;

» az esemény veszélyt jelent a közvédelemre, a közbiztonságra vagy az emberi életre;

» az esemény az Unió területén legalább egy felhasználó számára 1 000 000 EUR-t meghaladó kárt okoz;" (Forrás: A Bizottság (EU) 2018/151 végrehajtási rendelete a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról, 4. cikk a)-d) bekezdések).

A biztonsági esemény bejelentésére vonatkozó kötelezettség csak akkor áll fenn a szolgáltatóval szemben, ha rendelkezésére állnak azon adatok melyekkel fel tudja mérni az esemény hatását a fentiek szerint.

A biztonsági eseményről szóló bejelentésnek a bejelentés-köteles szolgáltatók biztonságára vonatkozó Korm. rendelet[11], valamint az eseménykezelő központok feladat- és hatásköréről szóló Korm. rendelet[12] alapján az alábbi adatokat kell tartalmaznia:

- a biztonsági esemény által érintett felhasználók száma
- a biztonsági esemény időtartalma
- a biztonsági esemény földrajzi kiterjedése
- a szolgáltatás működésében okozott zavar mértéke,
- gazdasági és társadalmi tevékenységekre gyakorolt hatása
- az esemény kezelésére kijelölt kapcsolattartó személy elérhetőségei
- közvetítő szolgáltató igénybevétele esetén annak neve és elérhetősége.

Az eseménykezelő központ szükség esetén a biztonsági esemény kezelésében és vizsgálatában is tud operatív vagy elméleti támogatást nyújtani az intézmény számára. A bejelentett esemény vizsgálata után készült összefoglaló jelentést a CSIRT átadhatja az illetékes hatóságnak hatósági eljárás megindítása céljából.

### *1.5.3. Illetékes hatóság feladatai és hatásköre:*

A hatóság a beérkezett regisztrációk alapján nyilvántartást vezet, melynek felülvizsgálata és folyamatos frissítése is a feladatai között szerepel.

A hatóság kötelezheti a szolgáltatót, hogy gondoskodjon a megfelelő szolgáltatási szint biztosításáról, a biztonsági események megelőzéséről, bejelentéséről, illetve kezeléséről. Szükség esetén kötelezheti a szolgáltatót a nyilvánosság tájékoztatására, vagy akár maga a hatóság is megteheti a tájékoztatást.

A hatóság ellenőrzést végezhet a szolgáltatók kötelezettségeinek teljesítésének ellenőrzése érdekében az eseménykezelő központtól vagy bármely más forrásból kapott információk alapján. A hatóság az eljárás során jogosult önállóan vagy más hatósággal együtt helyszíni ellenőrzést tartani a bejelentés-köteles szolgáltatást nyújtó szolgáltatónál, mely során bármely elektronikus információbiztonsággal kapcsolatos okiratot, vagy eszközt megismerhet. A helyszíni vizsgálat során jogosult a hatóság információtechnológiai műszaki vizsgálatokat is végezni.

A vizsgálat során a hatóság figyelembe veszi a független képesített ellenőr által készített vizsgálatot, illetve elfogadja az európai vagy nemzetközileg elfogadott tanúsítványok, akkreditációk alátámasztását.

A hatóság a helyszíni vizsgálat eredményeként további intézkedéseket (elhárítási és megelőzési egyaránt) javasolhat, illetve dönthet a nyilvánosság tájékoztatása mellett. A javasolt intézkedések a hiányosságok súlyától függően azonnali intézkedést vagy megadott határidőre megvalósítást igényelhetnek.

**A hatóság meghatározott jogszabálysértések esetén (Ekertv. 6/C §) bírságot szabhat ki a szolgáltatóra (az 1. mellékeltnek megfelelően):**

- regisztráció elmulasztása esetén
- adatváltozás bejelentésének elmulasztása esetén,
- kockázatelemzés hiánya esetén

[11] 270/2018. számú információs társadalommal összefüggő szolgáltatásokra vonatkozó Korm. rendelet

[12] 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

– kockázatokkal arányos intézkedések bevezetésének és alkalmazásának hiánya esetén
– kockázatelemzés és a biztonsági intézkedések éves dokumentált felülvizsgálatának elmaradása, valamint a hiányosságok okán szükségessé vált módosítások elmulasztása esetén
– a hatóság határozatában foglalt intézkedési javaslatok nem teljesítése esetén.

A rendelet kiemeli, hogy a bírság kifizetése nem mentesíti a szolgáltatót a szabálytalanság megszüntetésének kötelezettsége alól, illetve a határozat közlésétől számított 2 hónap múlva új bírság szabható ki a hiányosságra, ha továbbra sem történt a megszüntetését célzó intézkedés.

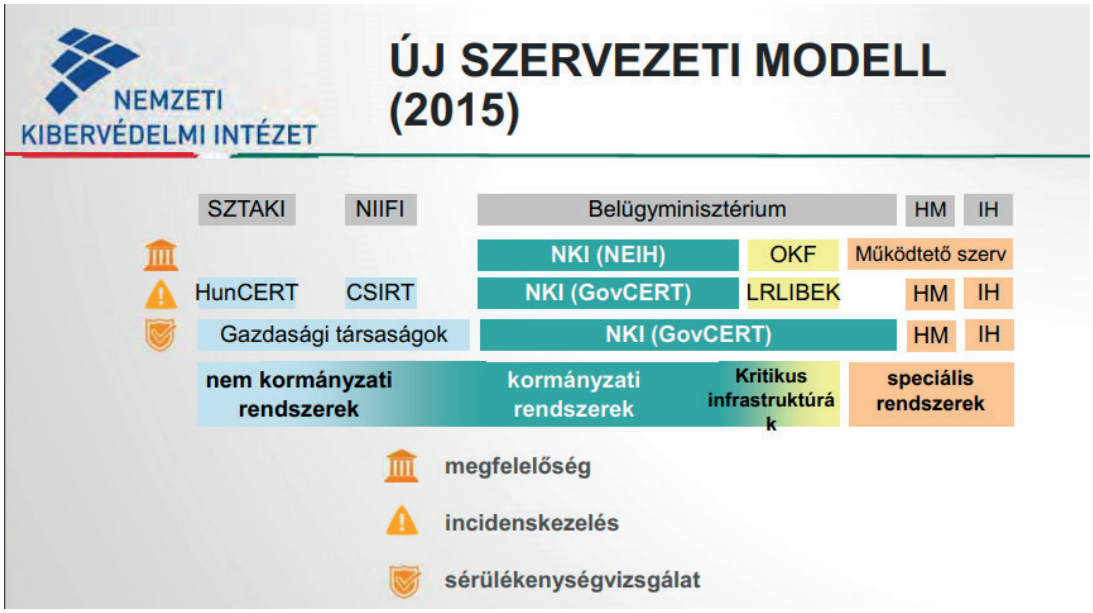
A rendelet alapján a kiszabható bírság minimum és maximum összegekben van meghatározva minden jogsértésre vonatkozóan, melynek mértéke ötvenezer forinttól egészen ötmillió forintig terjedhet.

A hatóság együttműködik a többi tagállam illetékes hatóságával abban az esetben, ha egy bejelentés-köteles szolgáltató központi ügyvezetésének helye másik tagállamban van.

## 1.6. A magyar kibervédemi szervezetrendszer változásai

A magyarországi kiberbiztonsági politika és szabályrendszer kialakításakor létrehozott kibervédelmi szervezetrendszer az évek folyamán folyamatos fejlődésen, átalakításon ment keresztül.

A kiberbiztonsági szervezetrendszer első jelentős változását 2015-ben figyelhettük meg, amikor a korábbi széttagolt, sok szereplő gyors és hatékony együttműködését igénylő szervezetrendszer felülvizsgálatának köszönhetően a Belügyminisztérium felügyelete alatt összpontosuló szervezetrendszer került kialakításra. Ezen folyamat részeként jött létre 2015. október 1-én a Nemzetbiztonsági Szakszolgálaton belül a Nemzeti Kibervédelmi Intézet, a korábbi Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), a Kormányzati Eseménykezelő Központ (GovCERT), valamint a sérülékenységvizsgálatokért felelős szervezeti egység (korábban: CDMA) összevonásával.




*2. ábra: 2015-ben létrejött szervezetrendszer*
*Forrás: Tikos Anita: Nemzeti Kibervédelmi Intézet bemutatása. Az információbiztonság törvényi szabályozása (2017.február 27.) in: Informatikai Szakbizottság anyagai (*https://eoq.hu/szakb/11/inf170227.pdf *) (letöltve: 2019. július 30.)*

2017. első felében pedig a honvédelmi ágazat elektronikus információs rendszereinek biztonságáért felelős hatóságot és eseménykezelő központot (HÁEIBEK) hivatalosan is létrehozta a honvédelmi célú elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóság és a honvédelmi ágazati elektronikus információbiztonsági eseménykezelő központ feladatainak végrehajtásáról, valamint a sérülékenységvizsgálat lefolytatásának szabályairól szóló 15/2017. (IV. 28.) HM utasítás.

## *1.6.1. A NIS irányelv által megfogalmazott intézményi feladatok, felhatalmazások alakulása 2019. január 1 előtt*

Ahogy fentebb a hálózati és információs rendszerek biztonságáról szóló irányelv fejezetben láthattuk, a NIS irányelv számos új hatósági és eseménykezelő központokra (CSIRT) vonatkozó szerepkört, nemzeti és EU-s szintű feladatot fogalmazott meg.

Az irányelvnek a magyar jogrendbe történő átültetése jelentősen meghatározta azt is, hogy a NIS szerinti feladatok és szerepkörök milyen módon kerüljenek kiosztásra, meghatározásra. A NIS irányelv rendelkezéseinek hazai implementációjának 2018 második felében megtörtént felülvizsgálata és módosítása (bejelentés-köteles szolgáltatókra vonatkozó rendelkezések) jelentős hatást gyakorolt az intézményrendszerre és a feladatok és szerepkörök alakulására is, így az intézményrendszerben bekövetkezett változásokat is ennek megfelelően, 2 részletben mutatom be.

### 1.6.1.1. Alapvető szolgáltatások a biztonságának felügyeletéért és támogatásáért felelős intézmények

Mivel az NIS irányelv szerinti alapvető szolgáltatásokra vonatkozó előírások és szabályok a létfontosságú rendszerek és létesítményeket szabályozó keretrendszerbe történő beillesztése mellett döntött a kormányzat, így egyértelmű volt, hogy az alapvető szolgáltatások felügyeletéért felelős hatóság és eseménykezelésükért felelős eseménykezelő központ is meg fog egyezni a létfontosságú rendszerek és létesítmények esetében felhatalmazott intézményekkel.

Ezért az alapvető szolgáltatók esetében több hatóság kinevezhető feladatuk és felhatalmazásuk alapján egy szektorra vonatkozóan. Ennek megfelelően van a felügyeletért és nyilvántartásért felelős hatóság, mely minden létfontosságú rendszerre és létesítményre, illetve a NIS irányelv átültetése óta az alapvető szolgáltatásokra vonatkozóan az Országos Katasztrófavédelmi Felügyelet (OKF) hatósága. Ezen kívül vannak még kijelölő és javaslattevő hatóságok is, melyek szektoronként, vagy ágazatonként eltérők. Ezen hatósági jogkörök az ágazatspecifikus jogszabályokban kerülnek kijelölésre, meghatározásra.

Az ágazati kijelölő hatóságok a létfontosságú rendszerek és az alapvető szolgáltatást nyújtó intézmények esetében egyaránt, minden ágazat és alágazat esetben a kijelöléshez megfelelő ismerettel rendelkező intézmények (minisztérium, hatóság, felügyelet vagy akár hivatal).

Az alapvető szolgáltatási szektorok kijelölő hatóságai az alábbi táblázatban foglaltak szerinti intézmények.

| ágazat | alágazat (ha eltérő a hatóság) | kijelölő hatóság |
|---|---|---|
| Energia | villamos energia | Magyar Energetikai és Közműszabályozási Hivatal |
| | a kőolaj és földgázipar | bányafelügyelet |
| | kőolaj-feldolgozás és kőolajtermék-tárolás | fővárosi és megyei kormányhivatal mérésügyi feladatkörében eljáró megyeszékhely szerinti járási hivatal |
| Banki szolgáltatások | | a pénz-, tőke- és biztosítási piac szabályozásáért felelős miniszter |
| Pénzügyi piaci infrastruktúrák | | a pénz-, tőke- és biztosítási piac szabályozásáért felelős miniszter |
| Egészségügy | | egészségügyért felelős miniszter |
| Digitális infrastruktúra | | Nemzeti Média- és Hírközlési Hatóság |
| Ivóvíz ellátás és elosztás ágazat | | területileg illetékes, vízügyi hatáskörrel rendelkező katasztrófavédelmi igazgatóság |

*2.táblázat: Az alapvető szolgáltatási szektorokban a szolgáltató kijelölés során eljáró hatóságok*
*Forrás: A táblázatot a szerző készítette a szektorális végrehajtási rendeletek rendelkezései alapján*

Egyes ágazatok javaslattevő jogosultsággal rendelkező hatóságokat is megnevez a szabályozás a létfontosságú rendszerelemekre vonatkozóan, mely jogosultságok így (ellenkező rendelkezés hiányában) az alapvető szolgáltatások kijelölés során is fennállnak. Javaslattevő hatósági felhatalmazással rendelkezik például a víz ágazat esetében a területi vízügyi igazgatóság, a pénzügyi ágazat esetében a Magyar Nemzeti Bank, az egészségügyi szektor alágazataiban pedig az Állami Egészségügyi Ellátó Központ, az Országos Mentőszolgálat, illetve az országos tisztifőorvos.

Az alapvető szolgáltatások felügyeletéért és a nyilvántartás vezetéséért felelős hatósági jogköröket és felelősségeket jogszabályi szinten is rögzíteni kellett, melynek az elektronikus információs rendszerek felügyeletéről szóló 187/2015. (VII. 13.) számú Korm. rendelet[13] 9. pontjának kiegészítésével tett eleget Magyarország.

Ezen rendelkezések szerint az OKF-nek mint hatóságnak az új feladata:

- a nyilvánosság tájékoztatása (alapvető szolgáltatást ért) biztonsági esemény esetén,
- Egyedüli Kapcsolattartó pont tájékoztatása szolgáltatók azonosítását biztosító nemzeti intézkedésekről, szolgáltatói jegyzékről, valamint az adott szolgáltatásra támaszkodó felhasználók számáról.

A létfontosságú rendszerek és létesítmények eseménykezelő központjának az Ibtv.19.§ (2) bekezdésében foglaltak, valamint a 185/2015. (VII. 13.) Korm. rendelet 6.§ (3) bekezdésének rendelkezései az Országos Katasztrófavédelmi Főigazgatóság Létfontosságú Rendszerek és Létesítmények Informatikai Eseménykezelő Központját (LRLIBEK) jelölik ki, eszerint a 185/2015. (VII. 13.) Korm. rendelet 6.§ (3) bekezdése rendelkezései kiegészítésének megfelelően az alapvető szolgáltatókra vonatkozóan is az LRLIBEK lett a kijelölt eseménykezelő központ.

[13] 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

Ezen felhatalmazás nem okozott jelentős eltéréseket az eseménykezelésben a korábbiakhoz képest. Az új felhatalmazás kapcsán felmerülő fő kihívásként inkább a NIS irányelv 1. számú mellékletében megfogalmazott követelményeknek való megfelelést emelném ki.

#### 1.6.1.2. Bejelentés-köteles szolgáltatást nyújtókra vonatkozó rendelkezések nemzeti átültetéséből fakadó változások az intézmények hatáskörében és feladataiban

A bejelentés-köteles szolgáltatást nyújtók az irányelvet megelőző időszakban egyetlen felügyeleti vagy eseménykezelési központhoz sem kötődtek.

Ezért a bejelentés-köteles szolgáltatást nyújtókról szóló 410/2017. (XII. 15.) Korm. rendelet az Országos Katasztrófavédelmi Főigazgatóságot jelölte ki a bejelentés-köteles szolgáltatások hatóságaként (4. § (1)-ben), valamint az eseménykezelő központjaként (2. § (1)) egyaránt.

Ezen kijelölések új feladatot nem jelentettek az OKF számára, maximum a meglévő eljárásait egészítették ki újabb szempontokkal vagy vizsgálandó kérdésekkel, illetve a létfontosságú rendszerekhez képest teljesen más természetű szolgáltatásokat nyújtó intézményekkel való hatékony kooperáció és új nézőpontok megtalálása jelentett kihívást a feladatra kijelölt OKF számára.

#### 1.6.1.3. A NIS irányelvből fakadó EU-s szintű feladatok ellátásáért felelő intézmény

A NIS irányelv rendelkezései által létrehozott EU-s szintű együttműködési mechanizmusokat elősegítő funkciókra a Nemzeti Kibervédelmi Intézet szervezeti egységei kaptak jogszabályi felhatalmazást.

Ennek megfelelően a 185/2015. (VII. 13.) Korm. rendelet 5. § (1) bekezdés e) pont felhatalmazása alapján a Nemzeti Kibervédelmi Intézet eseménykezelő központja (GovCERT) képviseli Magyarországot a CSIRT-ek hálózatában és annak munkacsoportjaiban.

A 187/2015. (VII. 13.) Korm. rendelet 6. § (1) bekezdés g.) pontba foglalt felhatalmazás alapján a Nemzeti Kibervédelmi Intézet keretén belül működő Elektronikus Információbiztonsági Hatóság (NEIH) képviseli Magyarországot a hatósági együttműködést biztosító együttműködési csoportban és annak munkacsoportjaiban. Felhatalmazást ad továbbá a Nemzeti Kibervédelmi Intézet hatóságának (NEIH) a 187/2015. (VII.13) Korm. rendelet a NIS irányelv részletszabályait biztosító végrehajtási rendeletek megalkotásáért felelős NIS szakértői csoport munkájában való részvételre is.

A határon átnyúló incidensek esetén megvalósuló együttműködés elősegítéséért és koordinálásáért felelős Egyetlen Kapcsolattartó Pont (SPOC) funkció betöltésére is a Nemzeti Kibervédelmi Intézet hatóságát, a NEIH-et hatalmazta fel az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 12/A pontja.

A nemzeti kapcsolattartó pont fő feladata az Európai Unión belüli nagy hatású kiber-incidensek hazai koordinálása, valamint az incidensekkel kapcsolatos jelentések fogadása, küldése az EU-s tagállamokban lévő partnerszervezetek irányába.

Ezen felül, a jogszabályban kapott felhatalmazás szerint a NEIH az egyetlen kapcsolattartó pont funkció betöltése során az alábbi feladatokat látja el:

- együttműködik az eseménykezelő központtal az Irányelvnek való megfelelés vizsgálata során, melynek eredményeit megküldi a Bizottságnak,
- a jelentős hatású biztonsági eseményekről (NIS szerinti szektorok esetében) jelentés küld az együttműködési csoportnak,
- szükség esetén együttműködik a rendvédelmi szervekkel, illetve a Nemzeti Adatvédelmi és Információszabadság Hatósággal,

– a NIS előírásai szerinti információkról az Irányelvben megadott időközönként tájékoztatást küld az Európai Bizottságnak (alapvető szolgáltatók jegyzéke, szereplők jelentősége, adott szolgáltatásra támaszkodó felhasználók száma, az eseményközpontok hatáskörének és eljárásainak bemutatása).

A NIS irányelvből adódó összes EU-s együttműködéshez és információmegosztáshoz kötődő feladatoknak egy helyen (az NKI-nél) való koncentrálása egy központosított, egykapus rendszert hozott létre az EU intézményeivel, tagállamok szervezeteivel való kapcsolattartása, kommunikációra vonatkozóan.

### *1.6.2. A 2019. január 1-től (a jogszabályi felülvizsgálat okán) hatályba lépő intézményi változások*

A bejelentés- köteles szolgáltatókra vonatkozó 410/2017. (XII. 15.) Korm. rendelet előírásainak felülvizsgálata és kiegészítése során 2018-ban az ezen szolgáltatók biztonságáért és eseménykezeléséért felelős intézményi felhatalmazását is módosította a kormányzat.

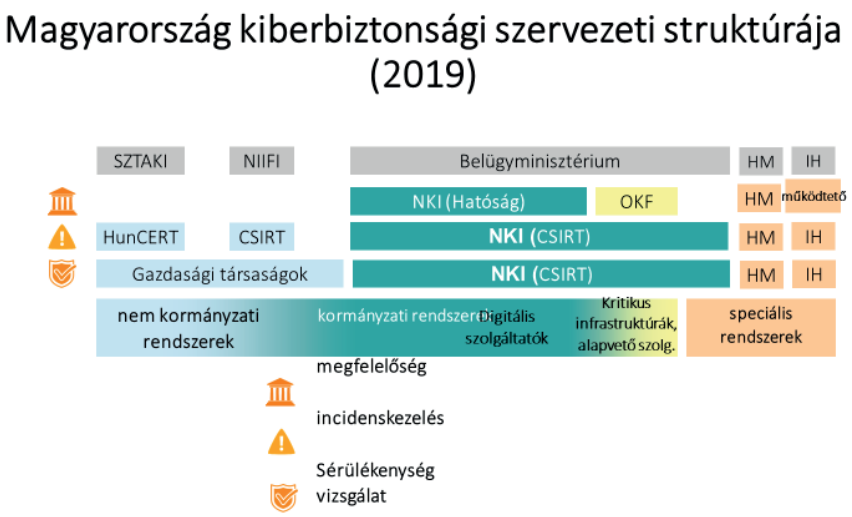
A 410/2017-es Korm. rendeletet felváltó 270/2018. (XII. 20.) Korm. rendelet már a Nemzeti Kibervédelmi Intézet hatóságát és eseménykezelő központját hatalmazza fel a bejelentés-köteles szolgáltatások hatósági felügyeletére és eseménykezelésére.

Az implementáció felülvizsgálata során fontos szempont lehetett az intézményrendszer és a felhatalmazások felülvizsgálatára az, hogy a NIS irányelv CSIRT szolgáltatásokra és képességekre vonatkozó ambiciózus előírásainak (irányelv 1. melléklet) a NIS irányelv szerinti szektorokért (de legalább az alapvető szolgáltatásokért) felelős OKF LRLIBEK-nek, valamint az EU-s CSIRT együttműködésre felhatalmazott GovCERT-nek egyaránt meg kellene felelniük. Ez komoly (költségvetésbeli és szakmai) ráfordítást igényelt volna a felelős Belügyminisztériumtól, hiszen mindkét érintett intézmény annak háttérintézményeként működik. A feladat és funkció központosításával lehetőség nyílik minden fejlesztést és forrást célzottan egyetlen intézmény fejlesztésére fordítani, így egy versenyképes, modern, a folyamatosan változó kihívásoknak megfelelni képest eseménykezelő központot létrehozni.

Valószínűleg ez az érv is közrejátszhatott abban, hogy a bejelentés-köteles szolgáltatásokról szóló szabályozás és felelősségi körök módosításával egyidőben, az alapvető szolgáltatások és a létfontosságú rendszerek és létesítmények eseménykezelésére vonatkozó felelősségeket és felhatalmazást is módosította a kormányzat, melynek következtében 2019. január 1-től a Nemzeti Kibervédelmi Intézet eseménykezelő központját hatalmazta fel a jogszabály a létfontosságú rendszerek és létesítmények, valamint az alapvető szolgáltatások összes ágazatának (és alágazatának) eseménykezelési feladatának ellátására.

Ezen változásoknak köszönhetően a Belügyminisztérium hatáskörébe utalt összes szektor (létfontosságú rendszerek és létesítmények; alapvető szolgáltatások, bejelentés-köteles szolgáltatások és az állami és önkormányzati intézmények) eseménykezelési feladata az NKI eseménykezelő központjánál összpontosul.

Az OKF eseménykezelő központjától elvont feladatok és hatáskörök jelentősen megváltoztatták Magyarország kiberbiztonsági szervezeti struktúráját, ahogy ezt a lenti ábra is mutatja.




*3. ábra: Magyarország kiberbiztonsági struktúrája (2019)*
*Forrás: a szerző a szervezeti ábrát a 2015-ben létrejött új szervezeti modell című ábra alapján, a változások átvezetésével készítette*

Eredeti forrás: Tikos Anita: Nemzeti Kibervédelmi Intézet bemutatása. Az információbiztonság törvényi szabályozása (2017.február 27.) in: Informatikai Szakbizottság anyagai (https://eoq.hu/szakb/11/inf170227.pdf ) (letöltve: 2019. július 30.)

Ahogy a fenti ábrán is láthatjuk az Országos Katasztrófavédelmi Főigazgatóság Eseménykezelő Központját (LRLIBEK) a feladatainak és hatáskörének átruházásával tulajdonképpen megszüntették a döntéshozók.

A fent említett szervezeti átalakulás olyan jelentős mértékű volt, hogy a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, az Ibtv. és annak végrehajtását segítő (hatósági felügyeletről szóló és eseménykezelő központok feladatairól szóló) Korm. rendeletek rendelkezéseinek (intézmények feladatai, felhatalmazásai, jogkörei, szervezetek közötti együttműködési és információmegosztási szabályok stb.) módosítása is szükségessé vált.

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 olyan jelentős mértékű módosítást igényelt, hogy hatályon kívül helyezték, és a módosított szabályokat az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet keretében fogalmazták újra.

## 1.7. A Nemzeti Kibervédelmi Intézet változó hatásköre

Ahogy a fenti fejezetekben láthattuk, a 2015. október 1-én a Nemzetbiztonsági Szakszolgálat keretén belül létrejött Nemzeti Kibervédelmi Intézet feladatai és felhatalmazása az elmúlt évek jogszabályi változásai során folyamatosan növekednek.

A NIS irányelv átültetésének első szakaszában a Nemzeti Kibervédelmi Intézet felhatalmazást kapott az EU-s együttműködési mechanizmusok (CSIRT-ek hálózata, együttműködési csoport, NIS szakértői csoport; egyedüli kapcsolattartó pont) keretében megvalósuló együttműködésekben Ma-

gyarország képviseletére, mely létrehozta az EU szervezetei és tagállami intézményei felé betartandó egykapus együttműködési és kommunikációs modellt, melyben az NKI kapta a vezető szerepet.

Az NKI ezt megelőzően is aktívan részt vett a különböző nemzetközi együttműködésekben a CSIRT közösségektől, a kiberbiztonsági regionális együttműködéseken át (Közép-Európai Kiberbiztonsági Platform-CECSP) a bilaterális kapcsolatokig, valamint számos bilaterális együttműködéssel is rendelkezett az EU-s intézményekkel (CERT-EU; ENISA; Európai Bizottság), de a NIS irányelv szerinti együttműködési mechanizmusokban való részvételre kapott felhatalmazása jelentősen megerősíti és részletesen meghatározza az EU-s szintű együttműködésben betöltött vezető szerepét.

2018. második felében, a NIS irányelv átültetésének felülvizsgálata, pontosítása és kiegészítése során a Belügyminisztérium hatáskörébe tartozó összes kiberbiztonsági szerepkör és szabályozás ellenőrzésen esett át, melynek eredményeképp jelentős intézményrendszert érintő változások kerültek végrehajtásra, mely maradéktalanul az NKI szerepének és felhatalmazásának növekedését jelentette:

- bejelentés-köteles szolgáltatások felügyeletéért felelős hatósági jogkört az OKF hatósági jogköreiből kiemelték és az NKI hatósága (NEIH) kapta meg a felhatalmazását,
- a bejelentés-köteles szolgáltatások információbiztonsági operatív támogatásáért felelős eseménykezelő központi funkciót az OKF hatósága helyett 2019. január 1-től az NKI eseménykezelő központja látja el,
- a létfontosságú rendszerek és létesítmények információbiztonsági, operatív támogatásáért felelős eseménykezelő központi funkciót az OKF hatósága helyett 2019. január 1-től az NKI eseménykezelő központja látja el,
- az alapvető szolgáltatások eseménykezelő központ általi operatív támogatását 2019. január 1-től az NKI eseménykezelő központja látja el az OKF eseménykezelő központja helyett.

Az NKI hatósága - a nemzetközi szerepein, feladatain, valamint a bejelentés-köteles szolgáltatók felügyeleti hatósági jogkörén túl - a felülvizsgált és új jogszabályoknak köszönhetően egy „új" hatósági eszköz, szankció alkalmazására is felhatalmazást kapott, mégpedig a bírság kiszabására nemcsak a bejelentés-köteles szolgáltatások vonatkozásában, hanem a költségvetési szervek esetében is a 2013. évi L. tv. 16.§ (3) d.) pontjának megfelelően.

A bejelentés-köteles szolgáltatások esetében a hatósági és eseménykezelői feladatok és felelősségek egy kézben tartásával az NKI-nak lehetősége nyílik egy komplex és sokrétű támogatás nyújtására ezen szolgáltatások számára, az állami és önkormányzati szervek esetében már megteremtett, teljes életciklust végig kísérő szolgáltatás portfólió mintájára.

Egyértelműen láthatjuk, hogy fent felsorolt nagyvolumenű változásoknak köszönhetően a Nemzeti Kibervédelmi Intézet központi szerepköre tovább növekedett, mellyel mára egy jelentős feladat és jogkörökkel bíró kvázi csúcsszervet hoztak létre a döntéshozók. Mivel az NKI eseménykezelő központja és hatósága immár nemcsak az állami és kormányzati szektorban lát el feladatokat, így meg kellett változtatni az elnevezésüket is, melyet természetesen át kellett vezetni a jogszabályokban is. Ezek a változások az alábbiak szerint valósultak meg:

A korábbi Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) neve egyszerűsödött, tehát a jogszabályok egyszerűen az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóságként, vagy az Ekertv. szerinti hatóságként hivatkoznak rá. Mindemellett fontosnak találom kiemelni, hogy a hatósági feladat ellátására pedig a Nemzetbiztonsági Szakszolgálatot jelölik ki a jogszabályok.

A Kormányzati Eseménykezelő Központ (GovCERT) esetében is hasonló névváltozást figyelhetünk meg, hiszen a 2013. évi L. törvény 19. § (1) bekezdésében, már úgy hivatkozik a korábbi GovCERT-re, mint „a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter irányítása alatt működtetett eseménykezelő központ."[14]

[14] (2013. évi L. törvény 19. § (1) alapján

Láthatjuk, hogy a Nemzeti Kibervédelmi Intézet neve továbbra sem jelenik meg egyetlen jogszabályban sem, minden esetben csak a Nemzetbiztonsági Szakszolgálat (vagy polgári nemzetbiztonsági szolgálatok) hatósága vagy eseménykezelő központjaként kerül azonosításra.

A fent bemutatott több különböző megnevezéseket/hivatkozásokat összegezve az új szervezeti és jogszabályi környezetnek köszönhetően most már Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet megnevezést használja hivatalosan az intézet, melynek keretében - immár minden egyéb jelző nélkül - az eseménykezelő központ, vagy CSIRT és a hatóság működik.

A CSIRT feladatok és funkciók egy helyre való összpontosításával Magyarország a NIS irányelv 1. mellékeltében megfogalmazott CSIRT kötelezettségeknek és szolgáltatási elvárásoknak szinte maradéktalanul eleget tesz határidőre az NKI CSIRT által.

A megnövekedett hatáskörének köszönhetően a jövőben az NKI-nak lehetősége nyílik az ágazatokon átívelő biztonsági eseményekre vonatkozó tendenciák és összefüggések azonosítására az alábbi ágazatokban:

- a létfontosságú rendszerek és létesítmények,
- alapvető szolgáltatók,
- bejelentés köteles szolgáltatások,
- állami és önkormányzati intézmények, valamint
- a központosított informatikai és elektronikus hírközlési szolgáltatók.

Ezen szektorokban összegyűjtött adatok hozzájárulnak a magyar és a nemzetközi információbiztonsági tendenciákról és irányokról készítendő elemzésekhez, jelentésekhez, valamint az egyedüli kapcsolattartó pontként végzendő nemzeti és koordinációs feladatok hatékony és gyors ellátásához.

## 1.8. Összegzés

Összességében elmondhatjuk, hogy Magyarországon az irányelv implementációja nem tette szükségessé teljesen új jogszabályi keretrendszer bevezetését a magyar kibertérre vonatkozóan, hiszen lehetőség nyílt majdnem minden kérdéskörben a meglévő szabályozási és intézményi keretrendszerbe való integrációval elvégezni az irányelv magyarországi átültetését.

Az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó előírások átültetésére hazánkban a létfontosságú rendszerelemekre vonatkozó szabályozás kiegészítésével, többletfeladatok minimalizálásával került sor. Ezen megközelítésnek köszönhetően az alapvető szolgáltatást nyújtó intézmények a létfontosságú rendszerelemek szűkebb halmazaként jelennek meg a nemzeti szabályozásban, mely szolgáltatók esetében a jogalkotók célja, hogy magasabb információbiztonsági szintet érhessen el az általuk nyújtott szolgáltatások folyamatossága.

Az alapvető szolgáltatásokra vonatkozóan nem került kidolgozásra a létfontosságú rendszerekre vonatkozó biztonsági követelményekhez képest szigorúbb vagy részletesebb biztonsági követelmény, így ilyen módon nem rendelkezik a magasabb biztonsági szint eléréséhez szükséges követelményekkel.

A digitális szolgáltatók, vagy a magyar jogszabályok szerint a bejelentés-köteles szolgáltatások esetében Magyarország új jogszabály (Korm. rendelet) kidolgozásával tett eleget az EU-s kötelezettségeinek. Ezzel egy mindeddig felügyelet és szakmai támogatás nélkül fejlődő és terjeszkedő szolgáltatói csoporttal kezdte meg a közös munkát, és a kibertérben megjelenő kihívásokra és fenyegetésekre való válaszok kidolgozását a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet.

A bejelentés- köteles szolgáltatások jelentősége és piaci meghatározó szerepe folyamatosan növekszik, illetve a digitális szolgáltatások alkalmazása is egyre elterjedtebbé válik az alapvető szolgáltatásokat nyújtó szektorokban, intézményekben. Várhatóan az ezen szektorokat összekötő üzleti kapocs számos új kihívást fog jelenteni mind a felügyeleti és eseménykezelési, mind pedig a piaci

szereplők számára melynek köszönhetően a kialakult szabályokat és eljárásokat a szektorokon átívelő folyamatokra, eseményekre is ki kell majd terjeszteni.

A 2019. január 1-től bekövetkezett változásoknak köszönhetően jelentősen átalakult Magyarország kiberbiztonsági intézményrendszere, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet jelentősége tovább erősödött, feladatai és jogkörei pedig jelentősen kibővültek (hiszen a Belügyminisztérium felügyelete alá tartozó összes szektor eseménykezeléséért az NKI CSIRT-je lett a felelős).

Az így kialakult, egyközpontú, egyetlen intézményhez koncentrált szervezeti modell sok lehetőséget hordoz magában (mint például a szektorokon átívelő fenyegetések hatékony kezelése, átfogó kiberbiztonsági helyzet elemzések, stb.), melyeknek kiaknázása és az új portfólió felépítése folyamatosan zajlik.

Átültetését és rendelkezéseinek alkalmazását követően is számos feladatot jelent még a NIS irányelv a tagállamokban, főként az előírások végrehajtásáért felelős intézmények számára, mint például az évenkénti incidens-összefoglaló jelentés elkészítése, a kijelölések kétévenkénti felülvizsgálata, valamint az együttműködési mechanizmusokban való aktív részvétel.

A NIS irányelv átültetése és alkalmazása során számos kérdés merült az érintett szereplők részéről, melyre a szakértői csoportok, valamint az ENISA egyaránt keresi a lehetséges válaszokat, megoldásokat. Ilyen például a fentebb említett alapvető szolgáltatók és digitális szolgáltatók közötti összefüggések és függőségek kérdése, melyet az ENISA is a napirendjére tűzött és kidolgozta a Jógyakorlatok az alapvető szolgáltatásokat nyújtó és a digitális szolgáltatásokat nyújtó intézmények közötti kölcsönös függőségekről című tanulmányt[15].

Fontos kiemelni, hogy a NIS irányelvnek megfelelő átfogó kiberbiztonsági felkészültség és képességnövelési feladatok mellett folyamatban van a digitális technológiától leginkább függő szektorokban (pénzügyi szektor, közlekedési szektor, valamint az energiaszektor) a szektorális kiberbiztonsági előírások megfogalmazása, továbbfejlesztése, valamint a NIS irányelv előírásainak szektorspecifikus részletszabályai fejlesztésére vonatkozó célitűzések megvalósítása.

Az Európai Bizottság a NIS irányelv hivatalos lapban történő megjelenését követően sem tétlenkedett: 2017. szeptemberében az EU-s kiberstratégia és a Digitális Egységes Piac stratégia kiértékelésének és felülvizsgálatának eredményeként bemutatta az új célkitűzéseket előíró ún. kibercsomag[16] javaslatot. A csomag célja, hogy válaszokat, mechanizmusokat és jogi biztosítékokat dolgozzon ki a megnövekedett kiberfenyegetésekre, és az egységes digitális piac megteremtésének még meglévő akadályaira vonatkozóan. A kibercsomag tulajdonképpen egy átfogó intézkedés- és célkitűzésgyűjtemény, mely komplex egységként a kiberbiztonság minden aspektusára (a tudatosítástól, a fejlesztéseken, tanúsításon, incidenskezelésen, szektorális szabályozásokon, K+F célkitűzéseken, kiberdiplomácián és a válságkezelésen keresztül a bűnüldözésig és az igazságszolgálttatásig) kiterjed.

Jelenleg a NIS irányelv alkalmazásán túl, a csomagban megfogalmazott ambiciózus célkitűzések és jogszabály tervezetek kidolgozása van a kiberbiztonsági szakértők napirendjén, melyet rövidesen az elfogadott intézkedések közösségi és tagállami szintű megvalósításából és alkalmazásából fakadó kihívások fogják felváltani.

---

[15] Good practices on interdependencies between OES and DSPs https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps

[16] Cybersecurity Package: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-MAIN-PART-1.PDF?utm_source=POLITICO.EU&utm_campaign=d9779adddb-EMAIL_CAMPAIGN_2017_09_13&utm_medium=email&utm_term=0_10959edeb5-d9779adddb-189862693

## 1.9. Felhasznált irodalom


- Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság: Hálózati és információbiztonsági feladatok a katasztrófavédelemnél: http://www.katasztrofavedelem.hu/index2.php?pageid=szervezet_hirek&hirid=5613
- Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság: Tájékoztató az alapvető szolgáltatást nyújtó szereplők részére: http://www.katasztrofavedelem.hu/letoltes/filedb/hirek/5613/Tajekoztato_Alapveto_szolgaltatast_nyujto.pdf (letöltve: 2019. 08. 19)
- Digitális Jólét Program 2.0 stratégia: https://digitalisjoletprogram.hu/files/58/f4/58f45e44c4ebd9e53f82f56d5f44c824.pdf (Budapest, 2017. július)
- Dr. Gyömbér Béla: Megjelent Magyarország hálózati és információbiztonsági stratégiája; Budapest, 2019.01.07. https://jogalappal.hu/megjelent-magyarorszag-halozati-es-informaciobiztonsagi-strategiaja/ ( letöltve: 2019. 08.19.)
- ENISA: State-of-play of the transposition of the NIS Directive: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive
- ENISA: Good practices on interdependencies between OES and DSPs (Athén, 2018011.30.) https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps (letöltve: 2019. 08.17.)
- ENISA: Security requirements for DSPs: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers ( Athén, 2017.02.16)
- Európai Bizottság: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak, A kiberbiztonsági irányelv maximális kihasználásának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 114/2016/EU irányelv hatékony végrehajtása felé, Brüsszel, 20170.10.4.
- Nemzeti Kibervédelmi Intézet: Nemzeti Elektronikus Információbiztonsági Hatóság: Bejelentés-köteles szolgáltatásokról : https://nki.gov.hu/hatosag/tartalom/a-bejelentes-koteles-szolgaltatasokrol/
- Nemzeti Kibervédelmi Intézet: Nemzeti Elektronikus Információbiztonsági Hatóság: Bejelentés-köteles szolgáltatók hatósági nyilvántartásba vétele (Ekertv.) ( http://neih.gov.hu/bksz
- Tikos Anita (előadás): Az NKI bemutatása, Óbudai Egyetem, Budapest https://docplayer.hu/47947406-Az-nki-bemutatasa-tikos-anita-nemzeti-kibervedelmi-intezet.html (letöltve: 20190 08.20.)

# 2. MOLNÁR ANNA – AZ EURÓPAI UNIÓ KIBERBIZTONSÁGGAL KAPCSOLATOS TEVÉKENYSÉGE

## 2.1. Bevezetés

Közhelynek számít, hogy az európai társadalmak, a kormányzati és magánszféra egyre inkább függenek a digitális technológiáktól, és így az elektronikus hálózatok és az információs rendszerek mindennapjaik részévé válta. Az elmúlt években a digitális technológia olyan alapvető eszközzé vált, amelyre nem csupán a gazdaság minden ágazata, hanem az életünk szinte minden területe is támaszkodik. Ha ezek közül csak néhányat emelünk is ki, például a villamosenergia-hálózatokat, a közlekedési hálózatokat, a termelési és pénzügyi folyamatokat, illetve az egészségügyi ellátó rendszereket, akkor is jól látható az egymásrautaltság és összefonódás jelentős mértéke.

Mindebből következően a rossz szándékú kibertevékenységek egyaránt fenyegethetik az európai gazdaságot, a kormányzati vagy védelmi infrastuktúrákat, illetve mindezekkel összefüggésben a demokrácia működését, a szabadságjogokat és az európai értékeket. Európa biztonsága jelentős mértékben függ attól, hogy a tagállamok és az uniós intézményrendszer mennyire tud felkészülni a folyamatosan változó és növekvő intenzitású kiberfenyegetésekkel szemben. Napjainkban számos üzleti modell épül az internet és az információs rendszerek zökkenőmentes működésére. Ezzel párhuzamosan a kiberbűnözés gazdasági hatása folyamatosan növekszik. A zsarolóvírus-támadások mellett számos más fenyegetés is jelentős kihívást jelent az európai gazdasági szereplők számára. A mai számítógépes korban a személyes adatok védelme döntő szerepet játszik a kiberbiztonság megvalósításában.

A kiberbiztonsági események - akár szándékosak, akár véletlenszerűek – jelentős fenyegetést jelentenek a civil infrastruktúra és a katonai kapacitások védelme szempontjából egyaránt. A különböző eredetű, bűnügyi, terrorista vagy állami támogatású támadásokra és balesetekre történő felkészülés sikeressége nem csupán a kiberbiztonság, hanem a biztonság szelesebb értelmezése szempontjából is elengedhetetlen.

## 2.2. Az Európai Unió kiberbiztonsággal összefüggő stratégiai kerete és a szabályozás

### *2.2.1. A 2000-es évektől kirajzolódó stratégiai keret*

A 21. század első évtizedének európai uniós stratégiai dokumentumai még csupán röviden említették a kiberbiztonsággal összefüggő veszélyeket és fenyegetéseket. Az EU első, a 2003-as biztonsági stratégiája már közvetetten utal a kiberbiztonság kérdésére. A Javier Solana, közös kül- és biztonságpolitikai főképviselő irányításával kidolgozott stratégia a terrorista mozgalmakat egyre jobban és egyre kiterjedtebben összekötő elektronikus hálózatok veszélyét emelte ki csupán.[17]

Az Európai Bizottság 2005-ben, a lisszaboni stratégia megvalósításának félidejében átfogó szakpolitikai iránymutatást fektet le és nyilvánosságra hozta az „i2010: Európai Információs Társadalom a növekedésért és foglalkoztatásért" elnevezésű stratégiai dokumentumot. Az új stratégia célja volt, hogy előmozdítsa a nyitott és versenyképes digitális gazdaság kifejlődését, és hangsúlyozza az IKT (információ- és kommunikációtechnológiai) meghatározó szerepét a társadalmi integrációban és az életminőségben. Az dokumentum számos esetben említi a biztonság kérdését. A biztonságos és kiszámítható IKT érdekében megfogalmazza egy, a biztonságos információs társadalmat célzó stratégia kidolgozásának szükségességét.[18]

A 2003-as európai biztonsági stratégia 2008-as felülvizsgálata azonban már rövid alfejezetben is kitért a számítógépes biztonság alapvető kérdéseire. A dokumentum hangsúlyozza, hogy a modern gazdaságok nagymértékben függnek a létfontosságú infrastruktúrától, például az internetettől is. Kiemeli, hogy „az internet alapú bűncselekményekkel a 2006-ban elfogadott, a biztonságos európai információs társadalomra irányuló stratégia foglalkozik. A tagállamok kormány- vagy magántulajdonban levő IT-rendszerei ellen elkövetett támadások következményeként azonban ez új dimenzióként jelenik meg, mint esetleges új gazdasági, politikai és katonai fegyver. E területen több munkára van szükség, egy átfogó uniós megközelítés lehetőségének felderítése, figyelemfelkeltés és a nemzetközi együttműködés fokozása céljából."[19] Az Európai Unió 2010-es belső biztonsági stratégiája az uniót fenyegető számítástechnikai bűnözés veszélyeire hívta fel a figyelmet.[20]

2010 májusában, a lisszaboni stratégia lezárulását követően, az Európai Bizottság útjára indította az Európa 2020 elnevezésű stratégiát, amely a versenyképesség növelése mellett a sérülékenység csökkentését is célozta.[21] Az Európai Bizottság az új stratégia egyik kiemelt kezdeményezéseként - elkészítette az európai digitális menetrendet (DAE). A menetrend célja, hogy az információs és kommunikációs technológiák (IKT) alkalmazása kulcsfontosságú szerepet kapjon az Európa 2020 stratégiában kitűzött célok megvalósítása érdekében. Az Európai Bizottság a tisztességes, nyílt és biztonságos digitális környezet biztosítása érdekében három pillérre építette a digitális egységes piaci stratégiát: 1) Európa-szerte a digitális termékekhez és szolgáltatásokhoz való jobb hozzáférés bizto-

---

17 BIZTONSÁGOS EURÓPA EGY JOBB VILÁGBAN Európai Biztonsági Stratégia, Brüsszel, 2003. december 12. 30. o. https://www.consilium.europa.eu/media/30811/qc7809568huc.pdf

18 A BIZOTTSÁG KÖZLEMÉNYE A TANÁCSNAK, AZ EURÓPAI PRLAMENTNEK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK „i2010: európai információs társadalom a növekedésért és a foglalkoztatásért". Brüsszel, 1.6.2005 COM(2005) 229 végleges, 6. o. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2005)0229_/com_com(2005)0229_hu.pdf

19 JELENTÉS AZ EURÓPAI BIZTONSÁGI STRATÉGIA VÉGREHAJTÁSÁRÓL – A biztonság megteremtése a változó világban, 13-14. o. https://www.consilium.europa.eu/media/30811/qc7809568huc.pdf

20 Az Európai Unió belső biztonsági stratégiája - Az európai biztonsági modell felé. 2010. 7. o. https://www.consilium.europa.eu/media/30741/qc3010313huc.pdf

21 Kovács László: Kiberbiztonság és –stratégiaKiberbiztonság és –stratégia. Dialóg Campus, Budapest, 2018, 85. o. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf

sítása a fogyasztók és a vállalkozások számára, 2) a digitális hálózatok és szolgáltatások fellendülését elősegítő feltételek megteremtése, valamint 3) a digitális gazdaság növekedési potenciáljának maximalizálása.[22] Az EU elsősorban azokra a digitális területen meglévő kihívásokra kívánt megfelelő válaszokat adni, mint például a digitális piac megosztottsága, az interoperabilitási problémák, a kiberbűnözés rendkívül gyors ütemű terjedése, az alacsony szintű K+F és az erre épülő beruházások elmaradása vagy a digitális írástudás régónként eltérő és sok esetben nagyon alacsony szintje. [23]

Az Európai Unió kiberbiztonsággal összefüggő stratégiai dokumentumai

| Év | Európai uniós stratégiai dokumentum |
|---|---|
| 2003 | Európai biztonsági stratégia |
| 2005 | I2010: Európai Információs Társadalom a növekedésért és foglalkoztatásért |
| 2006 | A biztonságos európai információs társadalomra irányuló stratégia |
| 2008 | JELENTÉS AZ EURÓPAI BIZTONSÁGI STRATÉGIA VÉGREHAJTÁSÁRÓL – A biztonság megteremtése a változó világban |
| 2010 | Az Európai Unió belső biztonsági stratégiája - Az európai biztonsági modell felé |
| 2010 | Európai Bizottság: európai digitális menetrend |
| 2013 | Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér |
| 2014 | Európai Unió kibervédelmi szakpolitikai kerete |
| 2015 | A kiberdiplomáciáról szóló tanácsi következtetések |
| 2015 | Az uniós biztonsági stratégia |
| 2016 | Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan |
| 2017 | Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése |
| 2017 | A digitális egységes piaci stratégia |
| 2018 | Európai Unió kibervédelmi szakpolitikai kerete |

*Forrás: Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018,* https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 *26 p.*
*(Az ábra alapján saját szerkesztés)*

## A 2013-as kiberbiztonsági stratégia

Az EU 2012-2013 folyamán kezdte kidolgozni első komprehenzív kiberbiztonsági stratégiáját. Mindez abban az időszakban ment végbe, amikor a fejlett országok ráébredtek a kiberbiztonsági kihívások stratégiai jelentőségére. A NATO-val összehasonlítva, amelynek első stratégiái (2008, 2011) kizárólag saját informatikai hálózatának védelmére szorítkoztak, az EU első stratégiája azonban szinte minden uniós kompetenciába tartozó területre kiterjedt.[24]

[22] Mariusz Maciejewski - Frédéric Gouardères: Az európai digitális menetrend, 05. 2019. Ismertetők az Európai Unióról, Európai Parlament, http://www.europarl.europa.eu/factsheets/hu/sheet/64/az-europai-digitalis-menetrend

[23] Kovács László: Kiberbiztonság és –stratégiaKiberbiztonság és –stratégia. Dialóg Campus, Budapest, 2018, 86. o. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf

[24] Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018, https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 18 p

A 2013-as stratégia „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" címet viselte".[25] A lisszaboni szerződés hatálybalépését követően a közös nyilatkozat elkészítésében az EU külügyi és biztonságpolitikai főképviselője, Chatherine Ashton irányításával az Európai Külügyi Szolgálat és az Európai Bizottság is együttműködött. E dokumentum említette először az EU nemzetközi kiber biztonsági politikáját és kibervédelmi céljait. A stratégia fő céljai és elvei között szerepelt a megbízható, biztonságos és nyílt kiberbiztonsági ökoszisztéma elősegítése.

A stratégia végrehajtásáért elsősorban az Európai Bizottság egyes főigazgatóságai feleltek. Az új kiberterületeken megvalósuló jogalkotásért, az iparpolitikai és a kutatással és fejlesztéssel összefüggő kérdésekért a Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága (DG CNETC) felelt. A kiberbűnüldözéssel összefüggő szakpolitika alakítását és az e területen megvalósuló tagállami együttműködés elősegítését a Migrációs Ügyes és Uniós Belügyek Főigazgatóság (DG HOME) látta el.

A stratégiában megfogalmazott alapelvek összhangban álltak az EU általános alapelveivel és értékeivel: 1) Az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikai világra; 2) az alapvető jogok, a szólásszabadság, a személyes adatok és a magánélet védelme; 3) mindenki számára biztosított hozzáférés; 4) demokratikus és hatékony, számos érdekelt fél bevonásával történő irányítás; 5) közös felelősségünk: biztonság.

A stratégia mindemellett öt prioritást fogalmaz meg: 1) a kibertámadásokkal szembeni ellenálló képesség elérése; 2) a számítástechnikai bűnözés drasztikus csökkentése; 3) a kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében; 4) a kiberbiztonsági ipari és technológiai erőforrások kifejlesztése; 5) az összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása.[26]

### *2.2.2. Az Európai Unió kibervédelmi szakpolitikai kerete (2014)*

A kibervédelem és a nemzetközi kiberpolitikával összefüggő célok megvalósításáért az Európai Külügyi Szolgálat (EKSZ) felel. A KBVP-ről szóló, 2013. decemberi európai tanácsi következtetések szerint a kibervédelmi szakpolitikai keretet az Európai Bizottsággal és az Európai Védelmi Ügynökséggel együtt az EKSZ dolgozta ki. Az EKSZ irányításával 2014-ben elkészült az Európai Unió kibervédelmi szakpolitikai kerete (EU Cyber-Defence Policy Framework).

A dokumentum a következő célokat fogalmazta meg:

1. a közös biztonság- és védelempolitikával összefüggő területeken a tagállamok kibervédelmi képességfejlesztésének támogatása;
2. az uniós szervezetek által használt, közös biztonság- és védelempolitikai kommunikációs hálózatok védelmének fokozása;
3. a civil-katonai együttműködés és a szinergiák előmozdítása az EU szélesebb körű kiberpolitikájával, a vonatkozó uniós intézményekkel és ügynökségekkel, valamint a magánszektorral;
4. a képzési, az oktatási és a gyakorlati lehetőségek javítása
5. az együttműködés fokozása az érintett nemzetközi partnerekkel, különösen a NATO-val.[27]

---

[25] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" JOIN/2013/01 final, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001

[26] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" JOIN/2013/01 final, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001

[27] EU Cyber Defence Policy Framework, Brussels, 18 November 2014, 15585/14 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

### *2.2.3. A hálózati és információs rendszerek biztonságáról szóló irányelv (2016)*

A 2013-as stratégia elfogadását követően az Unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv (NIS) elfogadásával.[28] A 2016 óta hatályos irányelvet az uniós tagállamoknak 2018. május 9-ig kellett átültetniük a nemzeti jogukba, és 2018. november 9-ig azonosítaniuk kellett az alapvető szolgáltatásokat nyújtó szervezeti egységeket.

Az irányelv célja olyan széleskörű intézkedések bevezetése, amelyek az Unió gazdasága és társadalma szempontjából létfontosságú szolgáltatások hálózati és információs rendszereinek biztonsági szintjét (kiberbiztonság) képes növelni. Az irányelvben foglaltak megvalósítása lehetővé teszi, hogy az uniós országok felkészüljenek, és készen álljanak a kibertámadások kezelésére és az azokra való reagálásra. Mindennek érdekében tagállami szinten szükségessé vált az 1) illetékes hatóságok kijelölése; 2) a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) felállítása; és 3) a nemzeti kiberbiztonsági stratégiák elfogadása. A bevezetett intézkedések mind a stratégiai, mind pedig a műszaki szintű együttműködést megerősítik az Európai Unióban. [29]

Az irányelv mindemellett kötelezi az alapvető szolgáltatásokat nyújtó szereplőket és digitális szolgáltatókat arra, hogy megfelelő biztonsági intézkedéseket hozzanak, és tájékoztassák az érintett nemzeti hatóságokat a súlyos eseményekről.

Az új szabályoknak megfelelően az EU tagállamainak a hálózati és információs rendszerekre vonatkozó nemzeti szintű kiberbiztonsági stratégiát is el kell fogadni. A nemzeti szintű stratégiáknak ki kell terjednie a kibertámadások kezelésére és azokra való reagálásra történő felkészültségre, a kormány és egyéb felek szerepeire, felelősségeire és együttműködésre; az oktatási, tájékoztató és képzési programokra; akutatás és fejlesztés tervezésére; és a kockázatok azonosításának tervezésére.

Az illetékes nemzeti hatóságok feladata, hogy figyelemmel kísérjék az irányelv alkalmazását. Ennek érdekében nemzeti hatóságoknak el kell végezniük az alapvető szolgáltatásokat nyújtók kiberbiztonsági és biztonsági szabályzatainak értékelését, és el kell látniuk a digitális szolgáltatók felügyeletét. Továbbá részt kell venniük az együttműködési csoport munkájában, amely az egyes uniós országok hálózati és információbiztonsági [NIS] illetékes hatóságaiból, az Európai Bizottságból és az Európai Uniós Hálózat- és Információbiztonsági Ügynökségből [ENISA] áll. Az illetékes nemzeti hatóságoknak tájékoztatniuk kell a nyilvánosságot, - a bizalmas adatkezelés szabályai mellett – egy estleges biztonsági esemény megelőzésével kapcsolatos teendőkről vagy a már folyamatban lévő biztonsági esemény kezelése esetén. Mindemellett feladatuk, hogy kötelező érvényű utasítások kiadásával segítsék a kiberbiztonsági hiányosságok orvoslását.[30]

### *2.2.4. Globális stratégia*

Az Európai Unió 2016-ban elfogadott kül- és biztonságpolitikára vonatkozó globális stratégiája (a továbbiakban: globális stratégia) már részletesen foglalkozott a kiberbiztonság kérdésével. A stratégia szerint meg kell erősíteni az EU-t mint biztonsági közösséget és fejleszteni kell az uniós polgárok

[28] 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 (HL L 194., 2016.7.19., 1. o.).

[29] Hálózati és információs rendszerek kiberbiztonsága, ÖSSZEFOGLALÓ AZ ALÁBBI DOKUMENTUMRÓL: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága, https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148

[30] Hálózati és információs rendszerek kiberbiztonsága, ÖSSZEFOGLALÓ AZ ALÁBBI DOKUMENTUMRÓL: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága, https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148

védelmével és a külső válságokra való reagálással kapcsolatos kapacitásokat és képességeket. Mindemellett erősíteni kell a polgári és katonai képességek interoperabilitását. [31]

A globális stratégia hangsúlyozza, hogy az Unió a jövőben kiemelt figyelmet fordít a kiberbiztonsággal kapcsolatos teendők ellátására, és hatékonyabban kíván fellépni a kiberfenyegetésekkel szemben. Az EU a nyitott, szabad és biztonságos kibertérrel kapcsolatos kérdéseket minden szakpolitikai területen figyelembe kívánja venni.

#### 2.2.4.1. Kiberbiztonság a globális stratégiában

„Az EU fokozottabb figyelmet fog szentelni a kiberbiztonság kérdésének, és megfelelő eszközöket biztosít az Uniónak ahhoz, hogy védekezzen a kiberfenyegetések ellen, és támogatja a tagállamokat a védekezésben, miközben fenntartja a nyitott, szabad és biztonságos kiberteret. Ez a fenyegetések csökkentését célzó technológiai képességek, valamint a kritikus infrastruktúra, a hálózatok és a szolgáltatások sokktűrő képességének megerősítését és a kiberbűnözés visszaszorítását teszi szükségessé. Továbbá azt is jelenti, hogy támogatni kell az adatok rendelkezésre állását és integritását garantáló innovatív információs és kommunikációs technológiák (ikt) használatát, ugyanakkor az adattárolás helyszínére és a digitális termékek és szolgáltatások tanúsítására vonatkozó megfelelő szakpolitikák révén garantálni kell a biztonságot az európai digitális térben. A kibertérrel kapcsolatos kérdéseket minden szakpolitikai területen figyelembe kell venni, meg kell erősíteni a KKBP-missziók és műveletek kibertérrel kapcsolatos elemeit és fejleszteni kell az együttműködés fórumait. Az EU támogatni fogja a kibertérrel kapcsolatos politikai, operatív és technikai együttműködést a tagállamok között, különösen az elemzés és a következménykezelés terén, és ösztönzi az uniós struktúrák és az illetékes tagállami intézmények közös értékeléseit. Javítani fogja a kibertérrel kapcsolatos együttműködést az olyan fő partnerekkel, mint az USA és a NATO. Az EU válasza az erős köz-magán társulásokban is tükröződni fog. A tagállamok, az intézmények, a magánszektor és a civil társadalom közötti együttműködés és információmegosztás révén javítható a közös kiberbiztonsági kultúra, valamint az informatikai rendszerek esetleges meghibásodására és az ilyen rendszerek ellen indított támadásra való felkészültség."[32]

### *2.2.5. 2017-es kiberbiztonsági stratégiai felülvizsgálat*

Mivel nem minden esetben teljesültek a 2013-as stratégiában kitűzött célok, és az utóbbi években olyan mértékű változások következtek be a kiberbiztonsági fenyegetések terén, így elkerülhetetlenné vált az első stratégia felülvizsgálata és egy új kidolgozása.

A kritikus infrastruktúrák, a demokratikus intézmények és a „tárgyak internete" (Internet of Things, IoT) elleni zavaró számítógépes műveletek, valamint a botnetek segítségével indított nagyszabású támadások és globális zsarolóvírusos (ransomware) fertőzések (pl. a „WannaCry"[33] és a „NotPetya") felhívták a figyelmet a számítógépes kockázatokra és az uniós szintű proaktív fellépés szükségességére. [34]

---

[31] Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf 15. o.

[32] Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf 17. o.

[33] 2017 májusában a WannaCry nevű zsarolóvírus – támadás több mint 150 országban 400 000-nél is több számítógépet érintett.

[34] Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018, https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 23 p

Az Európai Bizottság irányításával 2017-ben elkészült az EU új, felülvizsgált kiberbiztonsági stratégiája. Az EB és a külügyi és biztonságpolitikai főképviselőjének közös közleménye az Európai Parlamentnek és a Tanácsnak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése" címet kapta. [35]

A 2017-es stratégia hangsúlyozza:
„A kiberbiztonság jólétünk és biztonságunk szempontjából egyaránt kiemelten fontos. Mivel mindennapi életünk és gazdaságunk egyre inkább függ a digitális technológiáktól, egyre nagyobb veszélyeknek vagyunk kitéve. A kiberbiztonsági események sokfélesége az elkövetők, illetve az általuk elérni kívánt célok szempontjából egyaránt fokozódik. A rossz szándékú kibertevékenységek nem csupán gazdaságunkat, valamint a digitális egységes piac lendületét fenyegetik, hanem demokráciánk működését, szabadságjogainkat és értékeinket is. Biztonságunk jövője azon múlik, hogy kapacitásainkat hogyan tudjuk úgy kiigazítani, hogy megvédjük az Uniót a kiberfenyegetésekkel szemben: a civil infrastruktúra és a katonai kapacitás egyaránt digitális biztonsági rendszerekre támaszkodik." [36]

A dokumentum kiemeli, hogy ugyan „továbbra is az uniós tagállamok felelősek saját nemzetbiztonságukért, a fenyegetettség mértéke és határokon átnyúló jellege miatt mindenképpen szükség van az uniós fellépésre, ugyanakkor ösztönzést és támogatást kell nyújtani a tagállamoknak, hogy több és jobb nemzeti kiberbiztonsági kapacitást fejlesszenek és tartsanak fenn, az uniós szintű kapacitások egyidejű építése mellett." [37]

Az új stratégia az EU kibertámadásokkal szembeni ellenálló képessége, visszatartó ereje és védelme érdekében új intézkedéseket javasolt. Ezek közül fontos megemlíteni az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) megerősítését, a digitális termékek és szolgáltatások kiberbiztonságának növelését elősegítő önkéntes, uniós kiberbiztonság-tanúsítási keretrendszer kidolgozását, valamint a nagy léptékű kiberbiztonsági események és krízishelyzetek esetén a gyors, összehangolt reagáláshoz felhasználható tervezet megalkotását.[38]

A közös közlemény a kibervédelmet az uniós intézkedések prioritásaként emeli ki. Ezek végrehajtásához pedig a 2014-es uniós kibervédelmi szakpolitikai keretet megújítása szükséges.

### 2.2.5.1. A 2017-es kiberbiztonsági csomag és a digitális egységes piaci stratégia

2017. szeptember 13-án Jean-Claude Juncker, az Európai Bizottság elnöke az Európai Unió helyzetéről szóló éves beszédében az állandóan változó kiberfenyegetésekkel szembeni felkészültség érdekében egy kiberbiztonsági csomag megvalósítására tett javaslatot. Juncker hangsúlyozta, hogy 2013 óta az EU előrelépéseket tett ugyan az európaiak online biztonságának garantálása terén, de továbbra sin-

[35] Közös közlemény az Európai Parlamentnek és a Tanácsnak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése", Brüsszel, 2017.9.13. JOIN(2017) 450 final, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en

[36] Közös közlemény az Európai Parlamentnek és a Tanácsnak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése", Brüsszel, 2017.9.13. JOIN(2017) 450 final, 2. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en

[37] Közös közlemény az Európai Parlamentnek és a Tanácsnak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése", Brüsszel, 2017.9.13. JOIN(2017) 450 final, 3. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en

[38] Javaslat Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari ó, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról. Európai Bizottság, Brüsszel, 2018. 9. 12. COM(2018) 630 final

csenek megfelelő eszközök a kibertámadások elhárítására. Beszédében ismertette, hogy az Európai Bizottság új eszközöket javasol az kibertámadásokkal szembeni védelem megerősítése érdekében. Többek között egy európai kiberbiztonsági ügynökség létrehozására tett javaslatot."[39]

### 2.2.5.2. A kiberbiztonsági jogszabály

2017. szeptember 13-án elfogadott kiberbiztonsági csomag részeként vette kezdetét a kiberbiztonsági jogszabályként ismert rendelet megalkotása, amely a digitális egységes piaci stratégia egyik prioritása. 2018 szeptemberében az Európai Bizottság javasolta egy Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a kiberbiztonsági kompetenciaközpontok hálózatának létrehozását. A szervezeti átalakítások célja a kiberbiztonsági együttműködésre, kutatásra és innovációra elkülönített források hatékonyabb elosztása és használatának összehangolása.[40]

A digitális egységes piaci stratégia prioritása, hogy az online tranzakciók útjában álló akadályok elháruljanak, a fogyasztók biztonságosan hozzáférjenek a termékekhez és szolgáltatásokhoz. Mindezzel együtt, a vállalkozások, a különböző gazdasági szereplők és a kormányok ki tudják használni a digitális eszközök nyújtotta előnyöket. Mindennek érdekében az EU egységes piacát a digitális kor kereteihez kell illeszteni.[41]

A kiberbiztonsági rendeletre 2017-ben tett javaslat a következő területekre terjed ki:

- Az ENISA eredetileg 2020-ig szóló megbízásának állandóvá tétele és erőforrásainak növelése;
- az ENISA az új kiberbiztonsági tanúsítási keretben támogassa a tagállamokat a kibertámadásokkal szembeni hatékony fellépésben

A szervezeti átalakulások célja, hogy a 2005-től működő ENISA hozzájáruljon a kiberbiztonsági kapacitás növeléséhez, a kapacitásépítéshez és a felkészültség fokozásához, illetve független szakmai központként működjön. Ennek érdekében elősegíti az uniós polgárok és a vállalkozások tudatosságának növelését és támogatja az uniós intézményeket és tagállamokat a szakpolitikák kidolgozásában és végrehajtásában.

A kiberbiztonsági rendelet megalkotásának célja, hogy az EU teljes területén érvényes európai kiberbiztonsági tanúsítási keret jöjjön létre a termékek, eljárások és szolgáltatások számára. Az új belső piaci törvénynek köszönhetően a kiberbiztonsági tanúsítási keretrendszer a hálózatra kapcsolt termékek, a dolgok internetéhez kapcsolódó eszközök, valamint a kritikus infrastruktúra biztonságát javítja. A tanúsítványok a termékek műszaki tervezése és fejlesztése korai szakaszaiban elősegíthetik a biztonsági elemek beépítését (beépített biztonság), és a felhasználók számára megkönnyíthetik a biztonsági szint megállapítását is. Továbbá biztosítja a különböző biztonsági elemek független ellenőrzését.[42]

Az internet biztonságát elősegítő tanúsítványok szabályozási lépései nem csupán a lakossági és védelmi vonatkozású számítógépes technológiák számára fontosak, hanem jelentős hatást gyakorolhatnak az általános európai kiberbiztonsági környezetre is. Az EU 2018-as kibervédelmi szakpolitikai kerete szerint „a tanúsítási keretrendszernek, segítenie kell az ikt-folyamatokra, -termékekre és -szolgáltatásokra vonatkozó szigorú szabványok érvényesülését, versenyelőny forrásává kell válnia,

---

39 Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet, Brüsszel, 2017. szeptember 19., https://europa.eu/rapid/press-release_IP-17-3193_hu.htm

40 Digitális egységes piac, Az internetben rejlő lehetőségek kiaknázását nehezítő akadályok felszámolása, https://ec.europa.eu/commission/priorities/digital-single-market_hu

41 Digitális egységes piac, Az internetben rejlő lehetőségek kiaknázását nehezítő akadályok felszámolása, https://ec.europa.eu/commission/priorities/digital-single-market_hu

42 Az uniós tárgyaló felek megállapodtak az európai kiberbiztonság fokozásáról, Brüsszel, 2018. december 10. https://europa.eu/rapid/press-release_IP-18-6759_hu.htm

és hozzá kell járulnia a fogyasztók és a beszerzők bizalmának növeléséhez.” [43]

A Tanács 2019. április 9-én elfogadta a kiberbiztonsági rendelet szövegét. A jóváhagyott rendeletet először a Parlamentnek, majd a Tanácsnak is hivatalosan is el kell fogadnia. A rendelet az egész EU-ra kiterjedő tanúsítási rendszert vezet be, és - a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) helyett - létrehozza az Európai Uniós Kiberbiztonsági Ügynökséget.[44]

### *2.2.6. Kibervédelem és az állandó strukturált együttműködés (PESCO)*

2017-től, 25 tagállam részvételével megkezdődött a lisszaboni szerződésben szereplő állandó strukturált együttműködés (PESCO) megvalósításának folyamata. A résztvevő államok kötelezettséget vállaltak arra, hogy fokozzák a kibervédelem területén folytatott együttműködésre irányuló erőfeszítéseiket. A PESCO segíti a közös képességfejlesztések megvalósítását és a tagállamok közötti együttműködés fokozását. A 2017-től induló PESCO-projektek között szerepel két kibervédelmmel kapcsolatos projekt szerepel: a „Kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén”, illetve „A kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform” címmel. [45]

### *2.2.7. Az Európai Unió kibervédelmi szakpolitikai kerete (2018)*

A megváltozott biztonsági kihívásokat figyelembe véve a Tanács 2018 októberében elfogadta az uniós kibervédelmi szakpolitikai keret módosított változatát. A keret meghatározza a kibervédelem kiemelt területeit, továbbá pontosítja a szereplők feladatait.

A dokumentum alapján az „EU-nak és tagállamainak meg kell erősíteniük a kiberrezilienciájukat és megbízható kiberbiztonsági és -védelmi képességeket kell kialakítaniuk, hogy meg tudjanak felelni a változó biztonsági kihívásoknak.” Mindennek érdekében az EU támogatja a tagállamok kibervédelmi képességfejlesztését, kibervédelmének megerősítését. A dokumentum kiemeli: „A kibertér az ötödik műveleti terület a szárazföld, a tenger, a légtér és a világűr mellett: az uniós missziók és műveletek végrehajtásának sikere egyre nagyobb mértékben függ a biztonságos kibertérhez való zavartalan hozzáféréstől, ezért szilárd és ellenálló kiberműveleti képességeket igényel.”[46]

A dokumentum utal a 2016-os globális stratégiában és az EU és a NATO közötti együttműködésről szóló együttes nyilatkozatban megfogalmazott célok és prioritások végrehajtására. Mindemellett hangsúlyozza, hogy a kibervédelmi szakpolitika céljainak megvalósításához számos más uniós poli-

---

43 UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 2. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

44 Kiberbiztonság Európában: szigorúbb szabályok és nagyobb védelem, https://www.consilium.europa.eu/hu/policies/cybersecurity/
Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést, Az EU Tanácsa, Sajtóközlemény, 2018. 12. 19., https://www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

45 UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 7. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf; Permanent Structured Cooperation (PESCO)’s projects – Overview, 2019, https://www.consilium.europa.eu/media/39762/pesco-overview-of-first-collaborative-of-projects-for-press.pdf

46 UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 5. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

tika is hozzájárul. E szakpolitikai keret figyelembe veszi polgári területekre vonatkozó szabályozást (pl. a hálózat- és információbiztonsági irányelvet) is.

A Tanács az Európa kibertámadásokkal szembeni ellenálló képességének erősítéséről szóló, 2016. novemberi következtetéseiben célul tűzte ki az EU stratégiai autonómiájának növelését e területen is. Az Európai Tanács 2018 júniusában megerősítette ezt a célkitűzést, továbbá hangsúlyozta, hogy az EU-n kívülről érkező kiberbiztonsági fenyegetésekkel szembeni védelmi képességeket meg kell erősíteni. [47]

A szakpolitikai keret kiemeli, hogy a Tanács kiberbiztonsággal foglalkozó 2017. novemberi következtetései szerint a kiberbiztonság és védelem területei egyre jobban összefonódnak, így ösztönözni szükséges az elhárító, polgári és katonai tevékenységek közötti együttműködést. A tanácsi dokumentum hangsúlyozta, hogy egy különösen súlyos kiberbiztonsági esemény vagy válság esetén a lisszaboni szerződésben szereplő szolidaritási és/vagy kölcsönös segítségnyújtási klauzulája is aktiválható.[48]

A szakpolitikai keret hat prioritási területet határoz meg: 1) a kibervédelmi képességek fejlesztése, 2) az EU KBVP-vel kapcsolatos kommunikációs és információs hálózatainak védelme, 3) a képzés és gyakorlatok, 4) a kutatás és technológia, 5) a polgári-katonai együttműködés, 6) a nemzetközi együttműködés területi.

## 2.3. Az EU kiberbiztonsági intézményrendszerének kialakulása

A kérdés átfogó jellegéből adódóan az Európai Unióban gyakorlatilag szinte minden intézmény, szerv és ügynökség érintett a kiberbiztonság megvalósításában. Az alábbiakban kiberbiztonsági intézményrendszernek csupán azon intézményeit mutatjuk be, amelyek kizárólag e területen kitűzött célok végrehajtásáért és megvalósításáért felelnek.

### *2.3.1. ENISA - Európai Uniós Hálózat- és Információbiztonsági Ügynökség*

2004-ben jött létre az Európai Uniós Hálózat- és Információbiztonsági Ügynökség, az ENISA. Az ügynökség 2005-től Kréta szigetén működik. 2005-től az ügynökség feladata volt „az Unión belüli magas szintű hálózat- és információbiztonsághoz való hozzájárulás; az ezzel kapcsolatos tudatosság növelése; a biztonságtudatosság kultúrájának kialakítása és előmozdítása a polgárok, fogyasztók, vállalkozások és közszektorbeli szervezetek javára.”[49]

Az első kiberbiztonsági stratégia kidolgozásával párhuzamosan, 2013. május 21-én született meg az Európai Parlament és a Tanács új rendelete az ENISA működéséről, amely az Ügynökség megbízatását 2020-ig meghosszabbította, valamint megerősítette a kibertámadások és egyéb információbiztonsági kihívások leküzdésére való képességét. [50]

---

47 UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 5. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

48 Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU -Council conclusions (20 November 2017), https://www.consilium.europa.eu/media/31666/st14435en17.pdf

49 ENISA - Európai Uniós Hálózat- és Információbiztonsági Ügynökség, 06.04.2014, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=legissum:3103_2

50 526/2013/EU rendelete ( 2013. május 21. ), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32013R0526

A belső piac megfelelő működése érdekében az ügynökség feladatai 2013-tól:

- Az uniós politika és jog fejlesztésének támogatása azáltal, hogy a hálózat- és információbiztonsági politikához kapcsolódó valamennyi kérdésben tanácsot ad, ezzel kapcsolatban előkészítő munkát végez és tanácsot ad, valamint elemzi a nyilvánosan elérhető stratégiákat és előmozdítja közzétételüket.
- A képességek fejlesztésének támogatása azáltal, hogy kérésükre támogatja az uniós országokat, valamint az uniós intézményeket a hálózat- és információbiztonságot érintő problémák és váratlan események megelőzésének, észlelésének, elemzésének fejlesztésében és javításában. Idetartozik a hálózatbiztonsági vészhelyzeteket elhárító csoportok létrehozásának támogatása, valamint az uniós korai előrejelzési rendszer kialakítása.
- Az illetékes állami szervek és az érdekeltek, köztük az egyetemek és a kutatóközpontok közötti önkéntes együttműködés támogatása, valamint a figyelemfelkeltő tevékenységek előmozdítása.
- A kutatás és fejlesztés, továbbá a szabványosítás támogatása a kockázatkezelésre és az elektronikus termékek, hálózatok és szolgáltatások biztonságára vonatkozó nemzetközi standardok révén.
- Az uniós intézményekkel és szervekkel - köztük a kiberbűnözés elleni fellépéssel és a magánélet, illetve a személyes adatok védelmével foglalkozókkal - való együttműködés a szinergiák kialakítása és a közös érdekű ügyekkel kapcsolatos problémák kezelése érdekében.
- A hálózat- és információbiztonsággal kapcsolatos, harmadik országokkal és nemzetközi szervezetekkel folytatandó együttműködésre irányuló uniós erőfeszítésekhez való hozzájárulás.”[51]

Az első kiberbiztonságra vonatkozó uniós intézkedés, a hálózati és információs rendszerek biztonságáról szóló 2016-os irányelvvel az ENISAk központi szerepet kapott az irányelv végrehajtásának támogatásában. Az ENISA látja el a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-k) NIS-irányelv alapján létrehozott hálózatának titkárságát, és aktívan támogatja a CSIRT-ek közötti együttműködést.

A 2017 óta előkészített kiberbiztonsági rendelet szövegét a tanács 2019 áprilisában elfogadta. Az új jogszabály a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség helyett létrehozza az Európai Uniós Kiberbiztonsági Ügynökséget.[52] Az új jogszabályok szerint az ENISA 2020-tól állandó megbízatása mellett **új feladatokat is** kap a kiberkérdésekben a tagállamoknak, az uniós intézményeknek és minden más érdekeltnek nyújtandó támogatás terén. Az ENISA központi szerepet fog betölteni a tanúsítási rendszerek kialakításában, illetve a tanúsítványokra vonatkozó információkat tartalmazó honlapot fog működtetni. Az ügynökség új feladatai között szerepelni fog a rendszeres uniós szintű kiberbiztonsági gyakorlatok, illetve kétévente egy-egy nagyarányú átfogó gyakorlat szervezése. Az ENISA munkáját egy nemzeti összekötő tisztviselőkből álló hálózat segíti majd.[53]

---

51 ENISA - Európai Uniós Hálózat- és Információbiztonsági Ügynökség, 06.04.2014, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=legissum:3103_2

52 Kiberbiztonság Európában: szigorúbb szabályok és nagyobb védelem, https://www.consilium.europa.eu/hu/policies/cybersecurity/
Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést, Az EU Tanácsa, Sajtóközlemény, 2018. 12. 19., https://www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

53 Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést, Az EU Tanácsa, Sajtóközlemény, 2018. 12. 19., https://www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

Az ENISA 2018-tól gyakorlatai útján is igyekezett elősegíteni a kiberfenyegetésekkel szembeni védelem javítását. Az ügynökség a Bizottság és a Parlament támogatásával két gyakorlatot szervezett szervezett a kiberfenyegetésekkel szembeni felkészültség és reziliencia erősítése érdekében. Az ENISA által szervezett gyakorlatok hozzájárultak a nemzeti hatóságok felkészítéséhez például a választások legitimitását megkérdőjelező eseményekre, vagy olyan kibertámadásokra, amelyeket a kritikus infrastruktúrák ellen, az európai választások előtt és alatt hajtanak végre.[54]

## *2.3.2. A hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-EU)*

A 2010-ben elfogadott európai digitális menetrendben az Európai Bizottság vállalta, hogy a hálózatbiztonsági vészhelyzeteket elhárító csoportot hoz létre az uniós intézmények számára. A digitális menetrend alapján nem csupán az uniós, hanem a tagállami szinten is létre kellett hozni a hálózatbiztonsági vészhelyzeteket elhárító csoportokat, azaz a CERT-csoportokat annak érdekében, hogy 2012-re megvalósulhasson a nemzeti és kormányzati CERT-ek uniós hálózata.

Az egyéves kísérleti szakasz követően, 2012 szeptemberétől már teljes kapacitással működtek a CERT-ek. Az újonnan felállított állandó csoportok feladata, hogy hogy fokozza az Európai Unió intézményeinek számítógépes rendszereit érintő fenyegetések elleni küzdelmet és az elsősorban információbiztonságot érintő támadások esetén segítséget nyújtson azok elhárításában.

A CERT-ek feladata a hálózatbiztonság sérülékeny pontjainak és hiányosságainak megelőzése, a fenyegetések feltérképezése és a hiányosságok kijavítása. A rendszerbiztonság megőrzése és helyreállítása érdekében – a rendszer gyenge pontjainak feltérképezésével - a csoportok figyelmeztetik ügyfeleiket a fennálló biztonsági hiányosságokra és fenyegetésekre, intézkedéseket javasolnak a kockázatok csökkentésére.

A CERT-EU - az uniós intézmények kiberbiztonságának növelése érdekében - támogatja az EU-intézmények számítástechnikai biztonsági csoportjainak munkáját, és szoros kapcsolatot tart fenn a tagállamok közszférájában hasonló feladatokat ellátó szervekkel. A CERT-EU létrehozásának előzménye, hogy a korábbi években az állami és a magánszektorban is olyan hálózatbiztonsági szakemberekből álló kisebb csoportokat (CERT) hoztak létre, amelyek állandó szakértelmük folytán képessé váltak hatékonyan és eredményesen reagálni az információbiztonságot érintő eseményekre és kiberfenyegetésekre. Az uniós szinten létrehozott CERT-EU működéséhez szükséges forrásokat a főbb uniós bocsátotta rendelkezésre. „A csoport tevékenységét stratégiailag egy intézményközi irányító testület felügyeli. Munkája során a CERT-EU szorosan együttműködik az egyes intézmények számítástechnikai biztonsági csoportjaival, továbbá kapcsolatot tart fenn a tagállamokban és az unión kívül működő CERT-ekkel és számítástechnikai biztonsági cégekkel, hogy ezáltal biztosítható legyen a fenyegetésekre és az ezek kezelésére vonatkozó információcsere.”[55]

## *2.3.3. EUROPOL EC3*

Az EUROPOL hágai székhelyén még ugyanebben az évben, 2013-ban létrejött a számítástechnikai bűnözéssel foglalkozó európai központ, az EC3 (European Cybercrime Centre). Az Európai Bizottság javaslata lapján az új központ felállításának célja volt, hogy az európai polgárok és vállalkozások számára védelmet biztosítson a számítógépes fenyegetésekkel és segítse a kormányokat a számítógépes bűnözéssel szemben.

---

[54] Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról, KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, Brüsszel, 2019.6.14. JOIN(2019) 12 final, 9. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

[55] Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága, Európai Bizottság, Sajtóközlemény, Brüsszel, 2012. szeptember 12., https://europa.eu/rapid/press-release_IP-12-949_hu.htm

Az EU új központja kezdetektől a szervezett bűnözői csoportok által elkövetett jogellenes online tevékenységekre összpontosít, különös tekintettel az elektronikus banki szolgáltatásokra és egyéb pénzügyi tevékenységekre irányuló támadásokra. A központ támogatást nyújt, hogy hatékonyabb védelmet biztosítson a közösségi oldalak profiljainak az elektronikus bűnözéssel szemben, valamint tájékoztatást és elemzéseket nyújtson a nemzeti bűnüldöző hatóságok számára.[56]

Az EC3 megalapítása óta jelentős mértékben hozzájárult a számítógépes bűnözés elleni küzdelemhez: számos kiemelkedő műveletben és helyszíni operatív támogatás megvalósításában vett részt.

### *2.3.4. A számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)*

A 2016-os hálózati és információs rendszerek biztonságáról szóló európai parlamenti és tanácsi irányelv (2016/1148) átültetése tagállami szinten szükségessé tette a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) hálózatának, azaz a CSIRT-hálózatok létrehozását. Az uniós szintű hálózat a tagállamok CSIRT-jeiből és a hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT-EU) képviselőiből áll.

A CSIRT-hálózatok feladatai:

- „információk megosztása a CSIRT-szolgáltatásokra vonatkozóan;
- információk megosztása a kiberbiztonsági eseményekre vonatkozóan;
- az uniós országok támogatása a határokon átnyúló eseményekre való reagálásban;
- koordinált válasz megvitatása és azonosítása valamely uniós ország által bejelentett biztonsági eseményre;
- az operatív együttműködés további formáinak megvitatása, megvizsgálása és meghatározása a következőkkel kapcsolatban:
    - a kockázatok és biztonsági események kategóriái;
    - korai előrejelzés;
    - kölcsönös segítségnyújtás;
    - a koordináció az országok között egynél több uniós országot érintő kockázatokra és biztonsági eseményekre való reagálás során;
- az együttműködési csoport tájékoztatása a tevékenységeiről és iránymutatás kérése;
- a kiberbiztonsági gyakorlatokból levont tanulságok megvitatása;
- az egyes CSIRT-ek képességeinek megvitatása azok kérésére;
- iránymutatások kibocsátása az operatív együttműködésre vonatkozóan.”[57]

[56] Európai Bizottság, Sajtóközlemény, Brüsszel, 2012. július 9. Számítástechnikai bűnözés: az uniós polgárok aggódnak a személyes adatok és az online fizetési műveletek biztonsága miatt, https://europa.eu/rapid/press-release_IP-12-751_hu.htm?locale=en

[57] Hálózati és információs rendszerek kiberbiztonsága, ÖSSZEFOGLALÓ AZ ALÁBBI DOKUMENTUMRÓL: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága, https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148

### *2.3.5. Javaslat az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról*

Az Európai Bizottság 2018 őszére elkészítette az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendelettervezetet. A tervek szerint az új uniós szintű központ feladata, hogy megkönnyítse és segítse nemzeti koordinációs központok hálózatának munkájának összehangolását, valamint támogassa a kiberbiztonsági kompetenciaközösséget. A kompetenciaközpont az EU által javasolt Digitális Európa program és Horizont Európa program keretében a kiberbiztonságra fordítandó uniós pénzügyi támogatások fő végrehajtási szerve lesz, és szoros együttműködést folytat a Nemzeti Koordinációs Központok hálózatával és a kiberbiztonsági kompetenciaközösséggel. Mindezeken túl a Kompetenciaközpont feladata lesz, egyrészt, hogy erősítse a kiberbiztonság polgári és katonai vetületei közötti szinergiákat. Másrészt tanácsadással, a szakértelem megosztásával, továbbá a projektek és tevékenységek terén történő együttműködés elősegítésével támogatást kell nyújtania a tagállamoknak és a többi releváns szereplőnek. A központ elősegíti az Unió, a tagállamok és az ipar általi közös beruházások megvalósulását.

Az Európai Bizottság az alábbi problémák feltárása miatt tartja szükségesnek az új kompetenciaközpont létrehozását:

- Nem kielégítő az együttműködés a kiberbiztonság kínálati és keresleti szegmensei között
- Ipari kapacitásépítést célzó, hatékony tagállamok közötti együttműködési mechanizmus hiánya
- Elégtelen együttműködés a kutatói és az ipari közösségek között és ezeken belül
- Elégtelen együttműködés a polgári és a katonai kiberbiztonsági kutatói és innovációs közösségek között.[58]

## 2.4. Uniós kiberdiplomácia

A 2013-as stratégia meghatározta az EU nemzetközi kiberpolitikáját is. Az új szakpolitika a szabad és nyitott internet védelme mellett célul tűzte ki a felelősségteljes állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítását kibertérben és az EU stratégiai partnereivel történő együttműködés javítását. Ennek érdekében tárgyalások kezdődtek az Egyesült Államokkal, Kínával, Japánnal, Dél-Koreával, Indiával és Brazíliával. A résztvevő felek tárgyalások során többek között érintették a kibertérben zajló nemzetközi biztonság, az ellenálló képesség, a kiberbűnözés, az internet szabályozása és a kiberbiztonsági előírások területeit. 2015-ben fontos mérföldkő volt az EU kollektív erőfeszítéseinek elősegítése érdekében a kiberdiplomáciáról szóló tanácsi következtetések elfogadása volt. [59]

---

[58] Javaslat Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról. Európai Bizottság, Brüsszel, 2018. 9. 12. COM(2018) 630 final 4-5. o.

[59] Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018, https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 23 p

2015-től az EU főbb célkitűzései a kiberdiplomácia területén a következők voltak:

- előmozdítja és védi az emberi jogokat és amely az Unió alapvető értékein, vagyis a demokrácián, az emberi jogokon és a jogállamiságon, ezen belül a véleménynyilvánítás szabadságához való jogon, az információhoz való hozzáférés szabadságán és a magánélethez való jogon alapul,
- biztosítja, hogy ne lehessen az internet nyújtotta lehetőségekkel visszaélni gyűlöletkeltés és erőszakra való felbujtás céljával, valamint hogy az internet – az alapvető szabadságok teljes tiszteletben tartásával – továbbra is a szabad véleménynyilvánítás fóruma maradjon a jog maradéktalan betartása mellett,
- előmozdítja a nemek közötti egyenlőséget is figyelembe vevő kiberpolitikát,
- ösztönzi az európai növekedést, jólétet és versenyképességet, valamint védi a legfontosabb uniós értékeket, többek között a kiberbiztonság erősítése és a számítástechnikai bűnözés elleni küzdelem terén folytatott együttműködés javítása révén,
- diplomáciai és jogi eszközök igénybevétele révén hozzájárul a kiberbiztonságot fenyegető veszélyek mérsékléséhez, a konfliktusmegelőzéshez és a stabilitás növekedéséhez a nemzetközi kapcsolatok terén,
- segíti az internet irányítására vonatkozó többérdekeltes modell erősítésére irányuló erőfeszítéseket,
- ösztönzi a nyitott és virágzó társadalmak kialakulását harmadik országokban olyan kiberkapacitás-építési és -fejlesztési intézkedéseken keresztül, amelyek hozzájárulnak a véleménynyilvánítás és az információhoz való hozzáférés szabadságához való jog előmozdításához és védelméhez, és amelyek lehetővé teszik a polgárok számára, hogy teljes mértékben a javukra fordítsák a kibertér társadalmi, kulturális és gazdasági előnyeit, többek között a digitális infrastruktúrák biztonságosságának fokozása révén,
- előmozdítja a felelősség megosztását az érintett érdekelt felek között, többek között a köz- és a magánszektor, valamint a kutató-és tudományos intézetek között a kibertérrel kapcsolatban folytatandó együttműködés révén."[60]

Nemzetközi szinten az EU a kibertérben a konfliktusmegelőzés és a stabilitás érdekében a speciálisan alkalmazandó nemzetközi jog, különösen az ENSZ Alapokmánya és a nemzetközi humanitárius jog szigorú alkalmazását, és a felelősségteljes állami magatartás nem kötelező érvényű egyetemes számítógépes normáinak, szabályainak és alapelveinek teljes végrehajtását tartja fontosnak. A regionális szinten megvalósuló bizalomépítő intézkedések területén az EBESZ a legfejlettebb regionális szervezet.[61]

2017-ben az Európai Unió Tanácsa megállapodott arról, hogy az állami és nem állami szereplők részéről mutatkozó rosszszándékú és szándékos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat kidolgozza, amely támaszkodik az EU közös kül- és biztonságpolitikai eszköztárára. Azon információs és kommunikációs technológiák (ikt) felhasználásával végrehajtott tevékenységekkel szemben, amelyek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, az EU kész a közös kül- és biztonságpolitikai intézkedésekkel, ideértve a korlátozó intézkedéseket is, fellépni.

---

60 *A Tanács következtetései a kiberdiplomáciáról, Brüsszel, 2015. február 11. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf*

61 Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018, https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1 25 p

Az EU kiberdiplomáciai megközelítésével összhangban a közös intézkedések elősegítik a konfliktusmegelőzést, a kiberbiztonságot fenyegető veszélyek mérséklését, és a stabilitás növekedését a nemzetközi kapcsolatok terén. A Tanács célul tűzte ki, hogy a közös uniós diplomáciai intézkedések kerete segíti az együttműködést, előmozdítja a veszélyek csökkentését, valamint hatással lesz a potenciális támadók magatartására. Ezen uniós diplomáciai intézkedések esetében teljes körűen alkalmazni fogják a közös kül- és biztonságpolitika területéhez tartozó intézkedéseket, beleértve a korlátozó, esetleg szankciós intézkedéseket is. Az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú „kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival." Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett." Ezzel összefüggésben minden erőfeszítése arra irányul, hogy hozzájáruljon a kibertér biztonságához és stabilitásához, illetve hogy csökkentse az ikt használatából eredő félreértések, konfliktusterjedés és konfliktusok kockázatát.[62] A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat fogadott el. A dokumentum a kiberdiplomáciai eszköztáron belül öt intézkedéskategóriát sorolt fel. Ezek közé sorolta a korlátozó intézkedéseket, valamint ezen intézkedések bevezetésére vonatkozó eljárást.[63]

A 2018-as kibervédelmi szakpolitikai keret szerint a korábbi évek eseményei még inkább rávilágítottak arra a tényre, hogy a nemzetközi közösségnek együtt kell működnie a konfliktusok megelőzése és a kibertér stabilitásának erősítése érdekében. „Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel, az EBESZ-szel és az ASEAN regionális fórummal együtt, elő kíván mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: i. a nemzetközi jognak és különösen az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; ii. a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása;

iii. regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell."[64]

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá tétele érdekében. Az Európai Tanács 2018. júniusi és 2018. októberi következtetéseiben megfogalmazott célok elérése érdekében olyan uniós korlátozó intézkedések bevezetéséről döntött, amelyek segítik a a kibertámadásokkal kapcsolatos reagálási és elrettentési képesség javítását. 2019. május 17-én döntés született az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló KKBP határozat[65] és a tanácsi rendelet[66]. A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról dönt, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

---

62 Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is. https://www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

63 A TANÁCS (KKBP) 2019/797 HATÁROZATA, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN

64 UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 8. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

65 A TANÁCS (KKBP) 2019/797 HATÁROZATA, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN

66 A TANÁCS (EU) 2019/796 RENDELETE, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC

Az új jogi keret így már lehetővé tette az EU számára, hogy szankciókat is kivethessen (pl. eszközök befagyasztása, utazási tilalom) az Unióra vagy a tagállamaira külső fenyegetést jelentő kibertámadásoktól való elrettentés, valamint az azokra való reagálás érdekében.[67] A szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük (A Tanács (EU) 2019/796 rendelete 15. cikk).

„Az EU az alábbi elvek alapján fogja folytatni a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének kidolgozását:

- védeni kell az EU, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát,
- figyelembe kell venni az érintett állammal fennálló uniós külkapcsolatok tágabb összefüggéseit,
- biztosítani kell a KKBP- célkitűzések elérését, az Európai Unióról szóló szerződésben foglaltakkal és az e célkitűzések elérése érdekébenmeghatározott megfelelő eljárásokkal összhangban,
- az intézkedéseknek a tagállamok által közösen kialakított helyzetismereten kell alapulniuk és meg kell felelniük az adott helyzet támasztotta igényeknek,
- az intézkedéseknek arányosnak kell lenniük a kibertevékenység hatókörével, léptékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásaival,
- tiszteletben kell tartani az alkalmazandó nemzetközi jogot és nem szabad alapvető jogokat és szabadságokat sérteni.”[68]

## *2.4.1. EU–NATO együttműködés*

Az EU és NATO között együttműködés területén már 2012-től magas szintű konzultációk és találkozók valósultak meg. A folyamat azonban valódi lendületet 2016-tól kapott. Az EU és a NATO között 2016-tól, az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre.[69] A globális stratégia hangsúlyozza, hogy míg a NATO a kollektív védelem elsődleges keretét biztosítja a legtöbb tagállam számára, addig az EU elsősorban az olyan belső és külső kihívásokkal szemben kíván fellépni, mint a terrorizmus, a hibrid fenyegetések, a kiber- és energiabiztonság, a szervezett bűnözés és a külső határok igazgatása.

2016. július 8-án a NATO-csúcson Varsóban az EU részéről az Európai Tanács elnöke és az Európai Bizottság elnöke, illetve a NATO főtitkára együttes nyilatkozatot írt alá az EU és a NATO közötti együttműködésről. A nyilatkozat aláírását követően a két szervezet közötti együttműködés új lendületet kapott, és kiterjed a hibrid fenyegetések elleni küzdelemre; a kiberbiztonság és -védelem területeire is.[70] Az együttes nyilatkozata konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érde-

[67] Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról, KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, Brüsszel, 2019.6.14. JOIN(2019) 12 final, 9. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

[68] TERVEZET – A TANÁCS KÖVETKEZTETÉSEI A ROSSZ SZÁNDÉKÚ, KIBERTEVÉKENYSÉGEKKEL SZEMBENI KÖZÖS UNIÓS DIPLOMÁCIAI INTÉZKEDÉSEK KERETÉRŐL („KIBERDIPLOMÁCIAI ESZKÖZTÁR”), Brüsszel, 2017. június 7. (OR. en) http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf

[69] Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf

[70] EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából https://www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/

kében: megerősíteni a kibervédelemi interoperabilitást a missziók és műveletek során; az együttműködés erősítése a képzések és a gyakorlatokon; a kibervédelmi kutatásokkal és technológiai innovációval kapcsolatos együttműködés előmozdítása; valamint a kibernetikus szempontok beépítése a válságkezelésbe.[71]

2016 februárjában, az EU és a NATO képviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (Computer Emergency Response Teams – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (NATO's Computer Incident Response Capability – NCIRC) közötti technikai megállapodást. A megállapodás célja a technikai információk megosztásának megkönnyítése a számítógépes események megelőzése érdekében, illetve a kiberbiztonsági események felderítése és az azokra való reagálás erősítése mindkét szervezetben. Az e területeken megvalósuló tevékenységek mind a mai napig a két szervezet közötti együttműködés alapját képezik.

Az együttműködés másik legfontosabb eredménye, hogy – finn kezdeményezésre, de az EU és a NATO támogatásával - 2017-ben Helsinkiben létrejöhetett a Hibrid Tevékenységek Elleni Kiválósági Központ (European Centre of Excellence for Countering Hybrid Threats), amelynek feladata az elsősorban az Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.[72] Az új központ felállítása lehetőséget biztosított az Észak-atlanti Tanács és az uniós Politikai és Biztonsági Bizottság közötti informális találkozók megszervezésére, és így a hibrid fenyegetéssel szembeni koordinált fellépés kidolgozására.[73]

A 2017. novemberi második előrehaladási jelentésben elő helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a tengerbiztonsági, valamint a kiberbiztonsági és a védelmi fejlesztés területeken elért eredményeket. Ezek közül kiemelte a képzések és gyakorlatok területén megvalósuló együttműködések fontosságát. A NATO alkalmazottak például részt vehettek az uniós ügynökség, az ENISMA kiberbiztonsági gyakorlatán. A fejlesztési duplikációk elkerülése érdekében megkezdődött folyamatossá vált az együttműködés.[74]

Az önállóan működő központ munkájába 2019 januárjáig Ausztria, Kanada, Ciprus, a Cseh Köztársaság, Dánia, Észtország, Finnország, Franciaország, Olaszország, Németország, Lettország, Litvánia, Hollandia, Norvégia, Lengyelország, Románia, Spanyolország, Svédország, az Egyesült Királyság és az USA kapcsolódott be. Fontos megjegyezni, hogy az új együttműködési forma a semleges EU-tagállamok (Ausztria, Finnország és Svédország), illetve a nem uniós NATO-tagok (USA, Kanada és Norvégia) számára is lehetővé tette a csatlakozást. A meglévő ellentétek következtében Ciprus és Törökország kezdetektől nem vesz részt a megvalósításban.[75] Magyarország mindeddig nem kapcsolódott be a helsinki székhelyű kutatóközpont munkájába.[76]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytattak egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és tovább fejlesszék az EU és a NATO közötti együttműködést. 2017-ben a NATO-irányítással, 2018-ban pedig az Unió vezetésével hajtották végre a gyakorlatokat. A 2018-as „EU-HEX-ML 18 (PACE)" gyakorlat jelentősen segítette a szervezetek személyi állományok közötti együttműködést.[77] 2019-ben a jólbevált gyakorlat folytatódott, és a NATO CMX 19 gyakorlat is kiterjedt a személyi állományok közötti együttműködésre az EU intézményeivel (EKSZ, EK és a Tanács).[78]

---

71 Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, 2016.

72 European Centre of Excellence for Countering Hybrid Threats.

73 Hybrid CoE Supports Informal NAC-PSC Discussion, September 28, 2018.

74 Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016; 29 November 2017.

75 European Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?

76 lásd pl: Honvédelmi Minisztérium, 2017. május 30.; Jegyzőkönyv az Országgyűlés Külügyi bizottságának 2017. június 7-én, szerdán, 10 óra 07 perckor az Országház főemelet 55. számú tanácstermében megtartott üléséről

77 Crisis preparedness: EU launches civil-military crisis management exercise Bruxelles, 16/11/2018 - 15:25, UNIQUE ID: 181116_7, https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en

78 George ALLISON: NATO conducts Crisis Management exercise. UK Defence Journal. [online] Source: https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/ (Accessed on: 04/07/2019)

### *2.4.2. Az EU és az Európa Tanács közötti fellépés*

A számítástechnikai bűnözésről szóló 2001. évi Európa tanácsi egyezményt (Budapesti Egyezmény) az uniós tagállamok többsége aláírta. Ez az egyetlen olyan nemzetközi szerződés, amelynek célja egy közös büntetőjogi politika kialakítása, többek között megfelelő jogszabályok elfogadásával és a nemzetközi együttműködés elősegítésével a társadalom védelme érdekében a számítástechnikai bűnözéssel szemben.[79]

2013 és 2018 között az EU mintegy 80 millió eurót fektetett a kiberbiztonsági kapacitásépítésbe, mindezzel jelentős szerepet játszott a globális kiberbiztonság megerősítésében. Az EU, az Európa Tanáccsal együttműködve, egyre több pénzügyi forrást fordított a számítógépes bűnözés elleni fellépésre világszerte. Az uniós pályázati programok hozzájárulnak a kiberbiztonsági eseményekre való válaszadási képességek technikai és szervezeti szintű megerősítéséhez a fejlődő országokban. A kapacitásépítési erőfeszítések szintén kulcsfontosságú szerepet játszottak a harmadik országokkal folytatott szoros partnerségek kiépítésében, és segítették a nyílt, szabad és biztonságos kibertér fogalmának

## 2.5. Felhasznált irodalom


- 526/2013/EU rendelete ( 2013. május 21. ), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex:32013R0526
- A BIZOTTSÁG KÖZLEMÉNYE A TANÁCSNAK, AZ EURÓPAI PRLAMENTNEK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK „i2010: európai információs társadalom a növekedésért és a foglalkoztatásért". Brüsszel, 1.6.2005 COM(2005) 229 végleges, 6. o. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2005)0229_/com_com(2005)0229_hu.pdf
- A TANÁCS (EU) 2019/796 RENDELETE, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC
- A TANÁCS (KKBP) 2019/797 HATÁROZATA, (2019. május 17.), az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN
- A Tanács következtetései a kiberdiplomáciáról, Brüsszel, 2015. február 11. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf
- 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 (HL L 194., 2016.7.19., 1. o.).
- Az Európai Unió belső biztonsági stratégiája - Az európai biztonsági modell felé. 2010. 7. o. https://www.consilium.europa.eu/media/30741/qc3010313huc.pdf
- Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér" JOIN/2013/01 final, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001
- Az Unió helyzetéről szóló 2017. évi beszéd – Kiberbiztonság: a Bizottság megerősíti a kibertámadásokkal szembeni uniós reagálási képességet, Brüsszel, 2017. szeptember 19., https://europa.eu/rapid/press-release_IP-17-3193_hu.htm


[79] Zárójelentés a kölcsönös értékelések hetedik fordulójáról: „A számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtása és működése"– A Tanács tájékoztatása, Brüsszel,2017. október 9. 16. o. http://data.consilium.europa.eu/doc/document/ST-12711-2017-REV-1/hu/pdf

- Az uniós tárgyaló felek megállapodtak az európai kiberbiztonság fokozásáról, Brüsszel, 2018. december 10.
  https://europa.eu/rapid/press-release_IP-18-6759_hu.htm
- BIZTONSÁGOS EURÓPA EGY JOBB VILÁGBAN Európai Biztonsági Stratégia, Brüsszel, 2003. december 12.
  https://www.consilium.europa.eu/media/30811/qc7809568huc.pdf
- Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU -Council conclusions (20 November 2017),
  https://www.consilium.europa.eu/media/31666/st14435en17.pdf
- Crisis preparedness: EU launches civil-military crisis management exercise Bruxelles, 16/11/2018 - 15:25, UNIQUE ID: 181116_7,
  https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en
- Digitális egységes piac, Az internetben rejlő lehetőségek kiaknázását nehezítő akadályok felszámolása,
  https://ec.europa.eu/commission/priorities/digital-single-market_hu
- ENISA - Európai Uniós Hálózat- és Információbiztonsági Ügynökség, 06.04.2014,
  https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=legissum:3103_2
- EU Cyber Defence Policy Framework, Brussels, 18 November 2014, 15585/14
  http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf
- EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából
  https://www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/
- Európai Bizottság, Sajtóközlemény, Brüsszel, 2012. július 9. Számítástechnikai bűnözés: az uniós polgárok aggódnak a személyes adatok és az online fizetési műveletek biztonsága miatt,
  https://europa.eu/rapid/press-release_IP-12-751_hu.htm?locale=en
- Europan Centre of Excellence for Countering Hybrid Threats. What is Hyrid CoE?
- European Centre of Excellence for Countering Hybrid Threats.
- George ALLISON: NATO conducts Crisis Management exercise. UK Defence Journal. [online] Source:
  https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/ (Accessed on: 04/07/2019)
- Hálózati és információs rendszerek kiberbiztonsága, ÖSSZEFOGLALÓ AZ ALÁBBI DOKUMENTUMRÓL: (EU) 2016/1148 irányelv – hálózati és információs rendszerek kiberbiztonsága,
  https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148
- Honvédelmi Minisztérium, 2017. május 30.; Jegyzőkönyv az Országgyűlés Külügyi bizottságának 2017. június 7-én, szerdán, 10 óra 07 perckor az Országház főemelet 55. számú tanácstermében megtartott üléséről
- Hybrid CoE Supports Informal NAC-PSC Discussion, September 28, 2018.
- Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.
  https://www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
- Javaslat Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari ó, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról. Európai Bizottság, Brüsszel, 2018. 9. 12. COM(2018) 630 final
- Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést, Az EU Tanácsa, Sajtóközlemény, 2018. 12. 19., https://www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

- Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról, KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, AZ EURÓPAI TANÁCSNAK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK, Brüsszel, 2019.6.14. JOIN(2019) 12 final, 9. o. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN
- JELENTÉS AZ EURÓPAI BIZTONSÁGI STRATÉGIA VÉGREHAJTÁSÁRÓL – A biztonság megteremtése a változó világban, 13-14. o. https://www.consilium.europa.eu/media/30811/qc7809568huc.pdf
- Jochen Rehrl (ed.). Handbook on cyber security. The Common Security and Defence Policy of the European Union, irectorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018, https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1
- Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation, 2016.
- Kiberbiztonság Európában: szigorúbb szabályok és nagyobb védelem, https://www.consilium.europa.eu/hu/policies/cybersecurity/
- Kovács László: Kiberbiztonság és –stratégiaKiberbiztonság és –stratégia. Dialóg Campus, Budapest, 2018, 85. o. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf
- Közös jövőkép, közös fellépés: Erősebb Európa Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf 15. o.
- Közös közlemény az Európai Parlamentnek és a Tanácsnak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése”, Brüsszel, 2017.9.13. JOIN(2017) 450 final, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en
- Mariusz Maciejewski - Frédéric Gouardères: Az európai digitális menetrend, 05. 2019. Ismertetők az Európai Unióról, Európai Parlament, http://www.europarl.europa.eu/factsheets/hu/sheet/64/az-europai-digitalis-menetrend
- Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016; 29 November 2017.
- Sikeres kísérleti projekt hatására nőtt az uniós intézmények kiberbiztonsága, Európai Bizottság, Sajtóközlemény, Brüsszel, 2012. szeptember 12., https://europa.eu/rapid/press-release_IP-12-949_hu.htm
- TERVEZET – A TANÁCS KÖVETKEZTETÉSEI A ROSSZ SZÁNDÉKÚ, KIBERTEVÉKENYSÉGEKKEL SZEMBENI KÖZÖS UNIÓS DIPLOMÁCIAI INTÉZKEDÉSEK KERETÉRŐL („KIBERDIPLOMÁCIAI ESZKÖZTÁR”), Brüsszel, 2017. június 7. (OR. en) http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/hu/pdf
- UNIÓS KIBERVÉDELMI SZAKPOLITIKAI KERET, (2018. ÉVI NAPRAKÉSSZÉ TETT VÁLTOZAT), Brüsszel, 2018. november 19. (OR. en) 14413/18, 2. o. http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf
- Permanent Structured Cooperation (PESCO)’s projects – Overview, 2019, https://www.consilium.europa.eu/media/39762/pesco-overview-of-first-collaborative-of-projects-for-press.pdf
- Zárójelentés a kölcsönös értékelések hetedik fordulójáról: „A számítástechnikai bűnözés megelőzését és az ellene folytatott küzdelmet érintő európai szakpolitikák gyakorlati végrehajtása és működése”– A Tanács tájékoztatása, Brüsszel,2017. október 9. 16. o. http://data.consilium.europa.eu/doc/document/ST-12711-2017-REV-1/hu/pdf

# 3. BONNYAI TÜNDE: KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELEM

## 3.1. Kiberbiztonság a mindennapokban[80]

Az új évezred egyik legjellemzőbb sajátossága, hogy a technológiai fejlődés újabb és újabb produktumai mellett egyre több olyan kifejezést használunk, amelyekben szerepel a biztonság, az infokommunikáció, az informatikai védelem, a 4G, a smart city, a big data, a BYOD kifejezés, illetve az „IT-", a „felhő-" vagy a „kiber-" előtag. Az információs társadalom tagjainak egyre nagyobb hányada éli meg a XXI. század által nyújtott lehetőségeket kihívás helyett előnyként, probléma helyett eszközként, ami elvezet minket abba a digitális korba, ahol az Y generáció unokái már az érintőképernyők és önjáró készülékek világát élik majd.

Felmerülhet a kérdés, hogy vajon mindezek mentén párhuzamosan növekszik-e a infokommunikációs eszközök biztonságos használatával kapcsolatos tudás mértéke is, vagy a rutinná váló, megszokott kényelem, az egyszerűbb és gyorsabb ügyintézés, az elérhetőség és az állandónak tűnő rendelkezésre állás elaltatja az ésszerű óvatosságot? A kérdést vizsgálhatjuk az egyén, a szervezet, a közösség és a társadalom szintjén egyaránt, de napjainkban mégis általánosságban kijelenthetjük, hogy az ez irányú tudatosság, védekező reflex, önvédelmi képesség még nem éri el azt a szintet, amit kielégítőnek nevezhetünk.

Mindezt tovább erősítik az elmúlt évek összehangolt, globális és széles spektrumú célpontok ellen irányuló, kibertérben végrehajtott támadásai. Többféle példát említhetünk abban a relációban, amikor a kibertérből érkező fenyegetés adatvesztéssel, működésre gyakorolt súlyosan negatív következményekkel, gazdasági károkozással is járt. Az Amerikai Egyesült Államok egyik legnagyobb hitelbírálója, az Equifax ellen elkövetett adatlopás célú támadásnak 2017-ben kb. 145 millió amerikai személy – és további kanadai, illetve brit állampolgárok – látták kárát. Az adatlopás során nevek, születési dátumok, lakcímek, TB számok, vezetői engedély azonosítók és bankkártya adatok kerültek illetéktelen kezekbe. Ilyen mértékű és körű adatvesztés során már számolni lehet azzal a lehetőséggel, hogy az eltulajdonított adatokat személyazonosság lopásra, illetéktelen hitelfelvételre, fegyvervásárlásra vagy akár politikai célokra is felhasználják. A kompromittált adatok köre mellett rendkívül súlyos körülménynek tekinthető, hogy a sérülékenységre – amelyet a támadók kihasználtak – már volt patch, de a két hónapja közzétett biztonsági frissítést az illetékesek nem végezték el a hitelbíráló cég informatikai rendszerein.

Az informatikai eredetű támadások között a legismertebb példa mégis a WannaCry zsarolóvírus döbbenetes gyorsasággal bekövetkezett terjedése és károkozása 2017 májusában. Ismert volt a módszer, de soha nem látott méreteket öltött a kiterjedés, olyan nélkülözhetetlen rendszereket is érintve, amelyek hozzáférhetőségének korlátozása nem csak a gazdasági veszteség, hanem az élet- és vagyonbiztonság szempontjából is rendkívüli kihívást jelentett. A korábban megismert zsarolóvírusokhoz képest 2017-ben a WannaCry lett a ransomware támadások eddigi legnagyobb károkat okozó vírusa.

---

[80] Néhány kiemelkedő incidens kapcsán a fejezet végén lévő Irodalomjegyzékben hasznos linkek találhatóak.

Tette ezt azzal, hogy a mintegy 300 ezer érintett között Nagy-Britannia egészségügyi rendszerét, a spanyol Telefónica telekommunikációs vállalatot, a német Deutsche Bahn vasúttársaságot, a FedEx amerikai székhelyű, globális szállítmányozó céget is sikerrel bénította meg, azok elektronikus információs rendszereinek elérhetetlenné tételével. A négynapos támadás egy 2017 márciusában közzétett Microsoft sérülékenységet használt ki, de globális volumenét azzal érte el, hogy a fertőzött gépek LAN/WAN kapcsolatait is kihasználva terjedt.

Az említett támadások formája, de legfőképpen célkitűzése jelentős mértékben eltér, míg az elsők esetében kifejezetten a személyes adatok megszerzése volt a támadók célja, a zsarolóvírus általi támadás az informatikai rendszer(ek)ben tárolt információk teljes körének blokkolására és közvetlen anyagi haszonszerzésre irányult. Egy független kutatóintézet, a Ponemon Institute 2017-ben arra a megállapításra jutott, hogy az adatvesztések által okozott károk átlagos értéke az előző évekhez képest várhatóan 10%-kal csökken 2018-tól, ugyanakkor az adatvesztések mérete 2%-kal növekszik. Ez azt feltételezi, hogy az egyes, biztonsági célú intézkedések okán az adatvesztések száma nem feltétlenül változik, de a biztonsági követelményeknek történő jobb megfelelés által a lehetséges adatvesztés kisebb károkat okoz.

Történt mindez alig 10 évvel azután, hogy Észtországban, a világsajtóban is komoly visszhangot váltottak ki a tallinni szovjet hősi emlékmű eltávolítása miatt kitört zavargások. Azt azonban akkor még kevesebben tudták, hogy az eseményt követő néhány napon belül jelentős károkkal járó kibertámadások indultak meg az észt parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. Az információs társadalom történelmének első „dokumentált" támadásainak eredetét néhány esetben sikerült orosz szerverekig visszavezetni, de Moszkva értelemszerűen tagadta, hogy köze lenne az eseményekhez, miközben szakértők megállapításai szerint egyértelmű, hogy a célpont a balti állam online infrastruktúrájának használhatatlanná tétele, és ezen keresztül az észt gazdaság és telekommunikáció megbénítása volt. Az e-ügyintézés tekintetében már akkor rendkívül fejlett ország adatforgalmát irányító szerverek naponta omlottak össze, a weboldalak látogatottsági mutatói az egekbe szöktek, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről a mértéktelen megkeresések következtében, míg mások (például a rendőrség honlapja) többet álltak, mint amennyit működtek. Az online pénzátutalások rendszere, a webes kereskedelem nagyrészt megszűnt, illetve erősen akadozott. Az elkövetők kiléte és az elkövetés motivációja több összeesküvés-elméletre is okot adott, ugyanakkor a legfontosabb üzenete mindenképpen az volt, hogy egy ország az informatikai rendszerei által különböző kockázatoknak van kitéve, amelyekkel szembeni ellenálló képessége felértékelődik.

A teljesség igénye nélkül felsorolt példák alapján megállapítható, hogy magánszemélyektől egészen a globális tevékenységet végző multinacionális vállalatokon át, a közigazgatási szervekig mindenki célpontja, és így áldozata lehet a kibertérben megjelenő fenyegetéseknek. Az ezekből eredő következmények, hatások csökkentése érdekében világszerte kiemelt feladat a kibervédelmi intézkedések foganatosítása, a biztonságos internethasználatra törekvés terjesztése, a szabályozott környezet kialakítása. A biztonság informatikai szempontú vizsgálata természetesen nem újkeletű kérdéskör, a biztonságpolitikai alapelvek egyikeként a XXI. század egyik legmeghatározóbb szegmense, ugyanakkor kijelenthető, hogy a kiberbiztonság tényleges értelmezése, annak megteremtésére irányuló tudatos kezdeményezések az elmúlt évtized vívmányai.

## 3.2. Európai Uniós törekvések és követelmények

Az Európai Unió, mint gazdasági közösség kiemelt figyelmet szentel a biztonság kérdéskörére, annak szegmenseire. Ennek egyik fő pillére az 1993-as maastrichti szerződésben életre hívott *közös kül- és biztonságpolitika*, amely által valamennyi tagállam törekszik a békére és annak tartós megőrzésére, a biztonság nemzetközi szintű erősítésére, az ehhez szükséges nemzetközi együttműködések fokozására. Mindezek a demokrácia, a jogállamiság és az alapvető emberi és szabadságjogok tiszteletben tartása mentén valósulnak meg. A közös kül- és biztonságpolitika, mint alappillér, a 2007-es lisszaboni szerződés által megerősítést nyert, majd a további szakpolitikai stratégiák révén önálló biztonsági területeken (pl.: egészségügyi biztonság, élelmiszerbiztonság, humanitárius segítségnyújtás, környezetbiztonság, energiabiztonság stb.) is továbbfejlődött. Az Európai Unió közös kül- és biztonságpolitikájának elsődleges rendeltetése, hogy elősegítse a konfliktusok megoldását és a kölcsönös megértést tagállami szinten, illetve a külső dimenzióban egyaránt. Az EU folyamatosan fejlődő partnerségi kapcsolatokat ápol azokkal az országokkal, amelyek meghatározóak a nemzetközi politikai-gazdasági színtéren, valamint számos feltörekvő országgal és regionális tömörüléssel is. Fontos hangsúlyozni a biztonság és védelem aspektusát vizsgálva, hogy az Európai Unió nem rendelkezik állandó hadsereggel, hanem szükségszerűen, eseti alapon létrehozott fegyveres erőkre támaszkodik, amelynek állományát és képességeit a tagországok bocsátják rendelkezésére. Ilyen elven működnek az EU missziói a világ válságövezeteiben, amelyek célkitűzése, hogy felügyelje és megőrizze a közbiztonságot, részt vegyen békefenntartási műveletekben vagy humanitárius segítséget nyújtson.

Az éves rendszerességgel – a Külügyi Bizottság által – készített közös kül- és biztonságpolitika végrehajtásáról szóló jelentésekben jól nyomon követhető a kiberbiztonsági szempontok térnyerése. 2010-ben a Külügy Bizottság hangsúlyozta, hogy a nem hagyományos (pl.: számítógépes) fenyegetésekkel szembeni felkészülést jobban össze kell hangolni a tagállamok feletti szinten, ezért szükséges elvégezni a kapcsolódó fenyegetések és igények mélyreható elemzését, majd az eredmények alapján egy olyan többdimenziós és átfogó európai kiberbiztonsági stratégiát kell kidolgozni, amely alkalmas a számítógépes támadásokkal szembeni védekező képesség fokozását EU-szerte ösztönözni.

2016-ban és 2017-ben pedig már markánsan az szerepelt a jelentésekben, hogy az EU tagállamai egyedül nem képesek kezelni a XXI. század kihívásait, ezért még nagyobb hangsúlyt kell fektetni a közös fellépésre, különösen a globális digitális szférában jelentkező veszélyekkel szemben. Külön hangsúlyt kapott a kibertámadások veszélye, úgy is, mint a terrorizmus egyik potenciális megnyilvánulási formája. Ezek alapján az Európai Parlament célként határozta meg, hogy az uniós együttműködéseket és a közös kül- és biztonságpolitika területén meglévő kapacitásokat az információs hadviselés szempontjából is fokozni kell. Mindezek érdekében az Európai Parlament felszólította a tagállamokat, hogy fokozzák erőfeszítéseiket annak érdekében, hogy az EU még inkább képes legyen a hibrid- és kiberfenyegetéseket kezelni, a félretájékoztatás elleni fellépését hatékonyabbá tenni, illetve a közös kockázat- és sebezhetőségelemzési módszereket fejleszteni, összességében a kiberbiztonság javításához hozzájárulni. Ide tartozik továbbá, hogy az EP hangsúlyozta a kiberbűnözéssel kapcsolatos beazonosítások képességének javítását és felhívta a tagállamokat a NATO és az USA, illetve egyéb partnerekkel történő szorosabb együttműködésre a kibervédelem területén.

2018-ban ugyanezen éves jelentés sokkal inkább az EU-n belüli szolidaritás hangsúlyozását célozta, kisebb mértékben tartalmazott a biztonság, azon belül a kiberbiztonságra vonatkozó irányvonalakat. Kijelentette, hogy a belső és külső biztonság egyre fokozottabban összefügg egymással, amely miatt meg kell erősíteni az EU külső beavatkozásokkal szembeni ellenálló-képességét, mind a kritikus infrastruktúrák védelmére irányuló preventív intézkedések, mind a kibertámadásokkal és hibrid fenyegetésekkel kapcsolatos ellenlépések összehangolása érdekében.

Mindezekre alapozva kezdődött meg a kétezres évek elején a kiemelt jelentőséggel bíró szolgáltatások és infrastruktúrák védelmének prioritásként történő kezelése, majd a biztonságuk megteremtésének, fokozásának célkitűzését és közösségi módszertanát megfogalmazó EU normatívák kidolgozása. Már a 2001-ben elkövetett terrortámadások megindították azt a cselekvési hullámot, amelynek révén az Euró-

pai Unió eljutott a kritikus infrastruktúrák védelmére irányuló egységes jogi szabályozás megteremtésének igényéig. A tengerentúli tapasztalatok és néhány uniós tagállam meglévő gyakorlata alapján kezdődött meg az uniós kritikus infrastruktúra védelemre vonatkozó projekt kidolgozása. A kezdeményezés elsődleges célja volt, hogy nem tagállami, hanem együttműködésen alapuló, közösségi szintű program alakuljon ki, amely ötvözi az uniós szabályozást a tagállami jellegzetességekkel.

Ennek egyik eredménye volt az Európai Tanács 2003-as *biztonsági stratégiá*ja[81], amely még nem említette konkrétan biztonsági kihívásként a kiberfenyegetéseket, annak ellenére, hogy több tagország (pl.: Németország) már ekkor is hangsúlyozta az infokommunikációs technológiák fontosságát a szolgáltatásokat biztosító infrastruktúrák védelme terén. A stratégia felülvizsgálatát 2008-ban kezdeményezte először az Európai Tanács, ekkor került a potenciális fenyegetések közé a tagállamok IT-rendszerei ellen elkövetezett támadások fogalma, mint az ún. számítógépes biztonság kérdéskörében jelentkező kihívás.

Az Európai Tanács 2004. júliusi ülésén, a közelmúlt terrortámadásai (9/11 és 2004. Madrid) révén, nyomatékos hangsúlyt kapott az európai állampolgár biztonságérzete, vagyis az, hogy egy európai átlagember mit vár el a hétköznapok biztonságával kapcsolatban. A szükséges intézkedések megtétele érdekében az Európai Bizottság felkérést kapott a kritikus infrastruktúrák védelmére összpontosító, átfogó stratégia előkészítésére. Az Európai Tanács 2004. decemberi ülésén elfogadták a *Kritikus Infrastruktúrák Európai Programjának* (European Programme for Critical Infrastructure Protection, EPCIP) kialakítására vonatkozó előterjesztést, amely a terrorizmus elleni küzdelemmel kapcsolatos akcióterv részeként jelent meg. 2005 januárjában egy konkrétabb célkitűzéseket tartalmazó javaslatot is előterjesztettek, ami elsősorban egy többéves kutatási projekt megkezdését szorgalmazta az unió területén található kritikus infrastruktúrák mindennemű sebezhetőségének feltérképezésére. A projekt egy közös európai kockázat-elemzési rendszer kidolgozását, valamint olyan információ megosztásra alkalmas felület kialakítását javasolta, amely révén a tagállamok, a Bizottság és a Tanács az említett infrastruktúrákkal kapcsolatos tevékenységet folyamatosan nyomon tudja követni. Tartalmazta egy állandó válságkezelő központ életre hívását is, a tagállami és európai szinten működésben lévő korai figyelmeztetési (early warning system) és sürgősségi rendszerek (emergency system) összefogására, összehangolására vonatkozóan. A londoni robbantások utáni, 2005. július 13-án tartott rendkívüli tanácsülésen a tagállamok megerősítették a terrorizmus elleni küzdelem melletti határozott elkötelezettségüket, továbbá ehhez kapcsolódóan kihangsúlyozták, hogy az uniós állampolgárok és a kritikus infrastruktúrák védelmére irányuló egységes fellépéssel törekedni kell a fenyegetettség és kiszolgáltatottság csökkentésére. A fenti folyamatok eredményeként 2005 novemberében a Bizottság kiadta a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló *Zöld Könyvét*[82], amely a leendő EU-s programmal kapcsolatos alapvető elveket, célkitűzéseket, definíciókat és intézkedéseket rögzítette.

Elsődleges célja volt, hogy felhívja a figyelmet egy-egy terület megválaszolatlan kérdéseire, illetve aktív együttműködésre ösztönözze az egyes szektorok képviselőit. Végül – egy közel 7 éves folyamatot követően – 2008 decemberében megjelent az *európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK Irányelv*[83] (a továbbiakban: CIP Irányelv), az EPCIP – mint átfogó EU-s program – végrehajtására vonatkozó, a tagállamok által jogharmonizáció keretében átültetendő mechanizmust meghatározó szabályozás. Az ebben foglalt tagállami kötelezettségek egyik legfontosabb eleme az ún. üzemeltetői biztonsági terv (operator security plan), amelyben az egyes kritikus infrastruktúrák eszközrendszerét, azok védelmét szolgáló intézkedéseket szükséges összefoglalni. Ez a terv kiemelt hangsúllyal nevesíti a fenyegetettségi forgatókönyveket, a hatásalapú kockázatelemzés szükségességét, és a biztonsági/védelmi intézkedések rangsorolását. Utóbbiak egyik legmeghatározóbb összetevője az információs rendszerek biztonsága, és az ezzel kapcsolatos tudatosság növelése.

---

81 Európai Bizottság, 2003. – http://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf

82 Európai Bizottság, 2005 .– https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN

83 Európai Tanács, 2008. – https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=ENb

Ennek folyományaként és a 2003-as biztonsági stratégia már említett felülvizsgálatára válaszul készült 2009-ben az *„Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása”* című közlemény[84] (a továbbiakban: Közlemény), amely az időközben hatályba lépett CIP Irányelv szerinti létfontosságú rendszerek informatikai infrastruktúráinak védelméről szól, és elsőként fogalmazza meg EU szintű politikai célkitűzésként az információs társadalom védelmét. A közlemény közös gyűjtőfogalomként, információs és kommunikációs technológiák néven említi azokat a rendszereket, szolgáltatásokat, hálózatokat és infrastruktúrákat, amelyek egy része létfontosságú az európai gazdaság és társadalom számára, mivel alapvető termékek és szolgáltatások előállítására szolgálnak, vagy más kritikus infrastruktúrák alapját képezik. Itt érzékelhető tehát először, hogy az EU megközelítése szerint két esetben beszélhetünk kritikus informatikai infrastruktúráról[85]:

- egyrészt, amikor maga az infrastruktúra az infokommunikációs technológiák csoportjába tartozik és az általa biztosított szolgáltatás létfontosságú,
- másrészt, amikor valamely kritikus infrastruktúra információs rendszeréről van szó, amely alapvető feltétele az adott infrastruktúra működésének, így a szolgáltatás biztosításának.

A megelőzés, vagy a károkozás mértékének lehető legalacsonyabb szinten tartása érdekében a Közlemény olyan európai politikai irányvonalat határozott meg, amely több párhuzamosan zajló EU-s törekvést hozott az EPCIP égisze alá:

- Ilyen a 2006-ban elfogadott *biztonságos információs társadalomra irányuló stratégia*[86] főbb elemeinek végrehajtása, így különösen az IKT-infrastruktúrák ellenálló képességének fokozása, amelynek szükségességét a Tanács külön állásfoglalásban is támogatta.
- Hasonlóan ide tartozik, hogy a fenti stratégia tovább erősítette a 2004-ben életre hívott, majd 2008-ban meghosszabbított mandátumú, *Európai Hálózat- és Információbiztonsági Ügynökség* (ENISA) szerepét.
- Szabályozói szempontból meg kell említeni továbbá az *elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások keretszabályozásának átalakításáról szóló 2007-es Európai Bizottsági javaslat csomag*ot[87], amely már új rendelkezéseket tartalmazott a szolgáltatások biztonságára és a hálózatok integritására vonatkozóan, elsősorban az üzemeltetői felelősség fokozására és a feltárt kockázatok mentén történő üzletmenet-folytonosságra összpontosítva. Ugyanez a módosítás tartalmazta először, hogy a hírközlő hálózatokat üzemeltetők küldjenek értesítést az illetékes hatóságoknak a biztonság megsértésének meghatározott eseteiről. Ezek az intézkedések már abba az irányba mutattak 2007-ben, hogy a kritikus informatikai infrastruktúrák általános értelemben vett biztonságát, így az alapvető ellenálló képességét javítani szükséges.

A Közlemény egyúttal kijelentette, hogy a kritikus informatikai infrastruktúrákat fenyegető veszélyek között egyre kifinomultabbak a számítógépes támadások (vírusok, férgek, egyéb rosszindulatú malware-k növekvő száma, botnetek terjedése, kéretlen levelek terjedése), amelyeket sokszor már kimondottan profitszerzési, vagy politikai céllal hajtanak végre. Megállapítást nyert tehát 2009 tavaszán, hogy

---

84 Európai Bizottság, 2009. – https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52009DC0149

85 A következetesen kritikus informatikai infrastruktúrákként említett rendszerek jelentőségének alátámasztásául a Világgazdasági Fórum 2008-as becslését hangsúlyozta a közlemény, amely szerint a következő évtizedben (2019-ig) 10-20% esélye van annak, hogy jelentős üzemzavar keletkezik a kritikus informatikai infrastruktúrák területén, amely legalább 250 milliárd dollár kárt okozna a gazdaságnak világszinten. A viszonyíthatóság érdekében: a 10 éves időintervallumra prognosztizált 250 milliárd dolláros károkozás 25 milliárd dollár értékű károkat feltételez évente. Csak a Petya és a WannaCry zsarolóvírusok 2017-ben 3 hónap alatt összesen kb. 4 milliárd dolláros kárt okoztak világszerte.

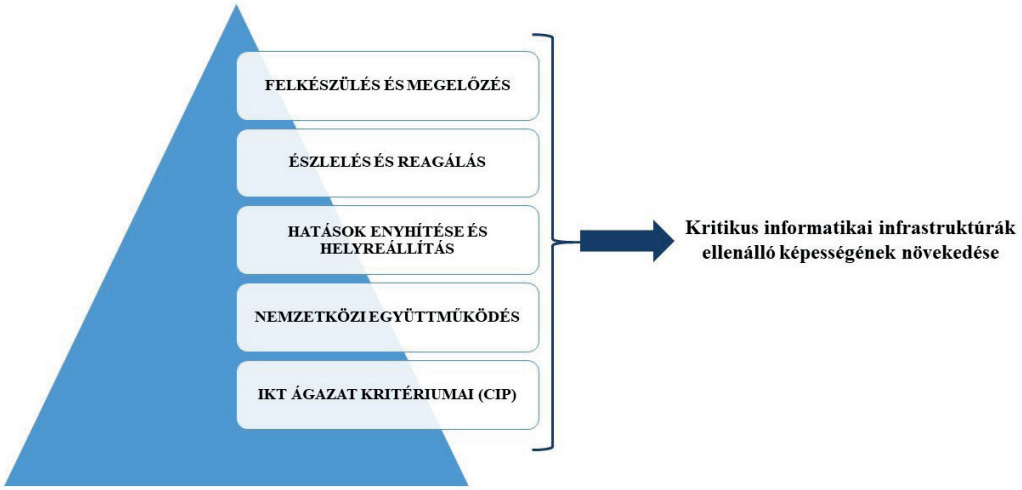
86 Európai Bizottság, 2006. – https://ec.europa.eu/transparency/regdoc/rep/1/2006/HU/1-2006-251-HU-F1-1.Pdf

87 Európai Bizottság, 2007. - https://ec.europa.eu/transparency/regdoc/rep/1/2007/HU/1-2007-697-HU-F1-1.Pdf; https://ec.europa.eu/transparency/regdoc/rep/1/2007/HU/1-2007-698-HU-F1-1.Pdf; https://ec.europa.eu/transparency/regdoc/rep/1/2007/HU/1-2007-699-HU-F1-1.Pdf

a társadalom, a gazdaság és a politika egyre növekvő függősége a kritikus informatikai infrastruktúrák rendelkezésre állásától kiemelt jelentőségű. Mindezt súlyosbítja, hogy a határokon átívelő kapcsolódások, illetve más infrastruktúráktól való közvetett vagy közvetlen függőségük, valamint a tény, hogy a számítógépes támadásokkal szembeni sérülékenységük markáns hatást gyakorolhat teljes országok, régiók működésére, az ellenálló képességük szisztematikus fokozása elengedhetetlen. Mindezek érdekében a CIP irányelvben foglaltakon túl a következő feladatok nevesítésére került sor:

- közösségi erőfeszítések megtétele a nemzeti szemléletmódok különbözőségének csökkentésére, a tudatosítás, az általános ismeretek szintjének növelése, a közös politikai célok elfogadásának ösztönzése, illetve a tagállami együttműködési formák erősítése útján;
- egységes európai irányítási modell kialakítása a kritikus informatikai infrastruktúrák számára, az állami és a magánszektorbeli szereplők partnerségeinek továbbfejlesztése által (tagállami szinten létező partnerségek mintájára egy, az ENISA hatáskörét kiterjesztő irányítási keret életre hívásával);
- a korai figyelmeztető és reagáló képesség célirányos fejlesztése, a nem hivatalos keretek közötti, vagy két/többoldalú megállapodások helyett, valamennyi tagállamban nemzeti ellenőrzés alatt álló számítástechnikai katasztrófaelhárító csoportok (CERT) létrehozása, amelyek rendelkezésre állása és működése közös alapképességeken nyugszik.

Az észtországi események tapasztalatai[88] alapján a tagállamok egyetértettek abban, hogy elsősorban megelőző intézkedésekkel és kockázatfelmérés, -értékelés, -kezelés útján, a biztonságot veszélyeztető esemény bekövetkezésekor előre eltervezett folyamatok bevezetésével mérsékelhetőek a károk. Szintén megállapítást nyert, hogy a szükséges és elégséges információk, illetve a bevált gyakorlatok szervezett keretek közötti, uniós kereteken belüli megosztása jelentős előrelépést hozhatna az egységes szintű védelmi képességek kialakításában. Mindezek érdekében az együttműködés meglévő eszközeit – így például az ENISA-t – meg kell erősíteni és további, új eszközöket szükséges létrehozni. Az EU eddigi, a kritikus informatikai infrastruktúrák védelme érdekében tett törekvéseit – tulajdonképpen a Közlemény érdemi tartalmi elemeit – az alábbi pillérek szemléltetik:




*1. ábra: A kiberbiztonság fokozásának fő pillérei*

A megvalósítást egy cselekvési terv (közismert megnevezése: CIIP Cselekvési terv) ösztönözte, amely az egyes pillérekhez rendelt konkrét tagállami feladatokat és az általuk elérni kívánt célokat tartalmazta (Közlemény 5. fejezete).

[88] 2008 májusában a NATO Észtországban hozta létre a NATO Kooperatív Kibervédelmi Kiválósági Központját, amely elsősorban oktatási, kutatási és fejlesztési tevékenységet végez. A központ létrehozására már 2003-ban javaslatot tett Észtország – akkor még nem NATO tagállamként – és a 2007-es események erősítették meg ennek szükségességét.

A 2003 óta zajló folyamatok fentiekben vázolt „kijövő eredményeit" alapul vette a 2010 márciusában kiadott, tíz éves időintervallumot felölelő *Európa 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégiája*[89] (a továbbiakban: EU 2020), amelynek megjelenését követően egyre nagyobb teret kapott a kibervédelem kérdésköre. Az EU 2020 ugyanis a közösség strukturális hiányosságai között azonosította az IKT elégtelen mértékű alkalmazását, majd megállapította, hogy az Európai Unió intelligens növekedésének egyik alappillére kell legyen annak biztosítása, hogy az IKT-k innovatív fejlesztéseiből új termékek és szolgáltatások szülessenek. Ide tartozik továbbá az a megállapítás, hogy Európa elmarad a nagysebességű internet használata terén is, ami jelentős mértékben befolyásolja az EU innovációs képességét – így az áruk és szolgáltatások terjesztését. Az EU 2020 összesen öt területen javasolt közösségi célokat, amelyek megvalósítása érdekében hét kiemelt kezdeményezést nevesített. Ebből kettő az „Innovatív Unió" és az „Európai digitális menetrend" kiemelten fontos a kritikus informatikai infrastruktúrák szempontjából. Mindkettő alapvetően befolyásolja az EU tagállamainak informatikai infrastruktúrájának fejlődését, így azok biztonsággal kapcsolatos szegmenseit is. Az EU 2020-ban foglalt célkitűzések tehát alapvető feltétellé tették a bizalom és a biztonság megteremtését az IKT-k széleskörű elterjedésének – vagyis az „intelligens növekedésnek" – eléréséhez. Minden érintett számára egyértelműsítették, hogy a biztonság és az ellenálló képesség fokozása a megelőzésre, a felkészültségre és a tudatosságra épül, amely kiemelt figyelemmel van a kibertámadások, összességében a kiberbűnözés egyre kifinomultabb formáira is.

Ugyanezen év szeptemberében látott napvilágot az Európai Bizottság *információs rendszerek elleni támadásokról szóló irányelv-javaslata*[90], amelynek célja a kiberbűnözés elleni küzdelem megerősítése és a botnetek elleni fellépéssel kapcsolatos új rendelkezések bevezetése volt. Ezzel párhuzamosan jelent meg az *ENISA megerősítésére és modernizálására vonatkozó*[91], szintén Bizottsági javaslat, amely már konkrétan megfogalmazta, hogy a bizalom erősítése keretében, valamint a hálózatbiztonság javítása érdekében szükséges a tagállamok és a magánszektor szereplőinek szakszerű felkészültségét biztosítani.

A következő mérföldkőnek tekinthető az Európai Bizottság 2011 márciusában kiadott, *„a kritikus informatikai infrastruktúrák védelméről szóló közleménye, Eredmények és következő lépések: a globális kiberbiztonság felé"*[92] címmel. A dokumentum legfontosabb része a CIIP Cselekvési terv hatásvizsgálatának eredményei alapján készített összefoglalás, amely az öt pillér (lásd: 1. sz. ábra) mentén foglalta össze az akkori helyzetet. A helyzetelemzés alapján, valamint a tapasztalatokra építve a Bizottság új feladatokat fogalmazott meg:

- nemzetközi alapelvek kidolgozása az internet ellenálló képességével és stabilitásával kapcsolatosan;
- nemzetközi stratégiai partnerségek kialakítása gyakorlatok, biztonsági incidensek kezelése és az együttműködések fokozása mentén;
- a globális hatást gyakorló technológiai fejlesztések (pl.: felhők) iránti bizalom erősítése szabályozás stratégiák útján;
- az EU felkészültségének javítása a nemzeti/kormányzati CERT-ekből álló hálózat 2012-ig történő létrehozásával;
- európai kiberincidens veszélyhelyzeti terv elkészítése 2012-ig és rendszeres kiberbiztonsági gyakorlatok tartása.

A meghatározott fő feladatok alapján a korábbi CIIP Cselekvési terv kiegészítésre került, és a dokumentum mellékleteként látott napvilágot. Az egyes pillérekkel kapcsolatos eredményeket és következő lépéseket tartalmazza, amely alapján a célkitűzések megvalósítása folytatható.

---

89 Európai Bizottság, 2010. – https://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf

90 Európai Bizottság, 2010. – https://ec.europa.eu/transparency/regdoc/rep/1/2010/HU/1-2010-517-HU-F1-1.Pdf

91 Európai Bizottság, 2010. – https://ec.europa.eu/transparency/regdoc/rep/1/2010/HU/1-2010-521-HU-F1-1.Pdf

92 Európai Bizottság, 2011. – https://ec.europa.eu/transparency/regdoc/rep/1/2011/HU/1-2011-163-HU-F1-1.Pdf

2012-ben az uniós döntéshozás meghatározó intézményeként az Európai Parlament állásfoglalást készített a fenti közleményről *(Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról*[93]*,* a továbbiakban: Állásfoglalás*)*. Az Állásfoglalás kimondottan előremutató célokat fogalmazott meg, ugyanakkor itt kezdődhetett a kritikus infrastruktúrák és a kritikus információs infrastruktúrák elhatárolása, amely napjainkban is több félreértésnek, vitának, eltérő megközelítésnek táptalaja. Az állásfoglalás 2. pontjában megállapították ugyanis, hogy a *„kritikus információs infrastruktúra védelme terén tett erőfeszítések nemcsak a polgárok általános biztonságát, hanem a polgárok biztonságérzetét is erősítik, továbbá fokozzák a polgároknak a védelmük érdekében tett kormányzati intézkedésekbe vetett bizalmát is"*. Ide kapcsolódóan fontos megemlíteni, hogy a 13. pontban az Európai Parlament állást foglalt az ENISA szerepét illetően, amelynek értelmében az „*kulcsfontosságú szerepet tölthet be európai szinten a kritikus információs infrastruktúrák védelme terén azzal, hogy technikai szakértelmet nyújt a tagállamoknak és az Európai Unió intézményeinek, valamint jelentéseket és elemzéseket készít az információs rendszerek biztonságáról európai és globális szinten".* Mindezen megállapítások *„A kritikus informatikai infrastruktúrák megerősítésére szolgáló nemzeti és uniós intézkedések"* cím alatt kerültek felsorolásra. A dokumentumban többször is felváltva szerepelnek a kifejezések, így nem jelenthető ki egyértelműen, hogy az EU-s terminológia külön kezeli a kritikus informatikai infrastruktúra és a kritikus információs infrastruktúra fogalmát, tehát az elhatárolásuk sem lenne indokolt. Ettől függetlenül azonban ki kell hangsúlyozni, hogy az Állásfoglalás előrevetítette a jelenleg hatályos irányelvek szakpolitikai irányvonalait a következő intézkedésekkel:

- a kritikus informatikai infrastruktúrák nemzeti és uniós védelme szorosan összekapcsolódik, ezért a szolgáltatás megzavarásával, a megsemmisítésre irányuló kísérletekkel vagy támadásokkal (értsd: biztonsági incidensek) szembeni készültség és védelem érdekében az ellenállóképességre vonatkozó minimumszabványok rendszeres frissítése szükséges;
- a tagállamoknak nemzeti/kormányzati CERT-eket kell létrehozniuk, nemzeti kiberbiztonsági stratégiákat kell kialakítaniuk, rendszeresen kell kiberbiztonsággal kapcsolatos gyakorlatokat tartaniuk, és nemzeti kiberincidens veszélyhelyzeti terveket szükséges kialakítaniuk;
- minden európai kritikus informatikai infrastruktúrára vonatkozóan üzemeltetői biztonsági tervet vagy azzal egyenértékű intézkedést lenne célszerű bevezetni, és biztonsági összekötő tisztviselőket kinevezni;
- a Bizottságnak és a tagállamoknak meg kell tenniük a szükséges intézkedéseket a kritikus infrastruktúrák kibertámadásoktól való védelme érdekében, és képesnek kell lenniük meghatározni olyan eszközöket, amelyek alkalmasak a kritikus infrastruktúrákhoz való hozzáférés hermetikus lezárására, arra az esetre, ha egy súlyos kibertámadás azok megfelelő működését súlyosan veszélyezteti;
- a Bizottság indítványozhatja a biztonságot és ellenálló képességet fokozó minimumszabványok előírását és a nemzeti számítógépes vészhelyzeteket elhárító csoportok (CERT-ek) közötti koordináció javítására vonatkozó kötelező intézkedéseket;
- az Európai Parlament mindezeken túl felkéri a Bizottságot, hogy javasoljon a kritikus ágazatokban (IKT-ágazat és a pénzügyi szolgáltatások, illetve az energiaellátás, a közlekedés, a víz- és élelmiszer-ellátás ágazatában) a biztonsági visszaélések bejelentésére vonatkozó uniós keretet, a tagállamok és a felhasználók kiberbiztonsági eseményekről, számítógépes támadásokról és hálózati zavarokról történő értesítése céljából;
- az Európai Parlament továbbá megkéri a tagállamokat, hogy hozzák létre a kritikus informatikai infrastruktúrák éjjel-nappal működő védelmi szolgálatát, illetve alakítsák ki a nemzeti kapcsolattartó pontok között alkalmazandó közös európai vészhelyzeti protokollokat;
- az Európai Parlament kijelentette, hogy támogatja az ENISA kulcsfontosságú szerepét európai szinten a kritikus információs infrastruktúrák védelme terén, amelyet azonban fokozni szükséges.

[93] Európai Parlament, 2012. – http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0237+0+DOC+XML+V0//HU&language=HU

A kétezres évek első évtizedében bekövetkezett események világszerte arra ösztönözték a döntéshozókat, hogy mind a társadalom közvetlen védelmét, mind a közvetett biztonságát magasabb szinten törekedjenek megvalósítani. Nem volt kérdéses, hogy mindennek már szerves része a kibertér védelme, a megbízható és biztonságos kibertér kialakítására, illetve megőrzésére törekvés. Az EU tagállamai szempontjából is egyértelműen kijelenthető volt, hogy az elmúlt 20 év – tulajdonképpen a vasfüggöny lebontását követő két évtized – olyan változásokat hozott a technológiai fejlődés terén, amely megkövetelte a biztonság egyes szegmenseinek célirányos modernizálását is.

Ezt követve a fentiekben ismertetett uniós törekvések 2013-ban az *Európai Unió kiberbiztonsági stratégiá*jában[94] (a továbbiakban: Stratégia) manifesztálódtak. Olyan markáns kijelentések kaptak helyet a Stratégiában, mint *„a kibertér csak akkor maradhat nyitott és szabad, ha a kibertérben is ugyanazok a normák, alapelvek és értékek érvényesülnek, mint amelyeket az Európai Unió a való életben képvisel”.* Mindez kvázi jogot és kötelezettséget formált arra, hogy a tagállamok szavatolják a virtuális tér biztonságát hasonlóképpen a közbiztonság jogállami intézményéhez. Az egységes digitális piac létrehozásának gondolata, a digitális versenyképesség, az infokommunikációs technológiákban rejlő gazdasági potenciál, a felhőszolgáltatások, az okoseszközök – a felsorolás hosszasan folytatható lenne – mind arra kell ösztönözzék az EU állampolgárait, kormányait és intézményeit, hogy az információs rendszerek zavartalan működésének garantálása legyen az egyik legmeghatározóbb biztonsági célkitűzés. Fontos hangsúlyozni, hogy a Stratégia a szubszidiaritás elvének tiszteletben tartása mentén, elsődlegesen tagállami felelősségként determinálta a biztonságos internetes környezettel kapcsolatos kötelezettségeket, de közösségi érdekek, értékek jegyében körvonalazható megoldásokkal kívánta támogatni annak megvalósítását. Az EU-s jövőképet ennek alapján öt stratégiai prioritásban határozták meg, amelyekhez a már meglévő intézkedéseken túl további feladatokat és célokat rendeltek:

| **prioritás** | **meglévő intézkedés** | **feladat/cél** |
|---|---|---|
| **I.**<br>**kibertámadásokkal szembeni ellenálló képesség elérése** | 2001 / hálózat- és információbiztonsági szakpolitika (NIS)<br><br>2004 / ENISA megalakítása | **Szabályozni legalább**:<br>– közös, nemzeti szintű minimum-követelményeket;<br>– illetékes hatóságok kijelölését;<br>– CERT-ek létrehozását;<br>– magánszektor részvételének javítására irányuló ösztönzőket;<br>– közös szimulációs gyakorlatok tartását és a tudatosság javítását. |
| **II.**<br>**számítástechnikai bűnözés drasztikus csökkentése** | Számítástechnikai bűnözéssel kapcsolatos irányelvek | **Megvalósítani legalább:**<br>– irányelvek átültetését a nemzeti jogrendekbe;<br>– Budapesti Egyezmény[95] ratifikálását és végrehajtását minden tagállam részéről;<br>– képességek megerősítését, hiányosságok feltárását és megszüntetését;<br>– Számítástechnikai Bűnözés Elleni Európai Központtal[96] (EC3) történő együttműködés fokozását. |

[94] Európai Bizottság, 2013. – https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=HU

[95] 2001 novemberében, Budapesten elfogadott Számítástechnikai bűnözésről szóló egyezmény, amely 2004. július 1-jén lépett életbe. Az egyezmény célja, hogy védje a számítástechnikai rendszerek, hálózatok, adatok hozzáférhetőségének sérthetetlenségét, azok titkosságát; biztosítsa a rendszerek, hálózatok, valamint az azokban fellelhető adatok visszaélésszerű használatának megelőzését. Az egyezmény bűncselekménnyé nyilvánította az ilyen eseteket, illetve meghatározta a kiberbűnözés elleni hatékony fellépéssel összefüggésben álló felderítési, nyomozati és üldözői tevékenységek végzését nemzeti és nemzetközi szinten biztosító jogköröket és rendelkezéseket.

[96] European Cybercrime Centre, feladata a számítástechnikai bűnözéssel kapcsolatos információk különféle forrásokból való összegyűjtése, a tendenciák és fenyegetések azonosítása, valamint a hírszerzés működésének javítása.

| | | |
|---|---|---|
| **III.**<br>**kibervédelmi politika és képességek fejlesztése a közös biztonság- és védelempolitika égisze alatt** | NATO együttműködési platformok<br>K+F projektek | **Fokozni legalább:**<br>– kritikus számítástechnikai eszközök védelmére irányuló civil és katonai módszerek közötti szinergiákat;<br>– NATO-val történő együttműködés hatékonyságát a kritikus kormányzati, védelmi és más információs infra struktúrák ellenálló képességének növelése érdekében;<br>– Európai Védelmi Ügynökséggel történő együttműködést. |
| **IV.**<br>**kiberbiztonsági ipari és technológiai erőforrások kifejlesztése** | Kutatási és fejlesztési kapacitások | **Kialakítani legalább:**<br>– az EU-ban használt IT-termékek kiberbiztonsági teljesítményre vonatkozó követelményeit;<br>– magánszektor ösztönzését a magas szintű kiberbiztonság megvalósítása érdekében;<br>– magán- és állami szektor számára egy NIS-megoldásokról szóló platformot;<br>– műszaki iránymutatásokat és ajánlásokat az ENISA közreműködésével;<br>– olyan erős IKT ágazati szakpolitikát, ami hozzájárul Európa külföldi technológiáktól való függőségének csökkentéséhez. |
| **V.**<br>**összehangolt nemzetközi szakpolitika létrehozása az EU-n belül a kibertér vonatkozásában** | Ágazati szakpolitikák | **Fejleszteni legalább:**<br>– a kibertérrel kapcsolatos kérdéseket az EU külkapcsolataiban, valamint közös kül- és biztonságpolitikájában;<br>– a kiberbiztonsággal kapcsolatos kapacitásokat és az információs infrastruktúrák ellenálló képességét harmadik országokban. |

*1. sz. táblázat: A Stratégia prioritásai*

Mindezek megvalósításához a Stratégia meghatározta a minimális felelősségi köröket. Körvonalazta a nemzeti szintű hatóságok szerepét és együttműködését, illetve az uniós szintű intézmények központi, felügyeleti jellegű hatáskörét. Az EU viszonylatában az ENISA – a NIS, mint szakpolitika tekintetében, az Europol és azon belül az EC3 – a bűnüldözés kapcsán, míg az Európai Védelmi Ügynökség kimondottan védelmi megközelítéssel foglalkozik a kiberbiztonsággal. Ezen intézményekben képviseltetik magukat a tagállamok és hoznak létre koordinációs platformokat az egyes részfeladatok közösségi szintű megvalósítása érdekében. A Stratégia szerint a három intézmény közötti együttműködést fokozni szükséges, ugyanakkor törekedni kell arra, hogy az egyes tagállamok – a nemzeti jellegükre való különös tekintettel – megőrizzék sajátosságaikat. Kiemeli és hangsúlyozza emellett, hogy a jelentős biztonsági eseményeknél is vizsgálni szükséges a meglévő képességeket, a fejlesztési irányokat mind az egyes tevékenységek folyamatossága, mind a bűncselekményhez kapcsolódás lehetősége, mind pedig egy esetleges kiberkémkedés/kibertámadás nemzetbiztonsági vetületei szempontjából. A Stratégia által a Bizottság tehát 2013-ban konkrétan felkérte az Európai Parlamentet és a Tanácsot – így a tagállamokat –, hogy mihamarabb készítsenek és fogadjanak el egy uniós közös, magas szintű hálózat- és információbiztonságra vonatkozó irányelvet, amellyel közösségi szintű és nemzeti garanciák alakíthatóak ki a kibertér biztonságos és megbízható használatához.

A tényleges szabályozási környezet, amely kötelezettségekkel és érdemi felelősségi körökkel terheli a tagállamokat, közel 4 évet váratott magára. Az Európai Parlament és a Tanács 2016. július 6-án fogadta el *„a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelvét”*[97] (a továbbiakban: NIS irányelv), amely gazdasági szempontok alapján – a belső piac működéséhez viszonyítottan – alapvető szükségletnek

[97] Európai Parlament és Tanács, 2016. – https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148

tartja a hálózati és információs rendszerek, valamint az ezek által biztosított szolgáltatások megbízhatóságát, biztonságát. A NIS irányelv kidolgozása – hasonlóan a kritikus infrastruktúrák védelmére vonatkozó szabályozáshoz – rendkívül hosszadalmas folyamat volt az EU jogalkotási procedúrájának és a témakör kiemelkedő fontosságának köszönhetően. Tartalmi elemeit tekintve számos, a korábbi EU-s szakpolitikai irányokat meghatározó közlemények és állásfoglalások által megfogalmazott szükségletet, törekvést, elvárást tartalmaz.

A NIS irányelv konkrétan célul tűzte ki, hogy a tagállamok biztonsági események megelőzése és kezelése terén tapasztalható – napjainkban markánsan eltérő – felkészültségét egységesen magas szintre fejlessze. Legfontosabb elvárásai ebből adódóan, hogy minden tagállam rendelkezzen minimális képességekkel, szükséges intézményekkel, szabályokkal, valamint a hálózat- és információbiztonság magas szintjét biztosító nemzeti szintű stratégiával. Mindezek megvalósításához több olyan sarkalatos tevékenységet nevesít, amelyek teljesítésével a célkitűzések fokozatosan érhetőek el. Előírja minden tagállam részére, hogy stratégiai szinten foglalja össze nemzeti kiberbiztonsági képességeit, majd azokat megfelelő felelősségi körök, határidők és intézkedések mentén tovább fejlessze. Ehhez a stratégiának – vagy a már meglévő jogszabályi környezetnek – tartalmaznia kell az egész feladatrendszer áttekinthetőségét biztosító szervezeti és szabályozási struktúrával, amelyben jól láthatóan különülnek el az egyes felelősségi körök, és amely lehetővé és alapvetővé teszi az együttműködést a rendszeren belül. A képességek javításának fontos alappillére továbbá, hogy a megfelelő felkészültségi szint is meghatározásra kerüljön, amelyhez az érintetteknek tartaniuk kell magukat. Ahhoz, hogy a szervezetek megfelelően felkészültek legyenek, ismerniük kell a tevékenységükre, működésükre, környezetükre jellemző valós kockázatokat, amelyeket meg kell vizsgálniuk, ki kell értékelniük és a szükséges és elégséges intézkedések elve mentén kezelniük szükséges. Az Európai Unió kiemelt figyelmet szentel a kockázatelemzési módszertanok, jó gyakorlatok megosztására, azok hasznosságának megértetésére, ugyanakkor nagy felelőssége van a tagállamoknak – és az érintett szervezeteknek közvetlenül – abban, hogy mindezek megfelelő formában alkalmazásra is kerüljenek. A kockázatmenedzsment tudatos és átgondolt kialakítása, majd működtetése elengedhetetlen egy elektronikus információs rendszer folytonos, zárt és teljes körű működése szempontjából, hisz ez által lesz képes garantálni a benne tárolt, feldolgozott, kezelt adatok sértetlenségét, bizalmasságát és rendelkezésre állását. Megállapítható tehát, hogy a NIS irányelv összességében rámutat arra, hogy a megfelelő kockázatmenedzsment kialakítása és működtetése jelentős mértékben járul hozzá az ellenálló képesség megacélozásához, amit tovább lehet és kell erősíteni oktatásokkal, illetve rendszeres továbbképzésekkel. Ennek egyik fő eszköze lehet – és kell legyen – a tudatosítás, ugyanis számos

tanulmány kimutatta már, hogy továbbra is az ember a leggyengébb láncszem, vagyis kiemelt figyelmet kell szentelni arra, hogy a humánerő ismerje és értse az őt közvetlenül érő kockázatok jelentőségét, majd pedig elsajátítsa azt a tudást, amivel ezeket a kockázatokat elfogadható mértékűre csökkenti. A megelőzés és ellenálló képesség fokozása mellett a direktíva az eseménykezelésre és helyreállításra is tartalmaz követelményeket. Ilyen markáns elem a súlyos biztonsági események bejelentésének kötelezettsége. Minden információs rendszerben számolni kell biztonsági események bekövetkezésével, amelyeket a rendszer sajátosságai, képességei, kapacitása, védelme alapján hozzávetőlegesen fel lehet mérni – ehhez segítséget ad az irányelv általános értelemben vett megfogalmazások útján. A kockázatok ismeretében nem csak a megelőzés, hanem a bekövetkező biztonsági események felderítési aránya, észlelése is fejlődik, ami jelentős mértékben képes hozzájárulni a kialakuló helyzetek hatékony, eredményes kezeléséhez, a megfelelően ismert, tesztelt rendszer, illetve a begyakorolt eljárásrendek érdemben csökkentik a biztonsági esemény hatásainak mértékét, és megalapozzák a következmények kezelését is.

Ahhoz, hogy a tagállamok megfelelően – és közösségi szinten egységesen – közelítsék meg a NIS irányelv által elérni kívánt célokat, mindenképpen tisztázni szükséges mire fókuszál a direktíva. Az eddigiekben bemutatott uniós törekvések kiindulási alapja az a kritikus információs infrastruktúra védelem, amely a 2008-as CIP irányelvből levezethetően nőtte ki magát szinte teljesen önálló szakpolitikává.

Ebből adóan fogalmazhatunk úgy, hogy a NIS irányelv szolgáltatásokra – a XXI. század informatikai technológiák által befolyásolt mozgatórugóira – helyezi a hangsúlyt, amelyhez minden tagállamnak a saját szempontjából kell megvizsgálnia, hogy mit tekint alapvetőnek, esszenciálisnak. Ezzel kapcsolatosan hangsúlyozni kell, hogy minden NIS irányelvhez kapcsolódó kötelezettség elsődlegesen a hatás vizsgálatából ered. Másképpen fogalmazva tudni kell, hogy mire gyakorol hatást, ha egy szolgáltatás nem érhető el. Ebből adódóan tehát a legfontosabb viszonyítási szempont az, hogy egy kiemelt szerepű szolgáltatás elérhetőségének korlátozottsága milyen és mekkora jelentőségű következményekkel jár. A NIS irányelv ebből a szempontból azért van, hogy valamennyire egységes módon, minden tagállam gondoskodjon az elektronikus információs rendszerek biztonsági szintjének növeléséről, fejlessze kockázatkezelési kultúráját, ezáltal összességében a nélkülözhetetlen szolgáltatásainak védelmét garantálja. Tételesen felsorolva tehát a célok elérése érdekében minden tagállamnak:

- ki kellett dolgoznia a nemzeti hálózat- és információbiztonsági stratégiáját;
- ki kellett jelölnie azt a nemzeti hatóságot, amely felügyeli az átültetést és a végrehajtást, egyben kapcsolattartó pontként is funkcionál;
- ki kellett jelölnie egy vagy több „gyors reagálású kibervédelmi csoportot" (CSIRT/CERT); valamint
- ágazatonként meg kellett határoznia, hogy mely kritériumok alapján esik egy-egy infrastruktúra az irányelv hatálya alá, és azonosítania kell a konkrét érintetteket is.

A NIS irányelv meghatározta az ún. alapvető szolgáltatásokat nyújtó szereplők és digitális szolgáltatók fogalmát, amelyek folyamatos rendelkezésre állását és megbízható működését a fenntartható biztonság alappilléreként definiálta. Kereteket szabott emellett a hálózati és információs rendszerek biztonságát szavatolni hivatott nemzeti szintű tevékenységeknek, a tagállamok közötti együttműködések formáinak, valamint a biztonság növelése érdekében szükséges további lépéseknek is. Az átültetés viszonylag nagy teret adott a tagállamoknak, ugyanakkor a meghatározott ágazatokban következetesen elvárja a végrehajtás érdekében szükséges intézkedések megtételét. Hatálybalépését tekintve három dátum irányadó: az irányelv 2016. augusztus 8-án lépett jogilag hatályba és 21 hónapot (2018. május) biztosított a tagállamoknak a szükséges nemzeti intézkedések megtételére (jogszabályok megalkotása, szervezeti struktúra megteremtése). További hat hónappal később – halasztott hatállyal, 2018 novemberéig – kellett eleget tenni azon rendelkezésének, amely alapján a már említett alapvető szolgáltatást nyújtó szereplők azonosítása megtörtént.

Mindezt érdemben kiegészíti még a *GDPR rendelettel*[98] járó kötelezettségek halmaza, amely elsősorban a magánszemélyek (felhasználók) védelmére irányul és a személyes adatok megóvása érdekében határoz meg az információbiztonsági követelményekkel összhangban álló rendelkezéseket. Fő célja, hogy növelje a digitális alapú szolgáltatások iránti bizalmat azzal, hogy az adatkezelést következetes, szigorú és ellenőrizhető keretek közé tereli. A rendelet 2016. május 24-én lépett hatályba, és kétéves türelmi időszak után 2018. május 25-től kell alkalmazni.

2017 szeptemberében a NIS irányelv végrehajtására történő felkészülési időszakkal párhuzamosan a Bizottság kiadta *2017/1584. ajánlását* (a továbbiakban: Ajánlás) a *nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról*[99]. Tette mindezt abból kifolyólag, hogy a NIS irányelv nem rendelkezik az EU-s együttműködés keretéről a nagyszabású kiberbiztonsági események és válsághelyzetek kezelését illetően. Az Ajánlás hangsúlyozza, hogy Európa-szerte megfigyelhető a vállalatok és az állampolgárok ágazatok közötti, illetve határokon átnyúló kölcsönös függősége, összekapcsolódása, ezért mind az EU intézményeinek, mind a tagállamoknak fel kell készülniük arra, hogy kiberbiztonsági esemény történik. Ez volt az első alkalom, hogy az EU – mint szövetségi rendszer – definíciós kereteket adott a kiberbiztonsági esemény kifejezésnek, amely alatt

[98] Európai Parlament és Tanács, 2016. – https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016R0679

[99] Európai Bizottság, 2017. - https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32017H1584&from=EN

olyan kiszámíthatatlan, gyakori és nagyon rövid időn belül kialakuló, földrajzi területre nem korlátozódó, gyorsan terjedni képes válsághelyzetet ért, amely súlyos zavarokat okozhat a belső piacon, tágabb körben az uniós gazdaság, a társadalom, összességében a demokrácia alapjául szolgáló hálózati és információs rendszerekben. Az így nevesített kiberbiztonsági események kezelését illetően az Ajánlás kijelenti, hogy gyors és hatékony együttműködést igényel, amely elsősorban a tagállamok felelőssége. Ugyanakkor megkülönbözteti az uniós szintű válsághelyzetet elérő kiberbiztonsági esemény kategóriáját, amely akkor állapítható meg, ha az érintett tagállam az esemény által okozott zavarokat azok kiterjedése miatt nem képes egyedül kezelni, vagy ha az adott esemény kettő, vagy több tagállamot érint és műszaki, vagy politikai jelentőséggel bíró hatást is széles körben képes kiváltani. Mindez már politikai koordinációt és reagálást tesz szükségessé EU politikai szinten. A tagállami felelősség elsődlegességén túl az Ajánlás meghatározza, hogy az uniós szintű kiberbiztonsági válsághelyzetek kezelésében részt vesznek a NIS irányelv által létrehozott struktúrák – így a CSIRT-ek hálózata, valamint az ügynökségek (pl.: ENISA, Europol, EC3, stb.) és egyéb szervezetek, amelyek együttműködését a CSIRT-hálózatnak kell biztosítania. A szintén a NIS irányelv által életre hívott együttműködési csoport[100] pedig feladatul kapta, hogy stratégiai iránymutatást nyújtson a CSIRT-ek hálózata által végzett tevékenységéhez. Az Ajánlás ráerősít továbbá a kockázatmenedzsment fontosságára és hasznosságára azzal, hogy kijelenti: *„a kockázati helyzetnek és a fenyegetéseknek a jelentéstétel, az értékelés, a kutatás, a kivizsgálás és az elemzés révén való megismerése és megértése kulcsfontosságú a jól megalapozott döntések meghozatalához”*[101]. Emellett ismételten hangsúlyt kapott a páneurópai kiberbiztonsági gyakorlatok szervezése, amelyeket az ENISA 2010 óta rendszeresen végrehajt. Az Ajánlás szerint a tagállamoknak és az EU intézményeinek létre kell hozniuk egy uniós kiberbiztonsági válságreagálási keretet, amelyben azonosítaniuk kell az érintett szereplőket (intézmények, hatóságok technikai, operatív, stratégiai és politikai szinten), illetve eljárási standardokat kell meghatározniuk arra vonatkozóan, hogy a szereplők milyen formában működnek együtt az EU-s válságkezelési mechanizmusok keretében. Ennek érdemi megvalósítása érdekében az Ajánlás melléklete tartalmazza a „Nagyszabású, határokon átnyúló kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálás” tervezetét, a kapcsolódó alapelvek, célkitűzések kifejtésével, a technikai, az operatív és a stratégiai/politikai szintű együttműködés lehetséges szereplőivel, a reagálás folyamatával. A melléklet leírja továbbá a kiberbiztonság integrálását az uniós politikai szintű integrált válság-elhárítási folyamatba.

A jogszabályi keretrendszer teljessé válását – egyelőre – két, 2019-ben napvilágot látott, kötelező jogi aktussal érte/éri el az Európai Unió. Az első az Európai Parlament és a Tanács áprilisban elfogadott, *az ENISA-ról*[102] *és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről*[103] szóló 2019/881 rendelete (a továbbiakban: kiberbiztonsági jogszabály). Tekintettel arra, hogy a legmagasabb szintű EU-s jogszabály formájában került kihirdetésre, a benne foglaltak teljes egészében kötelezőek és közvetlenül alkalmazandóak valamennyi uniós tagállamban. A kiberbiztonsági jogszabály preambuluma megállapítja, hogy az EU tagállamaiban az internethez bármilyen formában kapcsolódó eszközök a biztonság- és ellenálló képesség követelményeit nem teljesítik megfelelően, ami így unió szerte tapasztalható elégtelen kiberbiztonsághoz vezet. A magas szintű együttműködés megteremtése, illetve a kellően alapos tanúsítási kultúra kialakításával mindez fejleszthető, ezért döntött az EU intézményrendszere az ENISA szerepének megerősítéséről és kibővítéséről, valamint az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok egységes kiberbiztonsági tanúsításával kapcsolatos keretrendszer megalkotásáról. A tanúsítás eddigi, korlátozott alkalmazása révén a felhasználók nem rendelkeztek elegendő informá-

[100] NIS irányelv 1. cikk (2) b. pont és 11. cikk

[101] Ajánlás Preambulum (20)

[102] Új megnevezése szerint: Európai Uniós Kiberbiztonsági Ügynökség

[103] Európai Parlament és Tanács, 2019. – https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Cybersecurity Act)

ciókkal a termékek kiberbiztonsági jellemzőiről, ami aláássa a digitális megoldásokba vetett bizalmat. Ezzel szorosan összefügg, hogy az egyre nagyobb méreteket öltő digitalizáció és összekapcsoltság fokozatosan növeli a kiberbiztonsági kockázatokat, amelyek összességében sebezhetővé teszik a társadalmat. Így tehát minden szükséges intézkedést meg kell tenni annak érdekében, hogy a hálózati és információs rendszerek, a távközlési hálózatok, és ezek révén az állampolgárok, a szervezetek, a vállalkozások – különösen a kritikus infrastruktúrák – hatékonyabb védelemben részesüljenek. Ilyen intézkedésnek tekintik a tagállamok képességeinek és felkészültségének fokozását, az együttműködés hatékonyságának növelését, az információ-megosztás és a koordinációt tagállamok, illetve tagállamok és uniós intézmények között egyaránt. A kiberbiztonsági jogszabály hangsúlyozza, hogy az ITK-ba vetett bizalom növelését könnyebben el lehet érni az egész EU-ra kiterjedő olyan tanúsítás bevezetésével és alkalmazásával, amely a nemzeti piacokon és valamennyi ágazatban közös kiberbiztonsági követelményeket és értékelési kritériumokat biztosít.

Mindezek érdekében, arra alapozva, hogy az ENISA szerepe az új uniós kiberbiztonsági politika keretében egyre meghatározóbbá vált, felülvizsgálták a szervezet megbízatását és új feladatrendszeréhez kifejezőbb megnevezést is meghatároztak. Az Európai Uniós Kiberbiztonsági Ügynökség (rövidítése továbbra is ENISA) a szakértelem rendelkezésre bocsátása által és tanácsadás formájában, illetve információs és tudásközpontként működve az EU elsőszámú kiberbiztonsággal foglalkozó intézményévé nőtte ki magát. A kiberbiztonsági jogszabály II. címe (mint jogszabályi rész) célirányosan az újdonsült ENISA tekintetében tartalmaz rendelkezéseket. Meghatározza a megbízatását, a célkitűzéseit, a feladatait – szakpolitikai tekintetben, kapacitásépítés vonatkozásában, uniós szintű operatív együttműködés kapcsán, tudatosítás szempontjából, továbbá a tanúsítás, szabványosítás uniós szakpolitikájának kidolgozását és végrehajtását illetően –, valamint önálló fejezetet szentel az ENISA felépítésének, költségvetésének és személyzetének egyaránt.

Ezzel párhuzamosan a kiberbiztonsági jogszabály kijelenti, hogy szükséges egy közös megközelítés kialakítása és elfogadása, amely olyan európai kiberbiztonsági tanúsítási keretrendszert hív életre, amely nevesíti a fő horizontális követelményeket a kidolgozandó európai kiberbiztonsági tanúsítási rendszerekhez, illetve lehetővé teszi az IKT-k európai kiberbiztonsági tanúsítványainak, valamint EU-s megfelelőségi nyilatkozatainak minden egyes tagállamban történő elismerését és alkalmazását. Mindennek felügyeletére minden tagországban illetékes nemzeti kiberbiztonsági tanúsító hatóságokat kell felhatalmazni arra, hogy nyomon kövessék és betartassák a gyártók megfelelőségi nyilatkozathoz kapcsolódó kötelezettségeit, támogatniuk kell a nemzeti akkreditáló szerveket, figyelemmel kell kísérniük a tanúsítások terén bekövetkező fejleményeket. Emellett feladatuk, hogy engedélyezzék a megfelelőségértékelő szervek feladatellátását, és kezelniük kell a kapcsolódó panaszokat. Mindezek részletszabályait a III. cím (kiberbiztonsági tanúsítási keretrendszer, mint különálló jogszabályi rész) foglalja össze. Első feladatként a Bizottságnak közzé kell tennie gördülő munkaprogramját, hogy meghatározza a jövőbeli európai kiberbiztonsági tanúsítási rendszerek stratégiai prioritásait. A keretrendszerrel kapcsolatos további rendelkezések között kiemelt szerepe van az egyes tanúsítási rendszerek biztonsági célkitűzéseiről (pl.: jogosulatlan hozzáférés biztosítása, sebezhetőségek azonosítása, ellenőrzés lehetővé tétel, mielőbbi helyreállítási lehetőségek kialakítása stb.), a megbízhatóság szintjeiről (alap, jelentős, magas), az európai és nemzeti kiberbiztonsági tanúsítási rendszerekről szóló cikkeknek, valamint a megfelelőségértékelő szervezetek által teljesítendő követelményeket tartalmazó mellékletnek. Tagállami szempontból az egyik legmeghatározóbb rész az 58. cikk, amely a nemzeti kiberbiztonsági tanúsító hatóságokra vonatkozó részletes rendelkezéseket tartalmazza. Közösségi viszonylatban ezen hatóságok egyik fő feladata az európai kiberbiztonsági tanúsítási csoportban történő részvétel, amely szintén azzal a céllal jön létre, hogy a lehető legszakmaibb tanúsítási rendszerek kialakítását támogassa mind uniós, mind tagállami szinten. Az utolsó rendelkezések pedig a panasztétel, a jogorvoslati lehetőségek és a szankciók terén adnak útmutatást. A kiberbiztonsági jogszabály mindezen túlmenően – hiánypótlóan – számos szakmai terminológiát határozott meg a 2. cikkben, amelyek szintén az egységes uniós megközelítés kialakítását támogatják (lásd: Fogalomtár).

A kiberbiztonsági jogszabály 2019. június 6-án jelent meg az Európai Unió Hivatalos Lapjában, kihirdetését követő 20. napon lépett hatályba, így azt – a külön halasztott hatályú rendelkezések kivételével – már alkalmazni kell. A nemzeti kiberbiztonsági tanúsító hatóságokra, a megfelelőségértékelő szervezetekre, valamint a bejelentés, a panasztétel, a jogorvoslat és a szankcionálás szabályaira vonatkozó cikkek azonban kétéves halasztással lépnek majd hatályba, vagyis 2021. június 28-tól kell őket alkalmazni.

Ez az a pont, ahol ki kell hangsúlyozni, hogy az EU kezdeti törekvései (2009-2015) az információbiztonságot kifejezetten a kibertámadások szemszögéből közelítették meg. A legtöbb dokumentum preambuluma azokkal az eseményekkel támasztotta alá az intézkedések szigorításának, vagy következetesebbé tételének szükségességét, amelyek kibertámadásokként kerültek a köztudatba. 2016 után – már a NIS irányelvben – azonban változott ez a szinte kizárólagosnak tűnő trend, és egyre nagyobb figyelmet kapnak a technológiai, illetve humán erőforrás eredetű kockázatok, így azok kezelésének igénye is. A kiberbiztonsági jogszabály által megteremtett, a kiberbiztonsági tanúsítási keretrendszer is kifejezetten ezt a célt szolgálja.

A másik 2019-ben megjelent irányadó jogi aktus 2019 májusában jelent meg, az Európai Unió Tanácsa által kiadott az *Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről*[104] szóló rendeletet (a továbbiakban: Rendelet) formájában. A szabályozást azokra a jelentős hatású kibertámadásokra (beleértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat) kell alkalmazni, amelyek az EU-ra, vagy annak tagállamaira nézve külső fenyegetést (pl.: EU-n kívülről eredő, EU-n kívül letelepedett vagy tevékenységét az EU-n kívül végző szervezet követi el) jelentenek. A tagállamoknak fontos feladata, hogy megállapítsák e Rendeletben foglaltak megszegése esetén alkalmazandó szankciók szabályait, és biztosítaniuk kell azok végrehajtását. Ezeknek a szankcióknak elsősorban hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. Fontos mérföldkő, hogy a Rendelet megnevezi, mit ért az EU kibertámadás alatt. Konkrétan az alábbi tevékenységeket, amennyiben a sértett adatok és információk tulajdonosa a tevékenységet nem engedélyezte, vagy azt eleve az EU, vagy az érintett tagállam jogszabályai nem teszik lehetővé – így tehát

- az információs rendszerhez való hozzáférést;
- az információs rendszereket érintő beavatkozást;
- az adatokat érintő beavatkozást; vagy
- az adatkifürkészést.

Kiemeli ugyanakkor konkretizálva, hogy a tagállamok szempontjából mindenképpen veszélyt jelentő kibertámadásoknak kell tekinteni azokat, amelyek

- kritikus infrastruktúrához kapcsolódó információs rendszereket, vagy
- alapvető szolgáltatást nyújtó szereplőket érintenek, továbbá
- olyan támadásokat is, amelyek kritikus állami funkciókat (különösen a védelem, intézmények irányítása és működése, nyilvános választások, diplomáciai képviseletek, stb.) érintenek, vagy
- minősített adatok tárolását és kezelését végző szervezetek ellen irányulnak, illetve
- a kormányzati veszélyhelyzet-elhárító csoportokat célozzák.

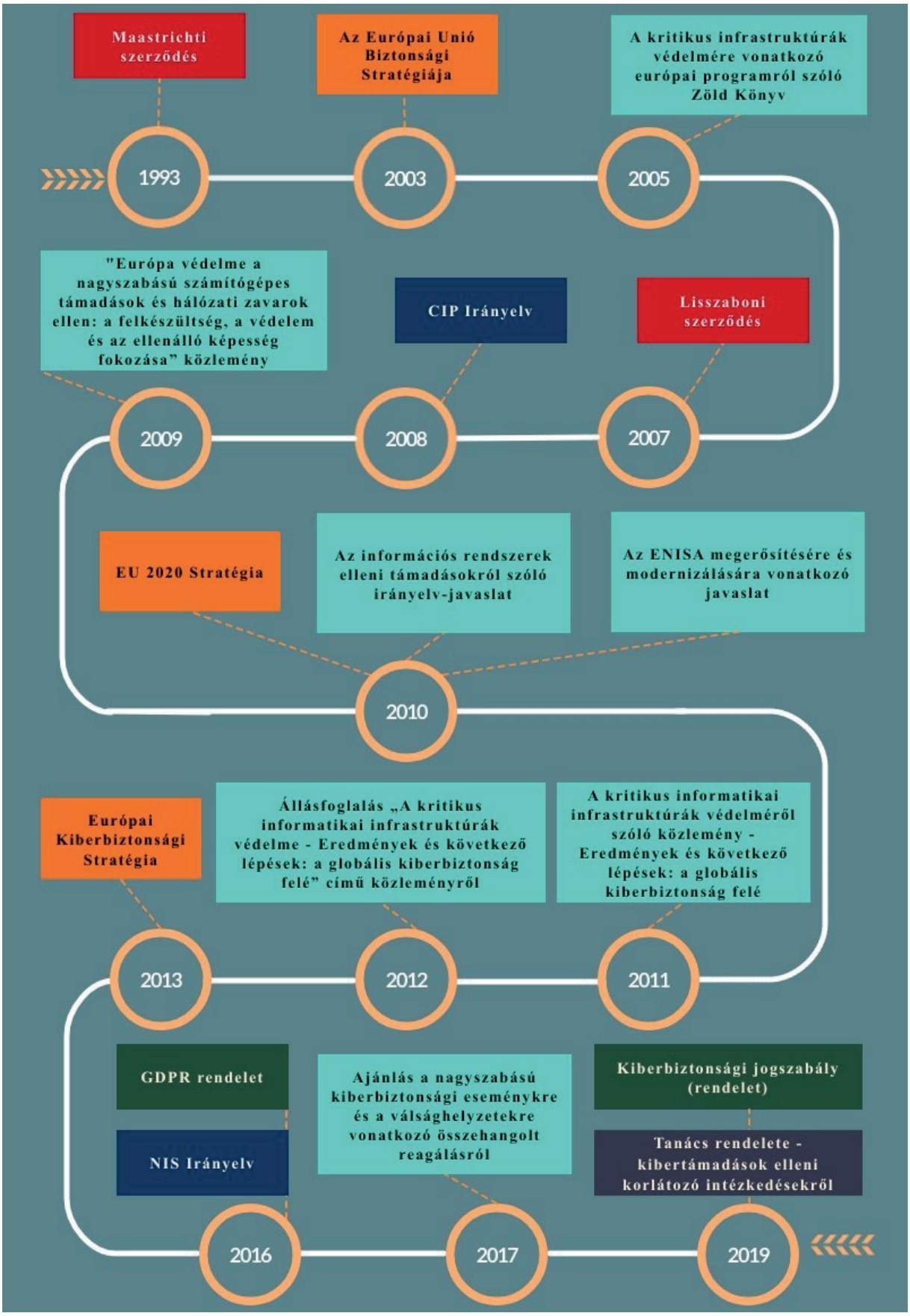
Ugyanígy konkretizálja, hogy az EU – mint közösség – számára veszélyt jelentő kibertámadások közé kell sorolni azokat, amelyeket az EU intézményei, a harmadik országokban található küldöttségei, illetve a nemzetközi szervezeteknél működő képviseletei, a közös biztonság- és védelempolitika műveletei és -missziói, valamint a különleges képviselői ellen intéznek. Ezek alapján meghatározásra került az is, hogy egy kibertámadás jelentős hatását milyen tényezők alapján lehet megállapítani. llyen szempont például az előidézett zavar hatóköre, léptéke, hatása és súlyossága; az érintett tagállamok

[104] Európai Unió Tanácsa, 2019. - https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0796&from=EN

száma; vagy az elkövető által saját maga vagy mások számára szerzett gazdasági előny. Mindezzel a Tanács létrehozott egy olyan keretet, amely lehetővé teszi, hogy az EU célzott korlátozó intézkedések vezessen be az olyan kibertámadásoktól való elrettentés, illetve az azokra történő érdemi reagálás érdekében, amelyek valós külső fenyegetéseket jelentenek. A Rendelet szerint ebbe beleértendőek a harmadik államok vagy nemzetközi szervezetek ellen irányuló kibertámadások is, amennyiben az EU közös kül- és biztonságpolitikai céljainak elérése érdekében ilyen korlátozó intézkedések foganatosítása indokolt. Amennyiben szükséges a szankció, a korlátozó intézkedés személyek esetében az EU-ba való beutazás tilalmát jelentheti, míg személyek és szervezetek esetében vagyonieszköz-befagyasztást is magukba foglalhatnak. Mindezen intézkedések jog- és szakszerű alkalmazása érdekében a tagállamok illetékes hatóságokat jelölnek ki.

A Rendelet 2019. május 17-és jelent meg az Európai Unió Hivatalos Lapjában, kihirdetését követő napon lépett hatályba, így azt már teljes egészében kötelezően és minden tagállamban közvetlenül alkalmazni kell.

A kiberbiztonsági szabályozási környezet kialakulásának idővonalát az alábbi ábra szemlélteti:




*2. ábra: Szabályozás kialakulásának idővonala*

## 3.3. Definíciós környezet

A korábbi alfejezetek alapján látható, hogy a vizsgált témakört illetően számos definíció fellelhető, ugyanakkor a hazai jogszabályi környezet alkalmazása szempontjából elsősorban a magyarországi fogalomrendszer az irányadó. Mindezeket a bemutatott jogi háttér nevesíti, így az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és végrehajtási rendeletei, illetve a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény és végrehajtási rendelete. A részletek kifejtése előtt fontos tisztázni az infrastruktúra, a kritikus infrastruktúra, a kritikus információs infrastruktúra, illetve a kritikus infrastruktúra információs rendszerei közötti különbségeket és párhuzamokat, továbbá áttekinteni a NIS irányelv által bevezetett új definíciókat.

Amennyiben általánosságban értelmezzük az *infrastruktúra* kifejezést, úgy a Cecei Katalin és Mórocz Attila szerzőpáros szerint a társadalmat körülvevő környezetet nevezzük infrastruktúrának, amely nem más, mint *„ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek”*[105]. Ebben a megfogalmazásban szerepelnek azok a célirányos jelzők, amelyek lehetővé teszik az infrastruktúra, mint komplex kifejezés megértését, és levezethetőek a legfontosabb tulajdonságok is, amelyek jellemezhetik, így például a hálózat jellegű kialakítás, a nagy kiterjedés, a szolgáltatási teljesítmény, a tömeges igénybevétel, illetve a veszélyeztető tényezők köre. Kiindulva ezen sajátosságokból a kritikus infrastruktúrát a következők szerint definiálhatjuk: *„azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére”*[106]. Magyarországon a hatályos szabályozás a kritikus infrastruktúra kifejezés helyett a létfontosságú rendszerek és létesítmények szóösszetételt használja.

Figyelemmel arra, hogy a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény végrehajtási rendelete[107] időben három hónappal megelőzte az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény hatálybalépését[108], a *létfontosságú információs rendszer és létesítmény*[29], mint definíció, már létezett a hazai információbiztonsági szabályozás megalkotásakor. Ebből adódóan napjainkban is kettősség jellemzi a fogalmakat, amelyre megoldást jelentett volna, ha a jogalkotási folyamatok során irányadónak tekintik és alkalmazzák a végrehajtási rendeletben szereplő tartalmat, vagy hatályon kívül helyezik azt és újat vezetnek be. Másik megoldás lehetett volna, hogy érdemben elkülönítik a kifejezések jelentéstartalmát attól függően, hogy melyik jogszabályi környezet az irányadó.

Az említett végrehajtási rendelet szerint létfontosságú információs rendszernek és létesítménynek tekintjük *„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”*[109]. Ez a definíció tulajdonképpen kijelenti, hogy valamennyi fizikai és virtuális létezésű rendszer/eszköz, amely kritikus infrastruktúraként azért

[105] Cecei Katalin, Mórocz Attila: Klímaváltozás és a kritikus infrastruktúra. IN: AGRO-21 Füzetek, 2004. 36. szám, pp. 32-63.

[106] Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklet (http://www.kozlonyok.hu/kozlonyok/Kozlonyok/10/PDF/2008/31.pdf)

[107] 65/2013. (III. 8.) Korm. rendelet, hatályba lépett: 2013. március 11.

[108] 2013. évi L törvény, hatályba lépett: 2013. július 1.

[109] 65/2013. (III. 8.) Korm. rendelet 1. § 3.

kerül kijelölésre, 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 alapfeltételéül szolgál. A bonyolult megfogalmazás mögött a rész-egész elv húzódik, amely kimondja, hogy egy infrastruktúra önmagában és egy nagyobb rendszer részeként is kritikusnak tekinthető, attól függően, hogy milyen feltételrendszer szerinti vizsgálatnak vetjük alá. Példaként a legkifejezőbb talán a repülőtereket és azok irányítási rendszerét venni, amelyben egyértelműen látszik, hogy a szolgáltatást biztosító nemzetközi repülőtér önmagában létfontosságú rendszerelem lehet – utasforgalmát, kereskedelmi jelentőségét, kockázatait tekintve –, ugyanakkor minden bizonnyal kijelölt rendszerelem lesz a légiforgalmi irányítás rendszere – irányítótorony, informatikai rendszer – is.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény alig néhány hónappal később hatályba lépett fogalom-meghatározását nézve, egy az előzőhöz képest szűkített definíciót találunk. Eszerint ugyanis *létfontosságú információs rendszerelemnek* csak a kijelölt kritikus infrastruktúrák 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”*[110]. Ez azt jelenti, hogy azok az elektronikus információs elemek kerülhetnek ebbe a halmazba, amelyek egy kijelölt kritikus infrastruktúra részét képezik és bármilyen okból kifolyólag annak rendelkezésre állására hatást gyakorolhatnak. Ez tulajdonképpen megegyezik az előbb ismertetett, végrehajtási rendeletben található definíció második felével és ténylegesen is értelmezhető a létfontosságú rendszereket tekintve.

Érdekesség azonban, hogy ez utóbbi kifejezés nem fordul elő túl sokszor a jogszabályi környezetben, mindössze két helyen említi a törvény, konkrétan az átmeneti rendelkezésekben, ahol a kötelezettségek teljesítésére vonatkozó határidőket szabta meg a jogalkotó. Itt azonban valójában pontatlanul alkalmazza a definíciót, tekintettel arra, hogy a rendelkezések a törvény személyi hatálya alá tartozó valamennyi létfontosságú rendszerelem kijelöléséről szóló határozatokra utalnak[111], amelyek nem csak létfontosságú információs rendszerelemekre vonatkozhatnak. Emellett a törvény további egy helyen alkalmazza még a *létfontosságú információs rendszer*[112] kifejezést is, amely a Nemzeti Közszolgálati Egyetem képzési tevékenységével összefüggő gyakorlatok típusaként szerepel a jogszabályban, de a fenti definíciók alapján nem értelmezhető pontosan.

A NIS irányelv mindehhez bevezet további kettő, egymástól funkciók tekintetében markánsan elkülönülő, fontosságát tekintve azonban hasonló prioritást élvező szolgáltatói csoportot jelölő fogalmat, a következők szerint:

*a) alapvető szolgáltatást nyújtó szereplők*: az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és elosztás, valamint a digitális infrastruktúra ágazatokban működő létesítmények, amelyek
- kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújtanak;
- a szolgáltatásuk nyújtása hálózati és információs rendszerektől függ; és
- a szolgáltatásukat érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában[113].

[110] állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény 1. § 33.
[111] állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény 26. § (6) és (7)
[112] állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény 23. § d)
[113] [10] 4. cikk 4. pont, 5. cikk 2. pont és II. melléklet alapján

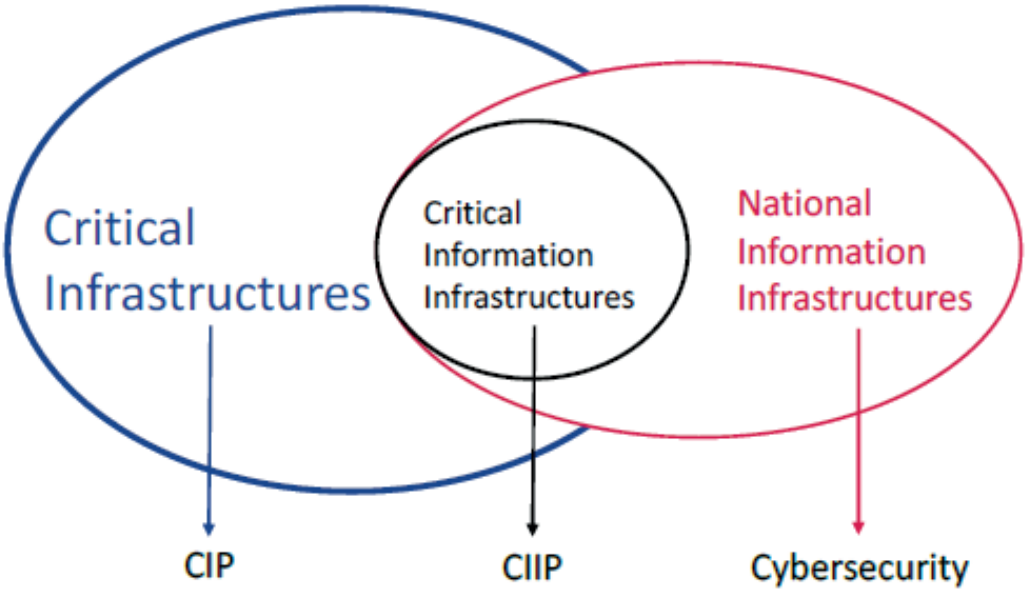
*b) digitális szolgáltatók*: minden digitális szolgáltatást nyújtó szereplő, amely szolgáltatása nem nélkülözhetetlen, de társadalmi szempontból kiemelt jelentőséggel bír. Digitális szolgáltatásnak tekintendő tehát
- az online piactér,
- az online keresőprogram és
- a felhőalapú számítástechnikai szolgáltatás[114].

Az alapvető szolgáltatásokat nyújtó szereplők kapcsán fontos kijelenteni, hogy a hazai jogi környezetben jelenleg kizárólag a kritikus infrastruktúrákra vonatkoznak, de azok közül csak egyes ágazatokat érintenek, tehát a hatályos létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény szerinti 10 ágazaton belüli kisebb halmazt képeznek, amit a következő ábra szemléltet:


*3. ábra: Fogalom-halmazok*

Nemzetközi vetületre kitekintve a fenti fogalmak értelmezése ugyanígy szerteágazó képet mutat. Hazánkhoz hasonlóan a legtöbb országban – a CIP irányelvben foglaltaknak megfelelően – megkülönböztetik a „critical infrastructure" kifejezést a „critical information infrastructure" szóösszetételtől. Egy 2016-os ENISA kiadványban[115] a közös metszeteket az alábbi ábrával szemléltették:

[114] [10] 4. cikk 6. pont és III. melléklet alapján
[115] Stocktaking, Analysis and Recommendations on the protection of CIIs




*4. ábra: Fogalom-halmazok (ENISA)*[116]

Mindez azt jelenti, hogy a kritikus infrastruktúráink a szolgáltatás jellegétől függően sorolhatóak különböző ágazatokba, de szinte valamennyiük közös metszete a kibertérrel való kapcsolódás és az általa hordozott kockázatok, amelyek az elektronikus információs rendszereiken keresztül fejtik ki hatásukat. Az EU szemszögéből ez indokolhatta egy újabb „alcsoport" megkülönböztetését, vagyis az alapvető szolgáltatást biztosító szereplők körének meghatározását. Meg kell állapítani, hogy nem egyértelmű az elhatárolhatóság az alapvető szolgáltatások és a kritikus infrastruktúrák között.

## 3.4. Tagállami szabályozási környezet és szervezet-rendszer Magyarországon

Hazánkban az információbiztonságra irányulóan – részint az EU-s törekvéseknek, részint a proaktivitásnak köszönhetően – 2013 júliusa óta létezik nemzeti jogszabályi keretrendszer, amelyet Magyarország Nemzeti Kiberbiztonsági Stratégiája, valamint *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény* (a továbbiakban: Ibtv) és végrehajtási rendeletei alkottak. Ahogy az előző alfejezetben már több utalás történt rá, ennek már a kezdetektől, vagyis az első hatályba lépéstől, része a kritikus infrastruktúrák információs rendszerei biztonságának szavatolása, tekintettel arra, hogy CIP Irányelv implementációjának eredményeként a *létfontosságú rendszerek védelmét szabályozó törvény*[117] (a továbbiakban: Lrtv.) is hatályba lépett 2013 márciusában. Mindezek „folytatásaként" – újabb kodifikációs tevékenység keretében – az új kötelezettségeket tartalmazó NIS irányelv és a GDPR nemzeti jogszabályi környezetbe történő integrálása megtörtént 2017-2018-ban. A fenti folyamat keretében lezajlott jogszabály-módosítások a hazai jogi környezetben is jelentős változásokat idéztek elő 2018. május 10-től.

[116] Myriam Dunn Cavelty, The Art of CIIP Strategy 2012. p. 20. Critical infrastructures: kritikus infrastruktúrák; Critical information infrastructures: kritikus információs infrastruktúrák; National information infrastructures: nemzeti információs infrastruktrúrák; Cybersecurity: kiberbiztonság.

[117] *Létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény*

Hazánkban jelenleg kettő, a témakörhöz kapcsolható stratégiai dokumentum van hatályban, a már említett kiberbiztonsági stratégia[118], illetve a 1838/2018. (XII. 28.) kormányhatározat Magyarország *hálózati és információs rendszerek biztonságára vonatkozó Stratégiá*járól[119]. Előbbi a 2013-ban meghatározott célok eléréséhez rendelt hozzá feladatokat, de felelősök meghatározása nélkül. Utóbbi egy ún. irányítási keretrendszert hozott létre, amelyben a tevékenységek összehangolásáért a Nemzeti Kiberbiztonsági Koordinációs Tanácsot tette felelőssé. A feladatokat a digitális környezet iránti bizalom erősítése, a digitális infrastruktúra védelme, illetve a gazdasági szereplők támogatása köré csoportosította, mindhárom feladatkörhöz tovább pontosított intézkedéseket társított. Jelenleg folyamatban van az intézkedési terv részletes kidolgozása a feladatok/intézkedések konkrét felelősökhöz delegálása.

Az Ibtv. jelenleg is hatályos verziója a személyi hatályát tekintve kiterjed a létfontosságú rendszerek és létesítmények elektronikus információs rendszereire, azok megfelelő szintű védelmének biztosítását is célul tűzte ki. Az Ibtv. alapján az elektronikus információs rendszereket – a kockázatarányos védelem megvalósítása érdekében – biztonsági osztályba, míg magát a szervezetet,– a védelmi felkészültségük alapján – biztonsági szintbe kell sorolni. Az Ibtv. rendelkezik a hatálya alá tartozó szervezetek feladatairól és kötelezettségeiről, az elektronikus információs rendszerek biztonsági osztályba sorolásáról, illetve a szervezet biztonsági szintbe sorolásáról, informatikai biztonsági incidensek bejelentéséről, illetve az elektronikus információs rendszer biztonságáért felelős személy feladatairól. Emellett – részben a jogharmonizációs kötelezettségeknek köszönhetően, részben a részletszabályok kifejtése érdekében – a következő jelenleg hatályos releváns jogszabályok irányadóak:

- 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;
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről;
- 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;
- 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.

### *3.4.1. Szervezeti feladatok és kötelezettségek*

Annak érdekében, hogy az Ibtv. hatálya alá tartozó szervezetek elektronikus információs rendszerei, így az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, valamennyi elektronikus információs rendszert be kell sorolni egy-egy *biztonsági osztályba* a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, kockázatelemzés alapján. Ennek a kockázatelemzésnek ki kell terjednie az elektronikus információs rendszer(ek) vagyonelemeinek felmérésére,

[118] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

[119] https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

így meghatározható a védelem tárgya (adatok, eszközök, kapcsolatok). A különböző vagyonelemek vonatkozásában meg kell határozni a fenyegetéseket IT, infrastrukturális, környezeti, humán, társadalmi, politikai, gazdasági stb. szempontból, majd vizsgálni a sebezhetőséget. Ezt követően meg kell tudni állapítani, hogy melyek azok az elfogadható kockázatok, amelyek a rendszer (szolgáltatás) működését jelentős mértékben nem képesek befolyásolni, illetve melyek azok, amelyek nem elfogadhatók a szervezet számára, vagyis intézkedéseket kell foganatosítani az adott kockázat csökkentésére. Ezen kockázatok mérséklésére alternatívákat kell felállítani, illetve fel kell tárni a maradványkockázatokat is, amelyek további értékelésre szorulnak.

Az osztályba sorolás a felsorolt szempontok alapján, egy ötfokozatú skálán történik, az adott elektronikus információs rendszerben kezelt adatoktól és a rendszer funkcióitól függően. A kritikus infrastruktúrák esetében, különösen a rendeltetésükből adódóan, a szabályozás a rendelkezésre állást követeli meg elsődlegesen az ismertetett hármas szempontrendszert nézve, ugyanakkor nem zárható ki, hogy bizonyos – például a pénzügy ágazatba tartozó – rendszereknél még hangsúlyosabb lesz a sértetlenség és a bizalmasság követelménye. Az egyes biztonsági osztályokhoz meghatározott követelményrendszer társul, amelyet az adminisztratív, a fizikai és a logikai védelmi intézkedések megtételével kell teljesíteni az irányadó osztály szerint. Az adminisztratív védelmi intézkedések körébe tartozik például a különböző szabályzatok készítése és a nyilvántartások vezetése, a kockázatelemzés, az egyes eljárásrendek kialakítása, az üzletmenet-folytonosság tervezése, illetve az oktatás, képzés is. A fizikai védelmi intézkedések a rendszerhez és a hozzá tartozó eszközökhöz történő hozzáférés szabályozását foglalják magukba, de itt említhető az áramellátás biztosítása, de a tűz, víz-, egyéb károk elleni védelem, vagy a karbantartási tevékenység egyaránt. A logikai védelmi intézkedések közé pedig többek között a biztonsági tesztelés, a logelemzési tevékenység, a konfigurációkezelés, a rendszeres naplózás, vagy a különféle adathordozók védelme tartozik. A jogszabályi előírások alapján meghatározható az egyes rendszerek irányadó biztonsági osztálya, amelynek meg kell felelni, és amelyhez társított követelményeket teljesíteni szükséges. A biztonsági osztályba sorolást a szerv vezetője hagyja jóvá, de ciklikusan – jelenlegi előírások szerint háromévenként, vagy szükség esetén soron kívül – dokumentált módon felül kell vizsgálni.

Az Ibtv. rendelkezéseinek megfelelően emellett a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintbe kell sorolni. A biztonsági szint az adott szervezet biztonsági menedzsmentjének fejlettségét, érettségét mutatja. Szintén ötfokozatú rendszerben határozható meg az adott szint, ebből a leggyengébb szint (1-es) azt jelenti, hogy a szervezetnél lévő információbiztonságot érintő szabályozók és folyamatok ad hoc jellegűek, ellenőrzésük nem biztosított. A szintek növekedésével párhuzamosan ezek a folyamatok szabályozottabbak, ellenőrzöttek, számon kérhetők, oktatottak, teszteltek, mérhetők, auditáltak lesznek. A rendszerek biztonsági osztálya és a szervezet biztonsági szintje között markáns összefüggés van, tekintettel arra, hogy szigorú és érdemi védelmi intézkedéseket csak fejlett biztonsági kultúrával rendelkező szervezet tud végrehajtani.

A biztonsági osztályokhoz és szintekhez tartozó követelményeket nem kell azonnal teljesíteni, az Ibtv. lehetőséget ad a fokozatos elérésre[120]. Ennek megfelelően először meg kell állapítani a vizsgálat idején tapasztalható aktuális biztonsági osztályt / szintet, a jogszabályi környezet alapján meg kell határozni az irányadó biztonsági osztályt / szintet, amelyet el kell érnie. Az eggyel magasabb osztályba / szintre lépéshez mindig 2 év áll rendelkezésre (fokozatos elérés elve), egészen addig, amíg el nem éri az irányadó fokozatot. Amennyiben az adott szervezet nem éri el az 1-es biztonsági szintet, abban az esetben az első vizsgálatot követően 8 év áll rendelkezésre, hogy az 1-es szinthez tartozó előírásoknak megfeleljen. Teljesen új elektronikus információs rendszer bevezetésével, illetve a meglévő és működő elektronikus információs rendszer továbbfejlesztésével kapcsolatban megállapított biztonsági osztályhoz tartozó követelményeket azonban a használatbavételig teljesíteni kell.

[120] Ibtv. 8. § (3) és 10. § (4) alapján

További kötelezettség a szervezetekre nézve, hogy elektronikus információs rendszer biztonságáért felelős személyt nevezzenek ki, illetve az adott rendszer védelmével kapcsolatos feladatokat, hatásköröket és ezek felelőseit az informatikai biztonsági szabályzatban szabályozzák. Meghatározó szerepe van tehát az információbiztonság szavatolásáért felelős, az egyes szervezetek részéről kijelölt személyeknek. Az Ibtv. 11. §-a egyértelműen kijelenti, hogy a elektronikus információs rendszerek védelmének biztosítása keretében a szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg[121]. Ebben a beosztásban a kijelölt személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, így konkrétan:

- gondoskodnia kell az elektronikus információs rendszerek biztonságával összefüggő tevékenységek jogszabályszerűségéről, a követelmények teljesüléséről, amelynek részeként elvégzi a kapcsolódó feladatok tervezését, szervezését, koordinálását és ellenőrzését is;
- össze kell állítania a szervezet informatikai biztonsági szabályzatát;
- elő kell készítenie a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását;
- véleményeznie kell az elektronikus információs rendszerek biztonságát érintő valamennyi a szervezetnél lévő/készülő szabályzatot és szerződést;
- kapcsolatot kell tartania a hatósággal és az eseménykezelő központtal;
- biztonsági esemény bekövetkezése esetén a jogszabályban meghatározottak szerint tájékoztatnia kell az eseménykezelő központot;
- részt kell vennie a számára miniszteri rendeletben előírt rendszeres szakmai képzésen, továbbképzésen.

### *3.4.2. Illetékes hatóságok*

Az elektronikus információs rendszerek biztonságának hatósági felügyelete több szervezet felelősségi körébe tartozik. A hatósági tevékenység két fő letéteményese a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) és a BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF), de egyes speciális rendszerek tekintetében egyedi felelősségeket határoz meg a jogszabályi környezet.

Az Ibtv., illetve *az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet* alapján az NBSZ valamennyi állami és önkormányzati szerv vonatkozásában eljárhat, kivéve:

- a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei;
- a honvédelmi célú elektronikus információs rendszerek; illetve
- olyan kritikus infrastruktúrák esetében, amelyek üzemeltetője nem állami/önkormányzati szerv.

[121] Ha a szervezet mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység is létrehozható.

Az európai vagy nemzeti létfontosságú létesítmények, rendszerek elektronikus információs rendszereivel kapcsolatos információbiztonsági hatósági feladatokat a BM OKF végzi, tehát az Lrtv. alapján kijelölt létesítmények, rendszerek elektronikus információs rendszerei esetében ellátja a hatósági feladatokat és a biztonsági felügyeletet a következő táblázatban ismertetett kivételekkel:

| **kivétel** | **eljáró hatóság** |
|---|---|
| a rendészetért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer | rendszert működtető szerv vezetője |
| a honvédelmi célú elektronikus információs rendszerek és a honvédelemért felelős miniszter alá tartozó szervek, gazdasági társaságok zárt célú elektronikus információs rendszerei | Katonai Nemzetbiztonsági Szolgálat főigazgatója |
| a külpolitikáért felelős miniszter alá tartozó szerveknél működő zárt célú elektronikus információs rendszer | külpolitikáért felelős miniszter |
| polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei | rendszert működtető szerv vezetője |

Jelen fejezet témakörét figyelembe véve a BM OKF, mint információbiztonsági hatóság tevékenységi körei a következők:

Biztonsági osztályba és szintbe sorolással, biztonsági események vizsgálatával kapcsolatos tevékenység során:

- végzi az osztályba sorolás és a biztonsági szint megállapításának ellenőrzését és az ellenőrzés eredménye alapján döntés meghozatalát,
- az osztályba sorolásra és – ehhez kapcsolódóan – a rendszert működtető szervek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzését,
- az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelését és eredményességének ellenőrzését,
- a rendelkezésre álló információk alapján kockázatelemzés elvégzését,
- a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálására irányuló hatósági eljárás megindítását (eljárás határideje 30 nap, logikai védelmi intézkedés teljesülésének vizsgálatára indított eljárás határideje 120 nap).

Nyilvántartás vezetésével kapcsolatos tevékenysége keretében kezeli:

- a szervezet azonosításához szükséges adatokat (megküldés 60 napon belül),
- a szervezet elektronikus információs rendszereinek megnevezését, besorolásait, technikai adatait,
- a szervezet elektronikus információs rendszereinek biztonsági felelősére vonatkozó adatokat (megküldés 60 napon belül),
- a szervezet informatikai biztonsági szabályzatát (megküldés 90 napon belül),
- a biztonsági eseményekkel kapcsolatos, a kormányzati eseménykezelő központtól kapott értesítéseket.
- A nyilvántartásból adattovábbítás kizárólag az eseménykezelő központok részére történhet.
- Az adatokat a tevékenység befejezésének bejelentését követő 5 év elteltével kell törölni.

Ellenőrzésekkel kapcsolatos tevékenység:

- a jogszabályokban foglalt biztonsági követelmények és az ezekhez kapcsolódó eljárási szabályok teljesülésének ellenőrzése,
- a követelményeknek való megfelelőség alátámasztásához szükséges dokumentumok bekérése,
- a központi költségvetési és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában az információbiztonsági követelmények megtartásának ellenőrzése, azokra ajánlások tétele,

- a fejlesztési projektek tervezési szakaszában szakmai részvétel biztosítása és a biztonsági követelmények beépülésének ellenőrzésére irányuló tevékenység folytatása,
- a sérülékenység megszüntetésére vonatkozó intézkedési terv készítése.

Mindezeken túl kiemelt feladata, hogy az információs társadalom tagjainak biztonságtudatosságát elősegítse és támogassa, részt vegyen a hazai és nemzetközi információbiztonsági, kibervédelmi, létfontosságú információs infrastruktúra védelmével kapcsolatos gyakorlatokon, illetve kapcsolatot tartson és építsen más hatóságokkal, valamint az eseménykezelő központokkal.

### *3.4.3. Eseménykezelési feladatellátás*

A biztonsági események kezelésének növekvő jelentőségét és jelentős következményeit az igazolja elsősorban, hogy a kritikus infrastruktúraként működő szolgáltatások egyre nagyobb mértékben működnek informatikai rendszerek támogatásával, vagy kifejezetten informatikai rendszereken keresztül valósulnak meg. Ebből adódóan az elektronikus információs rendszerekkel kapcsolatos fenyegetettségek és kockázatok közvetlenül érintik magát a kritikus infrastruktúrát is. Megállapítható, hogy egy nem megfelelően kezelt incidens a dominó hatás által nehezen azonosítható és lehatárolható károkat okozhat a termelés, a szolgáltatás működése terén, így a lakosság életében is.

Az Ibtv. hatálya alá tartozó szervezetek elektronikus információs rendszereit érintő súlyos biztonsági eseményekről az üzemeltetőknek tájékoztatniuk kell az esetükben illetékes eseménykezelő központot, ahol szükség esetén segítséget kap az esemény kezelésében, és együtt kell működnie az incidens kivizsgálásában. Az Ibtv. és végrehajtási rendeletei a kijelölt létfontosságú rendszerek és létesítmények elektronikus információs rendszerei tekintetében a kiberincidensek kezelését, vagyis az informatikai biztonsági eseménykezelő központ működtetését a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet feladatkörébe helyezte. Az eseménykezelő központ részletes feladatait, hatáskörét az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet szabályozza a következők szerint:

Biztonsági eseményekkel kapcsolatosan:
- biztonsági események és kockázatok kezelésére vonatkozó eljárások meghatározása,
- biztonsági események megelőzése céljából tájékoztatási és tudatosítási tevékenység végzése,
- a biztonsági események nemzeti szintű nyomon követése,
- a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítése,
- reagálás a biztonsági eseményekre,
- kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatás, korai előrejelzés, riasztás, bejelentéstétel és információterjesztés az érdekeltek számára,
- sérülékenységvizsgálat lefolytatása,
- a biztonsági eseményekről nyilvántartás vezetése (megtett intézkedések és azok eredménye beleértendő).

Sérülékenységekkel és fenyegető kockázatokkal kapcsolatosan:
- az elektronikus információs rendszerek biztonságáért felelős személyek tájékoztatása,
- a hatóságok és más eseménykezelő központok tájékoztatása,
- a sérülékenységekről és fenyegetésekről, valamint a hozzájuk kapcsolódó, javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatás biztosítása.

Összességében kijelenthető, hogy a kritikus infrastruktúrák elektronikus információs rendszerei, a kritikus információs infrastruktúrák, ezek védelme kiemelt figyelmet kap mind az EU intézményei szempontjából, mind hazai viszonylatban. Mindez a jövőben – a bekövetkező események és a megszerzett tapasztalatok függvényében – valószínűleg tovább fog mélyülni. A megfelelő biztonsági körülmények kialakítása érdekében létfontosságú egy-egy ilyen rendszer felkészültsége, vagyis a jogszabályi körülmények ismerete, a hatóságokkal történő aktív és érdemi kapcsolattartás, az együttműködésre történő hajlandóság, a megelőző szemlélet erősítése és a tudatosítás fokozása.

## 3.5. Irodalomjegyzék


- Szerződés az Európai Unióról (maastrichti szerződés), 1993.
- Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról (lisszaboni szerződés), 2007.
- Európai Biztonsági Stratégia, 2003.
- EPCIP program, 2004.
- Zöld Könyv az EPCIP végrehajtására, 2005.
- A biztonságos információs társadalomra irányuló stratégia, 2006.
- Az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások keretszabályozásának átalakításáról szóló Európai Bizottsági javaslat-csomag, 2007.
- CIP irányelv, 2008.
- Külügyi Bizottság jelentései (2010-2017)
- Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása című közlemény, 2009.
- Európa 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégia, 2010.
- Az információs rendszerek elleni támadásokról szóló irányelv-javaslat, 2010.
- A kritikus informatikai infrastruktúrák védelméről szóló közlemény, 2011.
- CIIP Cselekvési terv, 2011.
- A kritikus informatikai infrastruktúrák védelme - eredmények és következő lépések: a globális kiberbiztonság felé, Európai Parlament állásfoglalása, 2012.
- Az Európai Unió Kiberbiztonsági stratégiája, 2013.
- NIS irányelv, 2016.
- GDPR rendelet, 2016.
- Kiberbiztonsági jogszabály, 2019.
- Az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló rendelet, 2019.
- Cecei Katalin, Mórocz Attila: Klímaváltozás és a kritikus infrastruktúra. IN: AGRO-21 Füzetek, 2004. 36. szám
- Bonnyai Tünde: A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében. PhD értekezés, 2014.
- Myriam Dunn Cavelty, The Art of CIIP Strategy, 2014.
- Dr. Bonnyai Tünde: Az információbiztonság értelmezése a kritikus infrastruktúrák védelme kapcsán. Szakdolgozat, 2018.
- Bognár Balázs-Bonnyai Tünde-Vámosi Zoltán: Kritikus infrastruktúrák védelme I. Egyetemi jegyzet, 2019.
- Magyar Jogtár

## 3.6. Kiemelendő incidensek


– https://www.equifaxsecurity2017.com/frequently-asked-questions/
– https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; https://www.microsoft.com/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/?source=mmpc
– https://www.ibm.com/downloads/cas/ZYKLN2E3
– https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
– https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en

# 4. GÖRGEY PÉTER: A VILLAMOSENERGIA SZEKTOR MINT KRITIKUS INFRASTRUKTÚRA

## 4.1. Bevezetés

Az embert az állatoktól leginkább a gondolkodás képessége különbözteti meg. Az ember az evolúció folyamatában e képesség révén jutott el az egyszerűbb eszközök, majd szerszámok, végül a gépek használatáig. E fejlődés alapvető mozgatója az élethez szükséges alapvető tevékenységek (pl. élelemhez jutás, védekezés az időjárási viszontagságoktól, vadállatoktól) lehető leghatékonyabb elvégzése. A tűz kezdetben ösztönös, majd egyre tudatosabb használatával az energia használata is fokozatosan az emberi létezés részévé vált. Az eszközök (pl. kő), szerszámok (pl. kőbalta), majd gépek (pl. emelők) kialakulását az emberi képességek, erő, energia kiterjesztésének az igénye mozgatta. Minőségi ugrást jelentett, amikor az ember az izomerő helyett más energiaforrásokat is elkezdett kiaknázni. Elsőként a tüzet használta, majd az utolsó néhány ezer, majd száz évben sorra jelentek meg egyéb energiafajták, valamint köztes energiahordozók is, mint pl. a villamosenergia is.

Az elektromosság, villamosság révén az ember minden korábbinál hatékonyabb energetikai technológiát kapott élete hatékonyabbá, biztonságosabbá, kényelmesebbé tételéhez. Mára a villamosság az emberi létezés, civilizáció alapvető, nélkülözhetetlen feltételévé vált. Ez egyben azt is jelenti, hogy a villamosság bármely véletlen, vagy szándékolt zavara súlyos kihatásokkal jár. Ebből következően az ember a villamosságot mindinkább az életéhez szervesen hozzátartozó, védendő értéknek tekinti.

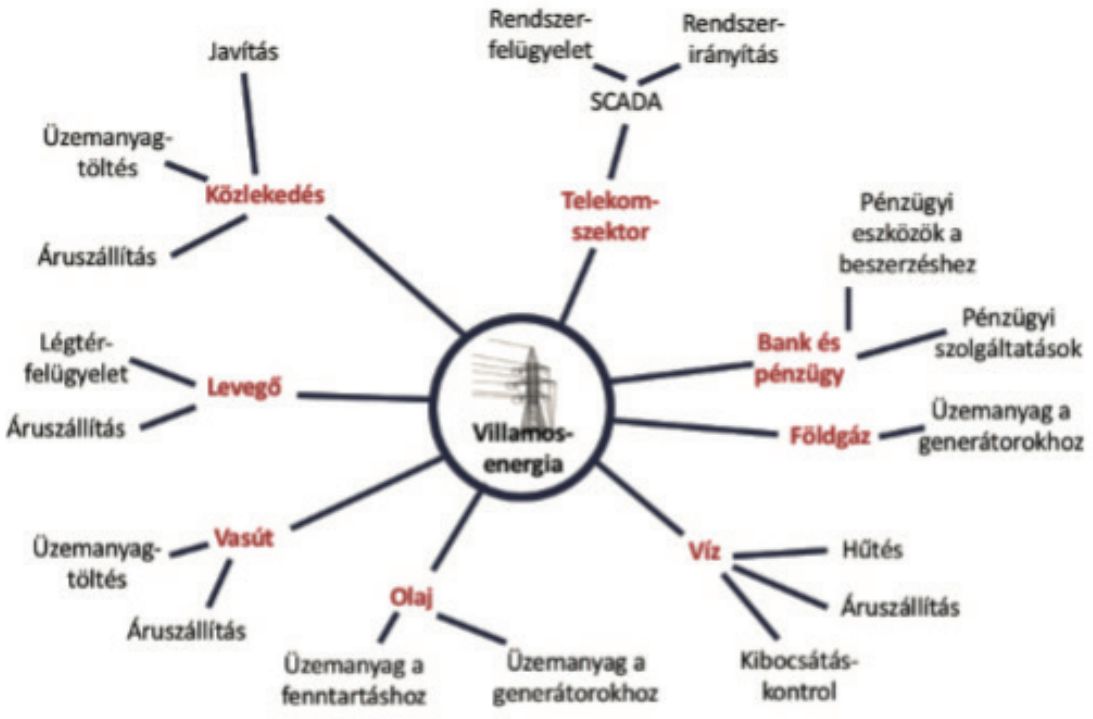
Az állatvilágnak, de különösen az emberiségnek egyik alapvető jellemzője – egyben az evolúció egyik alapvető mozgatója – az életfeltételek védelme, a támadások elhárítása. Az ember törzsfejlődése során folyamatosan fejlesztette a védekezés eszközeit, módszereit.

Az emberi létezés alapvető feltételeit biztosító – ezért különösen védendő – rendszereket *kritikus,* avagy *létfontosságú infrastruktúra*[122] gyűjtő-megnevezéssel azonosítjuk.

A villamosenergia termelő és elosztó rendszerek a kritikus infrastruktúrák körében is kitüntetett szerepet játszanak, mivel a villamosenergia relatíve könnyen alakítható át más energiafajtákba (hőenergia, mozgási energia, stb.). Ebből következően a többi kritikus infrastruktúra működésének is alapvető feltétele a villamosenergia ellátásuk biztosítása. A 1. ábra alapján is mondhatni a villamosenergia rendszer a „legkritikusabb kritikus infrastruktúra".

---

[122] Kritikus/létfontosságú infrastruktúra/rendszerelem: 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 –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna". (2012. évi CLXVI. tv. 1. § f. pont)
(Megjegyzés: elterjedt megnevezés a *kritikus infrastruktúra*, de ismeretlen okból a vonatkozó 2012. évi CLXVI. tv. megnevezése szerint *létfontosságú rendszerelem*.)




*1. ábra: A villamosenergia ellátás kapcsolatai és hatásai*
*Forrás: http://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_A_kiberter_vedelme.pdf*
*(Utolsó letöltés: 2019. augusztus 28.)*

Ráadásul a villamosenergia rendszer tipikusan olyan infrastruktúra, amely messze túllép a nemzeti kereteken és nagyobb zavarai gyakran túlmutatnak egy-egy ország villamosenergia rendszerein, szélsőséges esetben akár kontinentális kiterjedésűek is lehetnek. Erre is tekintettel a 2012. évi CLXVI. törvény 1. § c. pontjában európai szinten is definiálja a *kritikus infrastruktúra* fogalmát[123].

A fentiek alapján a villamosenergia rendszer kiemelt védelemre szorul. Különösen annak tudatában, hogy a technológiai fejlődés nem kívánt „mellékhatásaként" olyan technológiák jöttek létre és jutottak avatatlan kezekbe, melyekkel egyre hatékonyabban támadható a villamosenergia rendszer, pontosabban annak digitális irányító és szabályozó informatikai rendszerei.

Erre is tekintettel a kritikusinfrastruktúra-védelmi törvény végrehajtási rendeleteként kiadott 65/2013. (III. 8.) Korm. rendelet 1. § 3. pontja meghatározza a kritikus információs rendszer és létesítmény[124] fogalmát is: „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek".

[123] Az európai értelemben vett kritikus infrastruktúra vonatkozásában a korábban említettekhez hasonló módon a 2012. évi CLXVI. tv. 1. § c. pontja az *európai létfontosságú rendszerelem* kifejezést használja.

[124] A 65/2013. (III. 8.) Korm. rendelet 1. § 3. pontja *létfontosságú információs rendszer és létesítmény* megnevezést használ.

Külföldön már történtek fogyasztói kieséssel is járó támadások.

2015. december 23-án három ukrán villamosenergia elosztó vállalat 7 db 110 kV-os és 23 db 35 kV-os transzformátorállomása ellen történt támadás. Ennek nyomán 225-230.000 fogyasztó 3-6 óráig maradt ellátatlanul. A támadó a transzformátorállomási RTU-kban a firmware[125] felülírásával elérte a megszakítók kinyitását, valamint ellehetetlenítette az RTU-k távoli elérését. Emellett rendszerfájljainak a felülírásával a kezelői munkahelyeket is működésképtelenné tette.

Egy évvel később, 2016. december 17-én ismét Ukrajnában történt támadás a Kijev energiaellátásáért felelős egyik 330/220/110 kV-os alállomás ellen. A támadás nyomán ismeretlen számú fogyasztó kb. 1 óráig maradt ellátatlanul. A támadó rendszergazdai jogosultságot szerzett az alállomás RTU-i felett, és ennek birtokában távolról kikapcsolta azokat.

Bizonyára e támadások is szerepet játszottak abban, hogy az USA Belbiztonsági Minisztériumának illetékes szerve, a US-CERT[126] 2016-ban és 2017-ben egy-egy, míg 2018-ban már két riasztást is kiadott, melyek közül a 2018. március 15-ei egyenesen az orosz kormány amerikai energetikai és egyéb kritikus infrastruktúrák elleni kibertevékenységére hívta fel a figyelmet.[127]

A jelzett támadások itt[128] kerülnek részletes ismertetésre.

Ezek az esetek megkövetelik a magyar villamosenergia-rendszer védelmét is a minden eddiginél nagyobb fenyegetéssel szemben.

A kockázatok alakulása szempontjából beszédes a 2. ábra táblázata:

| 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|
| Severe income disparity | Severe income disparity | Income disparity | Interstate conflict with regional consequences | Large-scale involuntary migration | Extreme weather events | Extreme weather events | Extreme weather events |
| Chronic fiscal imbalances | Chronic fiscal imbalances | Extreme weather events | Extreme weather events | Extreme weather events | Large-scale involuntary migration | Natural disasters | Failure of climate-change mitigation and adaptation |
| Rising greenhouse gas emissions | Rising greenhouse gas emissions | Unemployment and underemployment | Failure of national governance | Failure of climate-change mitigation and adaptation | Major natural disasters | Cyber-attacks | Natural disasters |
| Cyber-attacks | Water supply crises | Climate change | State collapse or crisis | Interstate conflict with regional consequences | Large-scale terrorist attacks | Data fraud or theft | Data fraud or theft |
| Water supply crises | Mismanagement of population | Cyber-attacks | High structural unemployment or underemployment | Major natural catastrophes | Massive incident of data fraud/theft | Failure of climate-change mitigation and adaptation | Cyber-attacks |

*2. ábra: Az első öt globális kockázat bekövetkezési valószínűség szerinti alakulása*
*Forrás: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf*
*(Utolsó letöltés: 2019. augusztus 28.)*

125 RTU: Remote Terminal Unit (végponti adatkezelő egység). Firmware: rögzített, gyakran kisméretű program és/vagy adatstruktúra, amely digitális eszközök alapvető működését, ki- és bemeneteit vezérlik.

126 US-CERT: United States Computer Emergency Rediness Team.

127 Forrás: https://www.us-cert.gov/ncas/alerts/TA18-074A

128 Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme c. jegyzet IV.5. pont

A kibertámadás 2012-ben a 4., míg ’14-ben az 5. helyen jelent meg az öt legnagyobb bekövetkezési valószínűségű kockázat között, hogy aztán az ukrán támadások tükrében némileg meglepő háromévnyi szünet után a 3., majd 4. legnagyobb kockázatként tűnjön fel. További figyelmet érdemel, hogy a jelen jegyzet zárásakor, 2019-ben az öt legnagyobb bekövetkezési valószínűségű kockázat mindegyike (!) érintheti a villamosenergia-rendszer biztonságát is.

A jelen jegyzet lezárásakor hatályban lévő, 2012-ben jóváhagyott Nemzeti Energiastratégia egyetlen szóval sem utal a magyar energiarendszereket érő kiber fenyegetésekre, az azok elleni védekezés stratégiájára. Szerencsétlen módon a vonatkozó CLXVI. törvény is 2012-ben lépett hatályba.

Alig javít a helyzeten, hogy a kapcsolódó 65/2013. (III. 8.) sz. végrehajtási rendelet 2013-ban lépett hatályba. Azóta csak a létfontosságú rendszerek és létesítmények védelméről készült rendelet (249/2017. (IX. 5.) Korm. rendelet).

A jelen jegyzet ismereteket ad pl. a villamosság alapjairól; a villamosenergia termelés, elosztás, fogyasztás sajátosságairól, ezek sajátos kockázatairól; a bekövetkezett támadásokról, azok tanulságairól; a támadások elleni védekezés lehetőségeiről; a villamosenergia szolgáltatás folytonosságának a fenntartásáról, a megszakadt szolgáltatás helyreállításáról.

Lévén a jegyzet „célközönségébe” elsősorban nem villamos szakemberek tartoznak, ezért a jegyzetben szükségszerű egyszerűsítésekkel kell élni. A villamosenergia termelése, elosztása, fogyasztása számos reáltudományág (fizika, kémia, villamosságtan, gépésztan, matematika, informatika, stb.) bázisán nyugszik, informatikai rendszereinek a védelme pedig magas szintű és speciális informatikai ismereteket feltételez. Ugyanakkor a szakmai részleteket a jegyzet csak a célja szerint szükséges és elégséges mennyiségben és mélységben tárgyalja. A jegyzet az alapvető villamossági vonatkozású elméleti és gyakorlati, majd villamosenergia rendszer ismeretek után tér át a kiberbiztonsági vonatkozású sajátosságok ismertetésére és külön szövegdobozokban hívja fel a figyelmet az adott pontban taglaltak kiberbiztonsági kockázataira, valamint azok részletesebb tárgyalásának a helyeire.

A jegyzet kizárólag publikus forrásokra támaszkodik. A bemutatásra kerülő kockázatok nem támadási receptek, hanem figyelemfelhívások a villamosenergia-rendszer azon sajátosságaira, melyek ismerete nélkülözhetetlen biztonságuk garantálásához, ezzel a biztonságos villamosenergia ellátáshoz.

## 4.2. A villamosenergia ellátás alapjai

### *4.2.1. A villamosság fizika alapjai*

Az anyagi világ elemi részecskéinek töltésük van. A töltéssel rendelkező elemi részecskék között erők hatnak. A nyugalomban lévő töltött részecskék közötti erőhatások az ún. *villamos erőtérben*, míg a mozgásban lévő töltött részecskék közötti erőhatások az ún. *mágneses erőtérben* jönnek létre.

Az elektromosan töltött részecskék és testek erőhatást gyakorolnak egymásra. Az azonos töltésűek taszítják, a különböző töltésűek vonzzák egymást. A nyugalomban lévő töltések közötti erővonalak terét *villamos erőtérnek* nevezzük. Magunk is folyamatosan villamos erőtérben élünk: a magaslégkör pozitív töltéseket tartalmazó ionoszférája és a föld között állandó villamos erőtér van jelen. Az elektromosan töltött részecskékre vonatkozó törvény értelmében két pontszerű elektromos töltés között fellépő erő egyenesen arányos a két töltés nagyságának a szorzatával, és fordítottan arányos a köztük lévő távolság négyzetével[129].

A villamosság, a villamosenergia termelése, átvitele és fogyasztása elképzelhetetlen mágneses erőtér nélkül. Ennek alapesete a Föld mágneses erőtere. Életünket a Föld, mint óriási állandó mágnes statikus mágneses erőtérében éljük. A Föld óriási mágneses dipólus, északi és déli sarkokkal. Ugyanakkor a Föld állandó mágneses erőtere mellett számos változó mágneses erőtér is jelen van életünkben (pl. rádióadók, radarok, mobiltelefonok).

A töltések rendezett mozgása, azaz az áram révén az áram járta vezető körül *elektromágneses erőtér* jön létre. Az egyirányba, egyenletesen mozgó töltések áramlásának (azaz az *egyenáramnak*) a hatására állandó, míg a váltakozó irányba, változó sebességgel mozgó töltések áramlásának (azaz a *váltakozóáramnak*) a hatására változó mágneses tér keletkezik. Ugyanakkor a folyamat visszafelé is működik, azaz a mágneses erőtér változása erőt fejt ki a vezetőben lévő töltött részecskékre, mely erő elmozdítja e részecskéket, ezzel áramot hoz létre.

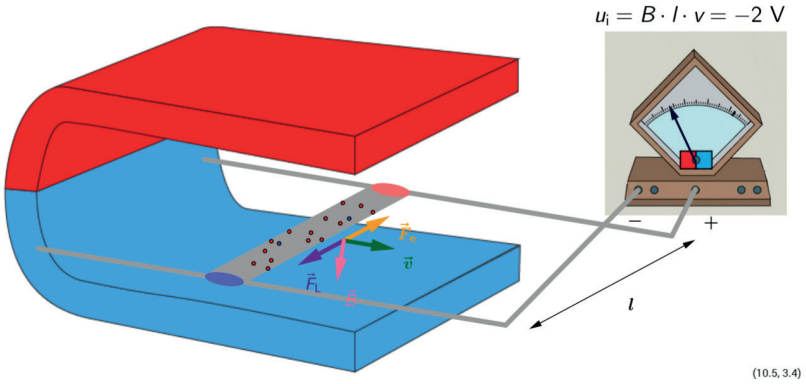
Míg az elektromosan töltött részecskék ún. monopólusok, azaz vagy +, vagy – töltésűek, addig a mágnesek dipólusok. A villamos tér erővonalaival szemben a mágneses tér erővonalai önmagukba záródó görbék.

A változó mágneses tér, valamint a mágneses térben való mozgás által a töltésekre gyakorolt erőhatás nyomán a töltések elkülönülnek, ezzel közöttük feszültség jön létre. E töltésszétválasztó hatás az *indukció*. Elektromágneses indukció nélkül nincs villamosenergia termelés, elosztás és fogyasztás. Az elektromágneses indukció lehet mozgási és nyugalmi indukció:

- A mágneses mező és valamely vezető anyag egymáshoz képesti, a mágneses erővonalakat metsző elmozdulásakor *mozgási indukcióról* beszélünk. A mozgási indukció a feszültség létrehozásának mozgással történő módja, a villamosenergia előállítás, a *generátorok* működésének az alapja. (lásd 3. ábra)
- El nem mozduló, de változó mágneses mező és el nem mozduló vezető között megvalósuló indukció esetén *nyugalmi indukcióról* beszélünk. Ebben az esetben az el nem mozduló, de időben változó áram által létrehozott elektromágneses erőtér változó mágneses erővonalai – azaz az időben változó *fluxus* – révén jön létre az indukció. A fluxus a felületet metsző mágneses erővonalak mennyisége. Minél nagyobb az időegység alatti fluxusváltozás, annál nagyobb az indukált feszültség. A nyugalmi indukció a villamosenergia elosztás, a *transzformátorok* működésének az alapja.

Az időben változó mágneses tér tehát vezetőben feszültséget indukál, melynek nagysága arányos a vezető által körülvett felületen átmenő indukciófluxus időegységre eső megváltozásával[130].

[129] Coulomb törvény
[130] Faraday-féle indukciós törvény




*3. ábra: A villamosenergia termelés fizikai alapja: mozgási indukció*
*Forrás:* http://tananyag.geomatech.hu/m/fYbnwzhL
*(Utolsó letöltés: 2019. augusztus 28.)*

Az indukált áram iránya mindig olyan, hogy mágneses hatásával akadályozza az őt létrehozó mozgást (mozgási indukció), vagy hatást (nyugalmi indukció)[131]. Az akadályozó hatás jól érzékelhető pl. kerékpár dinamó bekapcsolásakor, melyet követően a kerékpár tekerése érzékelhetően nehezebbé válik. Általánosságban is igaz, hogy a villamosenergia előállításához energiahordozókat kell befektetni és azok energiáját az *erőművekben* kell hasznosítani, az e pont szerinti alapvető fizikai jelenségek révén átalakítani villamos energiává.

A villamosenergia fogyasztóhoz való biztonságos eljuttatása szempontjából két törvénynek van különös jelentősége. Az ún. *csomóponti törvény* (avagy a töltésmegmaradás törvénye) értelmében csomópontban töltés nem halmozódhat fel, azaz bármely csomópontba befolyó és onnan kifolyó áramok algebrai összege zérus[132]. Bármely villamosenergia-rendszer csomópontokból (erőművek, *alállomások*) és azok összeköttetéseiből (távvezetékek, kábelek) áll. A csomópontok számítógépesítettek, így a kibertérből támadhatók, az összeköttetések nem, csak fizikailag. Belátható, hogy míg egy összeköttetés a jellegéből adódóan pont-pont kapcsolat, addig a csomópont több összeköttetéssel is kapcsolatban van, így esetleges kiejtése nagyobb kárt okoz.

Az ún. *huroktörvény* értelmében bármely zárt hurok mentén a feszültségesések algebrai összege zérus[133]. Minél inkább hurkolt egy villamos hálózat (azaz a hálózat csomópontjai minél több csomóponttal vannak kapcsolatban), annál több benne a redundancia, annál inkább képes csomópont, vagy összeköttetés kiesése esetén is a villamosenergia ellátás fenntartására. Hurkolt rendszerben egyetlen csomópont kiesése esetén még mindig ellátható az összes többi csomópont.

[131] Lenz törvény
[132] Kirchhoff I. törvény
[133] Kirchhoff II. törvény

De mindennek mi a kiberbiztonsági relevanciája? A villamosenergia civilizációnk működtetésének alapvető energiaformája. Származtatott energia, azaz bár a természetben is jelen van a villamosság (pl. villám, sarki fény, sőt elektromos rája), de a mindennapi életben használható formában (váltakozó áram), főleg a szükséges irdatlan mennyiségben nem áll a fogyasztási helyeken rendelkezésre. A villamosenergia előállítása (pontosabban más energiafajtából való átalakítása), átvitele, elosztása és fogyasztása a fentebb csak fő vonalaiban érintett fizikai jelenségeken alapuló igen összetett és érzékeny *egyensúlyi rendszerben* valósul meg. Minél nagyobb a villamosenergia termelés során termelt, a fogyasztóhoz eljuttatott, majd általa felhasznált energiatömeg, valamint minél nagyobbak a villamosenergia ellátással szemben támasztott minőségi elvárások, annál inkább nélkülözhetetlenek az ezt biztosító egyensúly minden időpillanatban való fenntartásához szükséges egyre fejlettebb digitális vezérlés- és irányítástechnikai, felügyeleti és adatátviteli rendszerek.

A fizika minden körülmények között „tudja a dolgát". Akkor is, ha az említett igen bonyolult szabályozó és vezérlő rendszerek zavartalanul működve biztosítják a fogyasztók villamosenergia-ellátását. De akkor is, ha pl. egy kibertámadással megzavart, vagy ellehetetlenített működésű vezérlő és szabályozó rendszerek nem képesek fenntartani az egyensúlyt, melynek következtében a villamosenergia-rendszer szélső esetben akár össze is omolhat. Pedig „csak" villamos töltések mozgásáról van szó. A fizika törvényeit a jövőben a jelenleginél is sokkal inkább digitális (és éppen ezért sérülékeny) felügyeleti rendszerek „fogják munkára" és egyre inkább e digitális rendszerek határozzák meg, hogy hol, mikor, milyen úton, mekkora töltésmennyiség mozogjon az egyensúly biztosítása érdekében.

### *4.2.2. Alapvető villamos mértékegységek*

A villamosság alapját képező fizikai jelenségek lényege villamos töltések rendezett mozgása és mozgatása, a villamos áram. Az áramerősség a vezető adott keresztmetszetén áthaladó töltésmennyiség és az idő hányadosa[134]. A *villamos feszültség* számértéke az a munka, amennyit a villamos tér végez egységnyi töltésen, amíg a töltés két pont között az egyik pontból eljut a másikba[135]. A mozgó töltések munkavégző képessége, energiája, azaz a *villamos munka (energia)* egyenesen arányos a töltések mennyiségével és a feszültség nagyságával[136]. A *villamos teljesítmény* az egységnyi idő alatt végzett villamos munka[137]. Kevéssé ismert, hogy váltakozó áram esetén a teljesítmény valójában összetettebb fizikai fogalom és az előbb említett teljesítmény annak csak egyik – bár a fogyasztó szempontból hasznos – összetevője. Átfogóbban a villamos teljesítmény megnevezése: *látszólagos teljesítmény*[138]. A látszólagos teljesítmény két összetevője:

- A fentebb említett villamos teljesítmény (szakszerű elnevezésével: *hatásos teljesítmény*). Ez a teljesítmény összetevő fedezi a fogyasztó által értékelhető munkák (világítás, főzés, fűtés, szellőzés, stb.) villamos teljesítményigényét.

134 Jele: I, mértékegysége: A (ejtsd: amper). A villamosenergetikában használt nagyságrendben: kA (ejtsd: kiloamper)

135 Jele: U, mértékegysége: V (ejtsd: volt). A villamosenergetikában használt nagyságrendben: kV (ejtsd: kilovolt)

136 Jele: W, mértékegysége: Ws (ejtsd: vattszekundum), J (ejtsd: dzsúl), Nm (ejtsd: nyútonméter). A villamosenergetikában használt nagyságrendekben: kWh (ejtsd: kilovattóra), MWh (ejtsd: megavattóra), GWh (ejtsd: gigavattóra).

137 Jele: P, mértékegysége: W (ejtsd: vatt). A villamosenergetikában használt nagyságrendekben: kW (ejtsd: kilovatt), MW (ejtsd: megavatt), GW (ejtsd: gigawatt)

138 Jele: S, mértékegysége: VA (ejtsd voltamper). A villamosenergetikában használt nagyságrendekben: kVA (ejtsd: kilovoltamper), MVA (ejtsd: megavoltamper)

- A fogyasztók többségében *induktivitások* (tekercsek) is vannak. A váltakozó áram ezeken váltakozó elektromágneses teret tart fenn, melynek teljesítményigénye van. A villamos töltések tárolására képes hálózati elemek a *kapacitások*. Az induktivitások és kapacitások teljesítménye az ún. *meddő teljesítmény*[139].

A meddő teljesítménynek közvetlen fogyasztói haszna, értéke nincs, viszont nélküle nem létezik a fogyasztó számára értéket jelentő működés. A hálózati elemeken (transzformátorokon, távvezetékeken) is keletkezik meddőenergia-veszteség. A hálózat meddőenergia igényét az egyensúlyi követelmény alapján a hatásosenergia igényhez hasonlatosan termelői oldalon ugyanúgy fedezni kell, azaz a meddőenergiát ugyanúgy meg kell termelni és el kell szállítani. Nagyobb meddőteljesítményhez nagyobb áramerősség tartozik, ami viszont lényegesen nagyobb hőveszteséget okoz, mivel a veszteség az áram négyzetével arányosan nő.

Emellett a meddőteljesítmény és a feszültség is kölcsönösen hat egymásra. Váltakozó áramú feszültségkülönbség esetén többnyire meddő áram is indul, ill. feszültség növeléskor nő a meddőteljesítmény igény. Ugyanakkor visszafelé, a meddőtermelés növelése a feszültség emelkedését okozza.

A meddőteljesítmény esetében is a hatásos teljesítménnyel azonosan biztosítani kell a termelés és fogyasztás érzékeny egyensúlyát. Meddőenergia pl. erőművi generátorok túlgerjesztésével, fázisjavító kondenzátortelepekkel (sőt a távvezetékek némi saját kapacitásával is) termelhető. Szakszerűen tervezett és üzemeltetett villamos hálózat esetében a meddőenergia egyensúly modulárisan (pl. feszültségszintenként, regionálisan), de a modulok közötti kapcsolattal valósul meg. Növekedő villamosenergia igény növekvő meddőenergia igényt jelent, amelyet korszerű irányítástechnikai eszközökkel ugyanúgy menedzselni kell.

A villamosenergia ellátás további alapvető mértékegysége a *frekvencia*, amely az időegység alatti ismétlődések – váltakozóáram esetében az áramirányváltások – számát adja meg[140].

Az *ellenállás* (pontosabban egyenáramú ellenállás) a villamos vezető két pontjára kapcsolt feszültség és az ennek hatására a vezetőn folyó áram erősségének a hányadosaként értelmezett, az adott vezető villamos vezetőképességét jellemző fizikai mennyiség[141].

### *4.2.3. A villamosenergia ellátás gyakorlati alapjai*

Az 1800-as évek végén Edison és Tesla (valamint Westinghouse) között zajlott az ún. áramok háborúja. Edison az *egyenáramú*, míg Tesla (és Westinghouse) a *váltakozóáramú energiaátvitel* mellett állt ki. A küzdelem végül Teslaék, ezzel a váltakozóáramú energiaátvitel győzelmével végződött. Az más kérdés, hogy mintegy 100 év elteltével a villamos technológia fejlődése lehetővé tette, hogy meghatározott (a 4.3.6. pontban ismertetendő) speciális feladatokra a váltakozó árammal szemben éppen az egyenáram jelentsen megoldást.

Amennyiben a mágneses térben csak egyetlen áramvezető keret (tekercs) forog, akkor egyfázisú a rendszerről beszélünk. Három – közös tengelyük körül 120-120 fokos eltolással rögzített – keret (tekercs) mágneses térben való forgása esetén háromfázisú rendszerről beszélünk. Az eltolással rögzített tekercseknek köszönhetően a három fázisban egymáshoz képest eltolva változik az áram iránya és nagysága. A háromfázisú rendszer sajátossága, hogy míg a termelés oldalán a generátor tekercseinek az álló mágneses térben való forgatásával jön létre villamosenergia, addig a fogyasztó oldalán a három fázison keresztül érkező villamosenergia a motorban forgó mágneses teret gerjeszt, amely forgásba hozza a motor forgórészét, ezzel pl. gépeket hajtva. A villamosenergia ellátás egyes speciális

[139] Jele: Q, mértékegysége: var (ejtsd: volt-amper-reaktív). A villamosenergetikában használt nagyságrendekben: kvar (ejtsd: kilovar), Mvar (ejtsd: megavar)

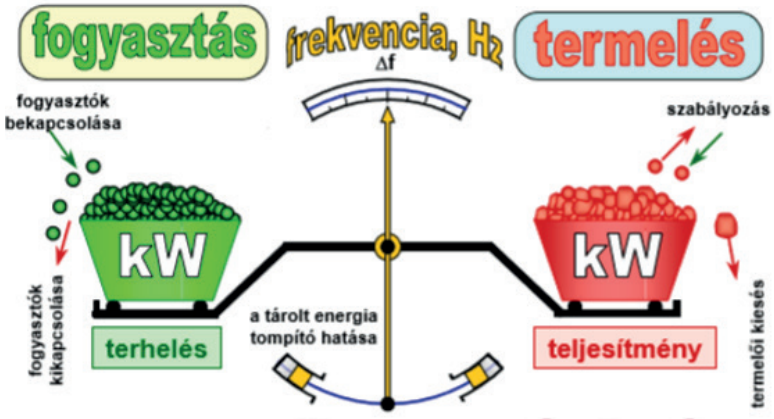
[140] Jele: f, mértékegysége: Hz (ejtsd: herc)

[141] Jele: R, mértékegysége: Ω (ejtsd: óm)

esetektől (pl. vasúti vontatás) eltekintve háromfázisú váltakozóáramú rendszerben történik.

Az akkumulátorokban tárolható egyenáramú energiával szemben a hegemón szerepbe került váltakozóáramú energia sajátossága, hogy közvetlenül nem tárolható. Más, tárolható energiafajtába alakítva, majd igény szerint onnan váltakozórammá visszaalakítva közvetett módon tárolható, ám az oda- és visszaalakítások vesztesége felemészti a megtermelt villamosenergia egy részét. Az átalakítás és a tárolás lehetőségei a későbbiekben kerülnek ismertetésre.

A váltakozóáramú villamosenergiatárolás hiányában a termelésnek és a fogyasztásnak folyamatos egyensúlyban kell lennie, azaz mindig annyi villamosenergiát kell termelni, amennyi az aktuális fogyasztás. Ugyanakkor szerencsés körülmény, hogy a fogyasztás alakulása bizonyos keretek között jól előrejelezhető. Ilyen jól becsülhető – és ezzel termelői oldalról is jól tervezhető – fogyasztói „mintázat" pl. a napon belüli, a téli és nyári, a munkanapi, vagy hétvégi (ünnepnapi) fogyasztások alakulása. A villamosenergia ellátás egyensúlyi viszonyait, az egyensúlyt befolyásoló fő hatásokat az alábbi ábra mutatja:




*4. ábra: A villamosenergia ellátás egyensúlyi rendszere*
*Forrás:* http://mavir.hu/documents/10258/107815/szabalyozas20050512.pdf/fd7f0903-53b9-4a3d-83b3-bddc290d652f *(Utolsó letöltés: 2019. augusztus 28.)*

Az ábra beszédesen mutatja, hogy a termelői kapacitás és a fogyasztói kapacitásigény (terhelés) egyensúlyának a megbomlása a frekvencia változását vonja maga után. A fogyasztói terhelés változásait annak irányától függően a termelői oldali szabályozásnak kell ellensúlyoznia a termelés növelésével, vagy csökkentésével. Hasonló módon a fogyasztói oldalon a termelés változásait annak irányától függően a fogyasztói oldali szabályozásnak kell ellensúlyoznia a terhelés növelésével, vagy csökkentésével. Szerencsés módon a villamosenergia rendszernek nagy méretéből adódóan van akkora „tehetetlenségi nyomatéka" (inerciája), amely bizonyos mértékig tompítani képes az egyensúlyt érintő akár termelői, akár fogyasztói oldali hatásokat.

Az egyensúly bármely okú, módú jelentős megbomlása (különösen a termelés és/vagy fogyasztás jelentős, nem tervezhető, üzemzavari változásai), vagy megbontása a villamosenergia ellátás biztonságát, mennyiségi és minőségi jellemzőinek a romlását, szélső esetben fenntarthatóságát kockáztatja.

Nagyobb egyensúlyi zavarok esetén elkerülhetetlen a villamosenergia rendszer üzemét felügyelő, vezérlő és szabályozó számos (később ismertetendő) termelői és/vagy fogyasztói oldali – egyre inkább (részben hálózatokba kapcsolt) digitális, ezért támadható – eszköz és rendszer helyes beavatkozása. Figyelmeztető lehet a Stuxnet malware[142] esete, amely erősen védett, leválasztott, speciálizált digitális vezérlő eszköz működését volt képes sikerrel megváltoztatni, ezzel a vezérelt eszközt tönkretenni.

[142] Malware: rosszindulatú program, szoftver

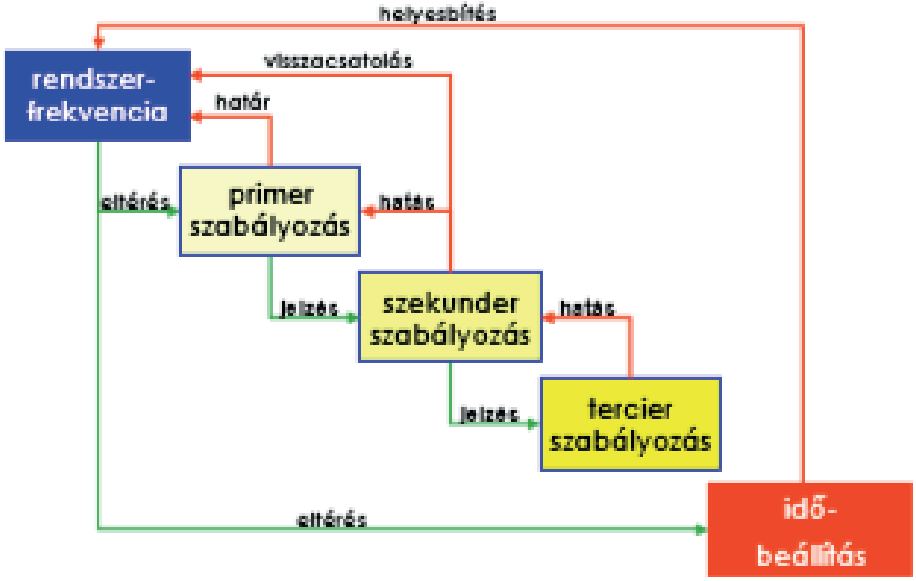
Az egyensúlyfenntartás termelői és fogyasztói oldali eszközeit a 4.2.4. pont ismerteti.

Nagy villamosenergia mennyiségnek az erőműből a fogyasztóhoz való eljuttatása esetén nem mindegy, hogy az átvitel és elosztás mekkora veszteséggel történik. Mivel ugyanazon energiamennyiség átvitele nagyobb feszültségen kisebb áram mellett lehetséges, továbbá a (hő)veszteség négyzetesen arányos az árammal, ezért belátható, hogy az átvitel feszültségszintjének az emelése kisebb áramú, azaz kisebb veszteségű energiaátvitelt eredményez.

A veszteségek a fém áramvezetők ellenállásán kívül azért is keletkeznek, mert egy kiterjedt villamos hálózat alkotóelemei kapacitással és/vagy induktivitással rendelkező – ezért a korábbiak értelmében energiát emésztő – villamos objektumok. Pl. vasmaggal összekapcsolt tekercsei révén a transzformátorok induktivitások. De a hosszú, több 10, de akár 100 km-es távvezetékek párhuzamosan futó sodronyai kapacitásként, sőt ún. földzárlat (pl. leszakadó sodrony) esetén indultivitásként sem elhanyagolhatók. E fizikai jelenségek miatti veszteségek egyaránt rontják a villamosenergia átvitel és elosztás hatásfokát.

## *4.2.4. Az egyensúlyfenntartásának eszközei a termelés oldalán*

A villamosenergia-rendszer egyensúlyának, az ezt megtestesítő 50 Hz-es frekvencia tartásának elsődleges eszköze az erőművek hierarchikusan egymásra épülő *primer, szekunder* **és** *tercier szabályozása*. Az egyes szabályozások egymás után lépnek be (5. ábra).

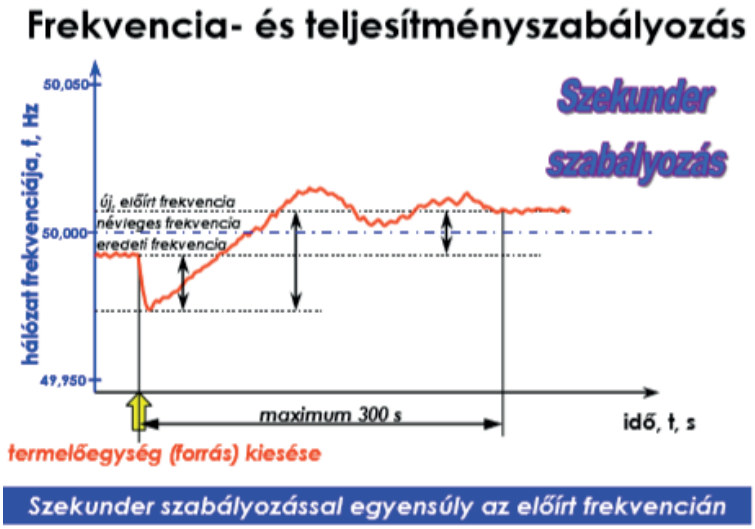



*5. ábra: Az erőművi szabályozások hierarchikus rendszere*
*Forrás:* http://mavir.hu/documents/10258/107815/szabalyozas20050512.pdf/fd7f0903-53b9-4a3d-83b3-bddc290d652f *(Utolsó letöltés: 2019. augusztus 28.)*

A primer szabályozás némi lengés után kevesebb, mint 1 perc alatt egy új egyensúlyi frekvencián stabilizálja a rendszert (6. ábra).


*6. ábra: Az erőművi primer (frekvencia) szabályozás elve*
*Forrás:* http://mavir.hu/documents/10258/107815/szabalyozas20050512.pdf/fd7f0903-53b9-4a3d-83b3-bddc290d652f *(Utolsó letöltés: 2019. augusztus 28.)*

A primer után belépő szekunder szabályozás feladata, hogy az eredeti teljesítményegyensúly beállításával a frekvenciát mintegy öt perc alatt visszaszabályozza majd tartsa a terhelés és a teljesítmény (azaz a fogyasztás és a termelés) kívánt egyensúlyát az 50 Hz-es frekvencia mellett. Mint minden szabályozórendszerben, itt is vannak szükségszerű lengések (7. ábra).




*7. ábra: Az erőművi szekunder (frekvencia és teljesítmény) szabályozás elve*
*Forrás:* http://mavir.hu/documents/10258/107815/szabalyozas20050512.pdf/fd7f0903-53b9-4a3d-83b3-bddc290d652f *(Utolsó letöltés: 2019. augusztus 28.)*

Az ezek után aktivizálódó tercier szabályozás feladata, hogy akár új – pl. gázturbinás – blokk(ok) indításával helyreállítsa az egyensúly megbomlása előtti szabályozási célú erőművi kapacitás tartalékot, ezzel a villamosenergia-rendszer visszanyerje képességét egy esetleges újabb egyensúlytalanság hatékony kezelésére. A folyamatot a szinkronórák 50 Hz-től eltérő frekvencia miatt pontatlanná váló idejének a visszakorrigálása zárja.

A villamosenergia-rendszer egyensúlya növekvő fogyasztói igény esetén az erőművi oldalon felterheléssel, ellenkező esetben leterheléssel biztosítható. Ugyanakkor az erőművek eltérő mértékben alkalmasak szabályozásra (pl. a megújuló alapú erőművek többsége csak „le" irányban szabályozható). Míg a *menetrendtartó*, de főleg a *csúcserőművek* képesek a fogyasztási igények rugalmas követésére, addig az *alaperőművek* (hangsúllyal a régebbi atomerőművek) erre jóval kevésbé alkalmasak. Bár a Paks II. Atomerőmű szabályozási képességei jobbak lesznek a jelenleg üzemelőknél, de így is messze elmaradnak pl. egy gázturbinás erőműétől. Bővebben lásd a 4.4.1. pontot.

Miközben a terjedőben lévő elosztott – közte megújuló alapú – energiatermelő kapacitások szabályozási problémákat is felvetnek, addig az ugyancsak terjedőben lévő *virtuális erőművek (szabályozó központok)* segíthetnek e kapacitások szabályozási szempontból is hatékony alkalmazásában. Lásd bővebben a 4.3.1. pontban.

### *4.2.5. Az egyensúlyfenntartásának eszközei a fogyasztás oldalán*

A termelési oldalon jelentkező hiány esetén csökkenő frekvencia nem csak a szinkronórák késését okozza. A kisebb frekvencia miatti túlterhelődés következtében elkezdenek kiesni az erőművek keringtető szivattyúi (amely különösen kritikus az atomreaktorok hűtővíz köreiben), emiatt erőművi blokkok is kiesnek, ami tovább növeli a termelés forráshiányát és egyfajta dominóhatás indul be. Radikális beavatkozás nélkül ez a villamosenergia-rendszer összeomlásához vezet. Ennek megakadályozására a mérleg másik, fogyasztói oldalán azonnali és drasztikus terheléscsökkentés szükséges. Ez a feladata az egyik legfontosabb üzemzavari automatikának, az *FTK*-nak[143], amely 49 Hz alá eső frekvencia esetén több fokozatban fogyasztói csoportok kikapcsolásával csökkenti a terhelést annak érdekében, hogy a lecsökkent termeléssel egyező mértékű fogyasztás maradjon üzemben, ezzel bár jelentős fogyasztói ellátatlansággal, de helyreállítva az egyensúlyt. 47,8 Hz alatt, ill. 51 Hz fölött az erőművi blokkok elkezdik önmagukat menteni: leválnak a hálózatról és ún. *házi-szigetüzemben* működnek tovább, ezzel teremtve meg a hálózathelyreállítás minimum feltételét. Az üzemzavari fogyasztói korlátozás másik eszköze az *FKA*[144], amely az üzemirányító döntése alapján gyors (10-30 mp-es reakció idejű) és automatikus terheléskorlátozást hajt végre.

Amennyiben az előre meghatározott módon és körben történő fogyasztói korlátozások sem biztosítják a villamosenergia rendszer új, üzemzavari egyensúlyi állapotát, akkor kerül sor a forráshiányos hálózatrészek előre definiált bontási helyeken (metszékeken) való szétválasztásra. Ezzel *szigetekre* bomlik az alapesetben egységes hálózat, melyek frekvenciáit és feszültségeit az egyes szigetek lokális villamosenergia egyensúlya, vagy egyensúlytalansága határozza meg. A fenti *rendszerautomatikák* hatásos működéséhez zavartalan adatkapcsolatok (ill. azokon megvalósuló zavartalan távmérések és automatikus távműködtetések) szükségesek. A fogyasztói korlátozó rendszerek tekintetében lásd még itt[145]!

[143] FTK: frekvenciafüggő terheléskorlátozó automatika

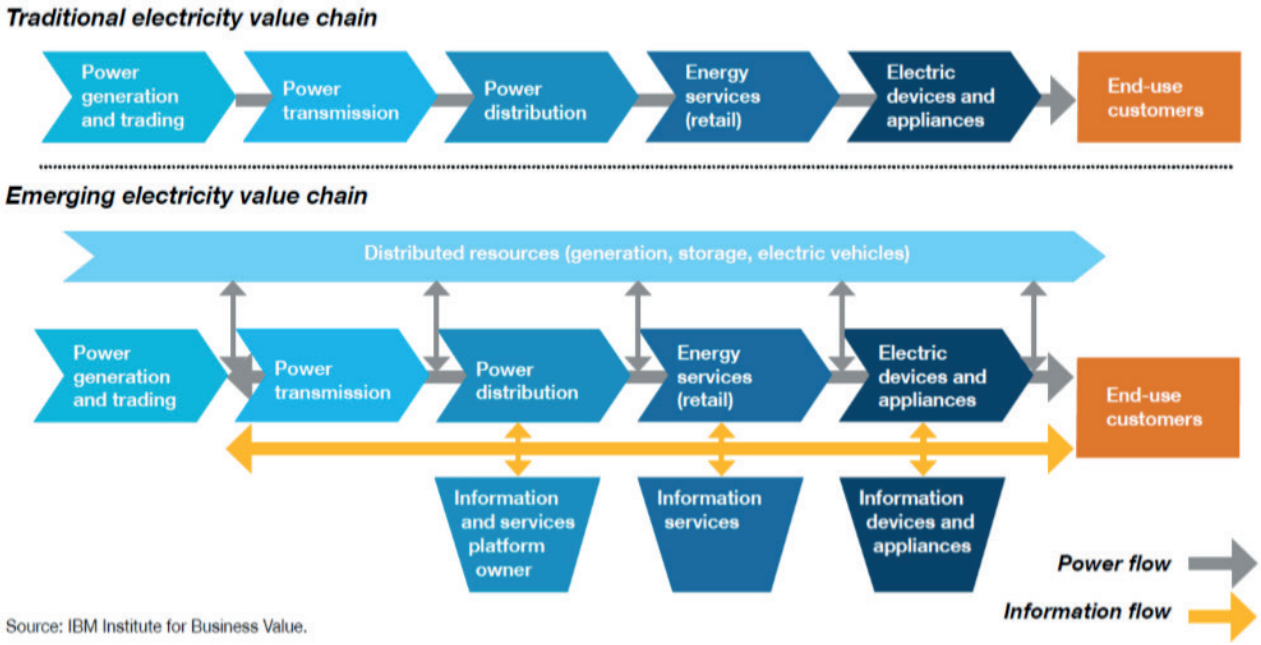
[144] FKA: frekvenciafüggetlen korlátozó automatika

[145] Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme c. jegyzet V.3. pont

### *4.2.6. A villamosenergia ellátás fő folyamata*

Tradicionálisan a villamosenergia egy többszörös energiaátalakítást, valamint szállítást, elosztást tartalmazó folyamat kimeneteként vehető igénybe a fogyasztói végpontokon a fogyasztó számára szükséges feszültségszinten, mennyiségben és minőségben. Összhangban a villamosenergia termelés erőművekbe koncentrálódó centralizált jellegével a folyamat – mint ahogy jellemzően az energiaáram is – tradicionálisan egyirányú.

Ugyanakkor a villamosenergia ellátás tradicionális folyamata, értéklánca átalakulóban van, melynek során az értéklánc lényegesen komplexszebbé válik.



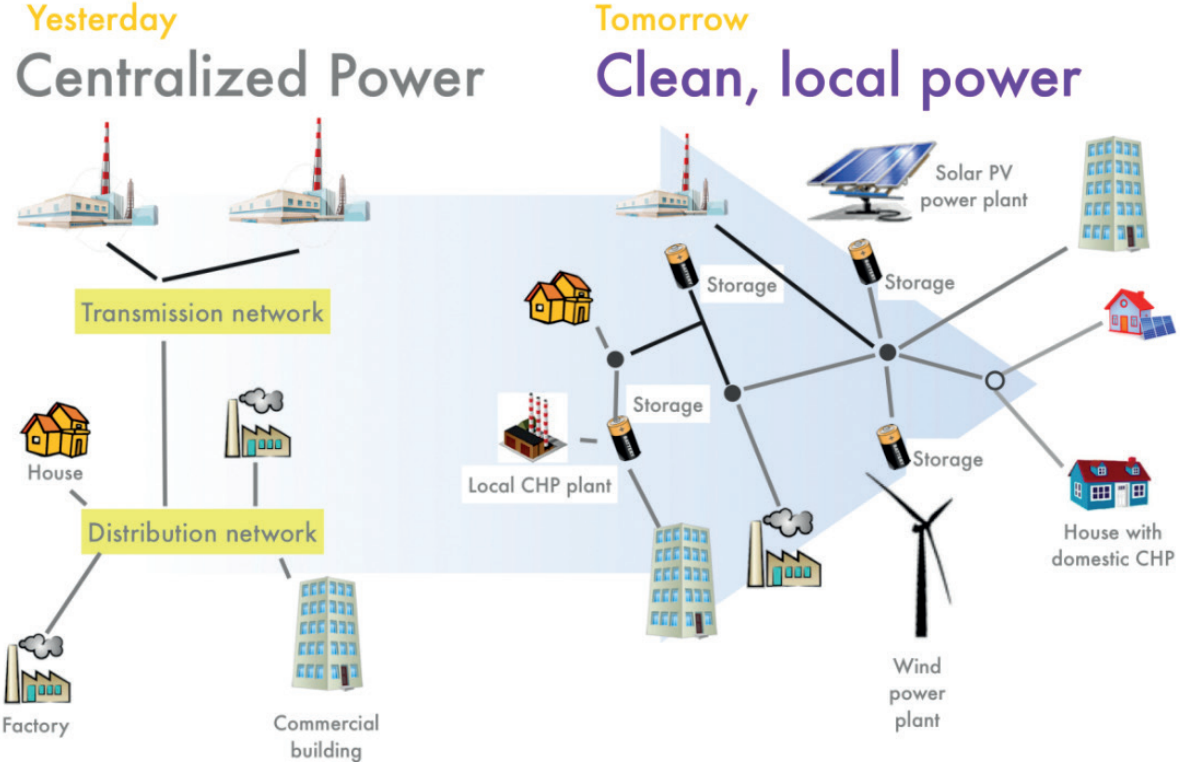

*8. ábra: A villamosenergia ellátás átalakuló értéklánca*
*Forrás:* https://rekk.hu/downloads/events/17-05%20ENTSOE%20REKK%20Energy%20Forum%20Changes%20in%20European%20Market%20Landscape.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

A *villamosenergia termelése* összetett energetikai folyamat, melyben jellemzően primer energiahordozó energiája kerül átalakításra hő-, majd mozgási-, végül villamosenergiává. A termelés a megújuló, elosztottan is kiaknázható energiaforrások előretörése ellenére bár csökkenő arányban, de még mindig jellemzően primer energiahordozók égetésével (ill. atomerőműben a szabályozott láncreakcióval), általa víz melegítésével előállított gőz energiájával történik. Megfelelő természeti adottságok esetén villamosenergia a víz, ill. a szél mozgási energiájából is előállítható. A villamosenergia termelés speciális, nagy energetikai gépek (turbinák, generátorok) nélküli esete a Nap sugárzási energiájának a *fotovillamos hatást* kihasználó, napelemekkel való közvetlen átalakítása villamosenergiává.

A *villamosenergia átvitel és elosztás* célja tradicionálisan a villamosenergia eljuttatása a földrajzilag a fogyasztóktól távoli és szétszórtan elhelyezkedő erőművektől a fogyasztói igények szerinti vételezési helyekre, igény szerinti mennyiségben és az előírások szerinti minőségben. A formálódó új értéklláncban az *elosztott energiatermelés* térhódításával, a villamosenergia termelés „demokratizálódásával" csökken az átviteli hálózat, míg és az elosztott energiatermelés (majd tárolás) nyomán megjelenő kétirányú energiaáramokkal átalakul az *elosztóhálózat* szerepe. Az „elosztás" helyébe egyre inkább talán a „megosztás" lép.

Végül a *villamosenergia fogyasztása, felhasználása* keretében ismételt energiaátalakítás történik, a felhasználás konkrét módja szerint szerinti energiafajtába (fény-, hő-, mechanikai-, stb. energiába).

Összességében a termelés említett „demokratizálódásával", bizonyos mértékben fogyasztói hatáskörbe kerülésével és ezzel a korábban passzív fogyasztók aktivizálódásával, a mindezt menedzselő *okos hálózatokkal (smart gridekkel)*[146] (és azokhoz kapcsolódó *SCADA/EMS*[147] rendszerekkel) alapvetően átalakulóban van. A 8. ábrán láthatóan az értéklánc komplexszebbé válásának a fő összetevői az elosztott technológiák, valamint a jelenleg sem kis mennyiségű és komplexitású ICS[148] rendszerek mellett még további fejlett informatikai szolgáltatások, eszközök, alkalmazások gyakorlatilag mindent lefedő megjelenése – az utóbbi esetében annak minden előnyével és kockázatával.




*9. ábra: A villamosenergia ellátás rendszerének az átalakulása*
*Forrás:* https://grist.org/article/2011-08-23-why-we-should-democratize-the-electricity-system-part-1/ *(Utolsó letöltés: 2019. augusztus 28.)*

Nagy erőművekre az átalakuló modellben is szükség lesz egyrészt pl. az ipar, a vasút jelentős villamosenergia igényének a fedezésére, másrészt az elosztott módon megtermelt energiamennyiséget meghaladó fogyasztói villamosenergia igények kielégítésére. Az elosztott energiatermelés és -tárolás megjelenésével, a hálózati struktúra és energiaáramok megváltozásával, a passzív fogyasztók aktivizálódásával, a mindezekhez kapcsolódó digitális megoldások tömegessé válásával a villamosenergia ellátás rendszerében *paradigmaváltás* körvonalazódik.

A paradigmaváltás révén minden eddiginél nagyobbá válik a villamosenergia ellátás digitális kitettsége.

[146] Közmű hálózatokhoz kapcsolódó informatikai hálózat, amely kétirányú kommunikációt és irányítási technológiákat, megosztott számításokat és ezekhez szükséges szenzorokat alkalmaz (beleértve a közmű felhasználók területére telepített berendezéseket is).

[147] SCADA: Supervisory Control és Data Acquisition (felügyeleti irányítás és adatgyűjtés), EMS: Energy Management System (energiafelügyeleti rendszer)

[148] ICS: Industrial Control System

## 4.3. A villamos energia ellátás infrastruktúrája

A villamosenergia ellátás infrastruktúrájának célja, hogy a villamosenergia a) igény szerinti mennyiségben, az előírások szerinti b) folyamatossággal és c) minőségben álljon a fogyasztók rendelkezésre.

A villamosenergia ellátás infrastruktúrájának az alapvető összetevői az *erőművek*, az átvitelt és elosztást megvalósító *távvezetékek* (kábelek), *alállomások* (transzformátor- vagy kapcsolóállomások). A villamosenergia termelését, átvitelét, kapcsolását, stb. a *primer berendezések* végzik, míg az ezek üzemi és üzemzavari állapotait felügyelő, ill. kezelő védelmi, automatika, irányítástechnikai, adatátviteli, elszámolási mérési, segédüzemi, vagyonvédelmi, stb. rendszerek a *szekunder rendszerek*. Az erőművek és a hálózat (vezetékek és alállomások) összefoglaló megnevezése: *villamos művek*.

A 4.3. pont a villamosenergia-rendszer azon szintjeire, alrendszereire és elemeire fókuszál, amelyeken koncentráltan a legnagyobb mennyiségű villamosenergia áramlik, ill. amelyek a legnagyobb mértékben képesek hatni az energiaáramra, így hibájuk – netán támadásuk – a legnagyobb zavarokat, kieséseket okozhatja. Ebben a megközelítésben a 4.3. pont így elsődlegesen a nagyerőművekre és az átviteli hálózatra fókuszál, miközben a decentralizálódó termelés, az energiatárolás és az egyéb új (okos) technológiák lehetőségeit és kockázatait is tárgyalja.

### *4.3.1. Erőművek*

A hagyományos hőerőművekben a primer energiahordozók (szén, olaj, gáz) kazánban való égetésével kinyert hőenergia gőzt fejleszt, melynek hő és mechanikai energiája turbinát hajt, amelyhez kapcsolódó generátor állítja elő a villamosenergiát. Az atomerőmű reaktorában a szabályozott maghasadás hőenergiája állítja elő a turbinát (és általa a generátort) hajtó gőzt. Vízerőműben a generátort meghajtó energia forrása a vízturbina lapátjaira zúduló víztömeg mozgási energiája.

A megújuló primer energiát villamosenergiává átalakító erőművek sorában sajátos átmenetet képez a biomassza erőmű, amely a gőzt a biomassza égetésével állítja elő. Napenergiából kétféle erőműben is előállítható villamos energia. A HCPV[149] erőművekben a napsugárzás tükrökkel, lencsékkel fókuszált hője állítja elő a gőzt, amely aztán turbinát hajt. A másikban a fotovillamos hatást kihasználva bárminemű mozgó, forgó gép, gőz, stb. nélkül a Nap által besugárzott napelemtáblák közvetlenül állítanak elő villamosenergiát. A szélerőműben a szél mozgási energiáját a széllapátok által forgatott generátorok alakítják át villamos energiává.

Az erőműveket funkciójuk, szabályozhatóságuk szempontjából osztályozva *alaperőműnek* azok minősülnek, amelyek nagy mennyiségben, csekély ingadozásokkal és – a karbantartási idők kivételével – egész évben termelik a villamosenergiát. Az atomerőművek jellemzően ebbe az erőművi kategóriába tartoznak, mivel a rendszeres terhelésváltozás a reaktorokat fokozottan igénybe veszi.

A *menetrendtartó erőművek* kifejezetten rugalmas, jól szabályozható gépegységekkel a tág határok között mozgó napi terhelések tervezhető változásainak a fedezésére szolgálnak. A tervezetthez, vagy lehetségeshez képest nagyobb fogyasztói igény, avagy erőművi blokkok kiesése, vagy rendszerüzemzavar miatti kapacitáshiány kezelésére a *csúcserőművek* szolgálnak. Ezek gázturbinás blokkjai néhányszor tíz perc alatt képesek terhelést felvenni. Speciális csúcserőművi fajta az ún. *szivattyús-tározós erőmű*, amely különösen alkalmas az egyes megújuló alapú erőművek időjárás, ill. napszakfüggésből adódó termelési ingadozások kompenzálására, de akár üzemzavari kisegítésre is. Energia túltermelésekor az erőmű szivattyúi vizet emelnek föl egy magasabb helyen lévő víztározóba. Energia hiány esetében a tározóból leeresztésre kerülő vízzel a vízturbinák elektromos energiát termelnek. Jórészt a menetrendtartó erőművek feladata az egyes megújuló alapú erőművek jobban tervezhető

[149] HCP: High Concentration Photovoltaics

napszakfüggéséből, míg inkább a csúcserőművek feladata a kevéssé tervezhető időjárási bizonytalanságokból adódó termelési ingadozások kompenzálása.

Az elosztott energiatermelés térhódításával terjedőben vannak a virtuális erőművek (szabályozó központok), amelyek területileg és tulajdonilag szétszórt, legalább 0,5 MW-os egységteljesítményű önként társult kiserőművek, tározós rendszerek kapacitásainak koordinált, látszólagosan egyetlen blokként való termelésirányítása és értékesítése. Integrált irányításuk (EMS rendszerük) megbízható adatkapcsolatot és irányítástechnikát kíván. Általában azonos jellegű berendezések (pl. szél-, naperőművek, gázmotorok) integrálódnak egy-egy virtuális erőműbe. A virtuális erőművek sikeresek a kapacitástendereken, mivel gyorsan és finoman szabályozhatók, mellyel hatékonyan simíthatók a termelési/fogyasztási csúcsok.

Közkeletű vélekedés a megújuló alapú erőművek időjárás, ill. napszak függése. A különösen a német villamosenergia termelésben egyre nagyobb szerepet játszó tengeri, parttól távoli, jórészt folyamatos és erős széllel hajtott ún. off-shore szélerőműveknél alig van ilyen függés. A kontinentális szélerőművek termelése valóban jelentősebben függ a széljárástól. A naperőművek esetében a termelés az év-, ill. napszak szerinti napállás, valamint a felhősödés függvénye. A biomassza alapú erőműnél nincs időjárás-, ill. napszakfüggés.

A „hagyományos”, forgógépes (szinkrongenerátoros) termeléshez képest a naperőművek forgó tömeg – azaz annak tehetetlensége (inerciája) – nélkül állítanak elő villamosenergiát. A naperőművi termelés arányának növekedése egyben a szinkrongenerátoros termelés arányának – ezzel a villamosenergia-rendszer inerciájának – a csökkenését is jelenti. Márpedig a csökkenő inercia a villamosenergia-rendszer súlyos zavara esetén kevésbé képes csillapítani a frekvencia változását.

A villamosenergia-rendszer fejlesztői előtt álló egyik aktuális kihívás a frekvencia stabilitás fenntartása az inercia nélküli villamosenergia-termelés egyre inkább növekvő aránya mellett. Ez fejlett teljesítményelektronikai és digitális megoldásokat kíván.

Ugyancsak közkeletű vélekedés, hogy minél erősebb (akár viharos) a szél, annál több energiát termel egy szélerőmű. Ez csak korlátozottan igaz, mert a túl erős szél veszélyezteti a szélturbina torony stabilitását, ezért ilyen esetben a lapátokat szélirányba – „vitorlába” – állítják, így a szélturbina leáll. Hasonló téveszme a napelemeket is övezi. Esetükben a túl sok, túl erős napsugárzás a napelemtábla hőmérsékletét az ideális 25 C° fölé emelve rontja annak hatásfokát.

A megújuló alapú villamosenergiatermelés egyre nagyobb aránya – és egyes termelési fajták kétségtelen termelési kockázatai – növelik a termelési ingadozásokat kezelni képes tartalék kapacitási igényeket. Ugyanakkor Németországnak már másfajta gondja van. Az off-shore szélparkok termelése időnként már meghaladja a fogyasztói igényeket. Ráadásul az észak-déli átvitelre hivatott távvezeték kapacitás szűkössége miatt az északon megtermelt energia a szomszédos országok hálózatán is „kerülve” jut el Németország déli iparvidékeire, kéretlenül terhelve a szomszédos országok hálózatait. A megújuló alapú villamosenergiatermelés ingadozásainak a kezelése tekintetében lásd a 4.4.1. pontot.

Az erőművek gépészeti és villamos berendezéseit komplex – egyre inkább (részben hálózatokba kapcsolt) digitális – védelmi, automatika és irányítástechnikai rendszerek védik és felügyelik. Súlyos üzemzavar esetén több órás áthidalási képességű akkumulátoros és dieseles alátámasztású segédüzemi berendezések gondoskodnak a kritikus erőművi elemek áramellátásáról.

### *4.3.2. Távvezetékek*

A távvezetékek biztosítják az egymástól és a fogyasztóktól távol lévő erőművektől a fogyasztók felé irányuló energiaáramok fizikai feltételeit[150]. Mennyiségileg a legnagyobb energiaáramok az *átviteli hálózaton* folynak, az átviteli veszteség csökkentése érdekében nagyobb, jellemzően 400 kV-os feszültségszinten. Az erőművekben megtermelt energiát az átviteli hálózat csomópontjait képező alállomások továbbítják a nagyfeszültségű (120 kV-os) *elosztóhálózatba*. A közép- (20, 10 kV-os) és kisfeszültségű (0,4 kV-os) elosztóhálózat egyre nagyobb arányban földkábeles kialakítású[151].

Az új technológiák (elosztott energiatermelés, tárolás, *e-mobility*) nyomán megváltozó áramlási és terhelési viszonyoknak szükségszerű hálózati kihatása is van, mindenekelőtt a kis- és középfeszültségű, de egyre inkább a 120 kV-os elosztóhálózaton is. Bővebben a 4.4.2. pontban.

Az egyre inkább szélsőséges időjárás a távvezetékeket is sújtja. Az immár egyre gyakrabban orkán erejű szél (különösen ha ónos esővel társul) sodronyszakadásokat, sőt oszloptöréseket is okoz a nem ilyen szélsőséges igénybevételekre méretezett távvezetékeken. Egyetlen távvezeték kiesése az n-1 elvnek[152] megfelelő villamosenergia rendszerben nem okozhat gondot, de egyrészt a szélsőséges időjárás általában nagyobb körzetben pusztít, másrészt a távvezeték sérüléseknek van egy másik, kevéssé ismert hatása: a távvezetéki nyomvonalakon futó száloptikai összeköttetések sérülése. Ezek az optikai kapcsolatok biztosítják egyebek mellett a villamosenergia-rendszer adat- és kommunikációs kapcsolatait. Ezek sérülése zavart okozhat a rendszer üzemirányításában, védelmi és automatika rendszereiben, az üzemzavarok kezeléséhez (is) szükséges nagy megbízhatóságú kommunikációban (adat + beszéd), a folyamatos M2M[153] kapcsolatokban.

### *4.3.3. Alállomások*

Az alállomások a villamosenergia-szállítás meghatározó csomóponti elemei. Az alállomásokon belüli energiaáramok a betápláló mező(k)ből a *szakaszolók* által kijelölve, a *megszakítók* által kapcsolva, transzformátorokkal fel-, vagy letranszformálva a *gyűjtősíneken* haladnak át a fogyasztói leágazásokig. Az energiaáram jellemzőit a *mérőváltók* mérik, a szükség szerint munkavégzés egyik biztonsági feltételét pedig a *földelőszakaszolók* biztosítják. A felsorolt primer készülékek közül hálózati szerepük és áruk miatt kiemelendők a transzformátorok. Általuk történik az erőművekben termelt energiatömeg kis veszteségű átviteléhez szükséges fel-, majd letranszformálás, valamint a feszültségszabályozás. Áruk miatt korlátozott a tartalékolásuk, így meghibásodásuk csökkenti a hálózati redundanciát, ezzel az ellátásbiztonságot. Ugyancsak kiemelendők a megszakítók, melyek egyrészt zárlat esetén védelmi parancsra megszakítják a zárlati áramot, másrészt rendszerüzemzavar esetén egyes kritikus hálózati helyeken ismét összekapcsolják az esetleg szétvált, aszinkron frekvenciájú hálózatrészeket.

[150] Az elosztott villamosenergia termelés, tárolás térhódításával a távoli nagyerőművek mellett egyre inkább sok, kisebb és közeli kis – akár háztartási méretű – „erőmű" által termelt energiát kell szállítani, „megosztani".

[151] A villamosenergia-rendszer feszültségszintjei: *kisfeszültség* (váltakozó áram esetében nem nagyobb, mint 1000 V, egyenáram esetében 1500 V; *nagyfeszültség* (váltakozó áram esetében nagyobb, mint 1000 V, egyenáram esetében 1500 V). A nagyfeszültség fogalmába a közép- és igen nagy feszültség is beletartozik.

[152] n-1 elv: a rendszer bármely egyetlen termelő, vagy átviteli elemének a meghibásodása, kiesése nem veszélyeztetheti a rendszer működését, nem okozhat távvezeték kikapcsolódásokat, jelentős mértékű fogyasztói kiesést, nem kiszabályozható áram vagy feszültség határérték túllépést, illetve nem veszélyeztheti a többi berendezés biztonságos üzemét.

[153] M2M: machine-to-machine (gép-gép) kapcsolat

A főleg az átviteli hálózati alállomásokra jellemző felsorolt berendezések némelyike közép- és kisfeszültségen hiányozhat. Pl. a transzformátor nélküli, csak az azonos feszültségű vezetékek/kábelek közötti kapcsolatokat (áramutakat) biztosítani hivatott *kapcsolóállomásokban*.

Az erőművek, távvezetékek és alállomások üzemi és üzemzavari működését szekunder és egyéb berendezések, rendszerek támogatják.

### *4.3.4. Szekunder berendezések, rendszerek*

A 4.3. pont bevezetőjében említett szekunder berendezések, rendszerek mindegyikével szemben támasztott alapvető követelmény a *megbízhatóság*. Ennek egyik alapvető garanciája a *redundancia*. A különösen kritikus – egyre inkább (részben hálózatokba kapcsolt) digitális – *villamos védelmek* esetében a redundancia nem csak egyszerű duplikálással valósul meg, hanem a két (egyébként azonos funkciójú) védelem gyökeresen eltérő kialakításával. A villamos készülékek és hálózat hibáit hárító villamos védelmekkel és *automatikákkal* (a hibák hatásait kezelni hivatott üzemzavari automatikákkal, valamint a normál működéshez tartozó üzemviteli automatikákkal) szemben további sajátos kettős megbízhatósági követelmény is fennáll: minden indokolt esetben (pl. zárlat) garantáltan működniük kell, ugyanakkor nem szabad működniük (pl. megszakítót tévesen kikapcsolva), ha az nem indokolt. A redundancia kapcsán további követelmény az ugyanazon hálózati rendellenesség kezelésére hivatott védelmek működésének a *szelektivitása*, azaz egyidejű működésük tervszerű megelőzése, ezzel a fogyasztói kiesések minimalizálása. Ezt az egyes eszközök eltérő működési (kioldási) idejével, érzékenységével, stb. lehet biztosítani, megadva a lehetőséget egy esetleges nem, vagy hibásan működő védelem helyett üzembe lépő *fedővédelemnek*. Az időnek, a *gyorsaságnak* is különös jelentősége van. Bár a 4.2.3. pontban írtak alapján a villamosenergia-rendszernek van bizonyos tehetetlensége, azaz zavartűrű képessége, de ez nem korlátlan. Különösen a nagyobb területeket érintő extrém időjárási viszonyok (pl. pusztító, orkán erejű szél, kiugró klímahasználatot okozó hőhullám), avagy nagy erőművi blokkok kiesése (pl. vízerőművek tartós aszály miatt kiürülő víztározói miatt) bonthatja meg az egyensúlyt, melyet a védelmeknek és automatikáknak kell gyorsan kezelniük. A védelmi működések milliszekundum (a másodperc ezredrésze) nagyságrendbe esnek. A villamos védelmekre és automatikákra vonatkozó bővebb információk itt[154] olvashatók.

Az *irányítástechnikai rendszerben* az erőművi, alállomási RTU-k *távjelzésekkel* és *távmérésekkel* képezik le a villamosenergia-rendszer üzemi és üzemzavari állapotait, ill. fogadják az üzemirányító rendszer felől érkező *távparancsokat*, ezzel biztosítva a villamos berendezések *megfigyelhetőségét és irányíthatóságát*.[155] Az RTU-k és üzemirányító központi SCADA rendszer(ek) közötti adatforgalom fenntartása a dedikált adatátviteli hálózat feladata. Az üzemirányító egyrészt a SCADA rendszerek révén kap átfogó képet a villamosenergia-rendszer nyers, vagy feldolgozott mennyiségi és minőségi jellemzőiről, másrészt egyre fejlettebb technológiákat (pl. Fuzzy logikát[156]) tartalmazó számítógépes támogatás mellett ennek révén végezheti, vagy végeztetheti el a szükséges üzemi, vagy üzemzavari beavatkozásokat, távműködtetéseket. Üzemirányítás, az ennek előfeltételét jelentő irányítástechnika nélkül nem beszélhetünk villamosenergia-rendszerről. Az irányítástechnikai rendszerekre vonatkozó bővebb információk itt[157] olvashatók.

---

154 Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme c. jegyzet V.2. és V.3. pontok

155 Megfigyelhetőség és irányíthatóság: irányítástechnikai alapelv, melynek értelmében csak olyan rendszer tartható kézben, melynek az aktuális állapotára vonatkozó valamennyi releváns információ, valamint az ezek ismeretében szükséges beavatkozások lehetősége rendelkezésre áll.

156 Fuzzy logika: eljárás pontatlan, „elmosódott” adatokon végzendő logikai műveletekre.

157 Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme c. jegyzet V.1. pont

Az itt[158] bővebben ismertetésre kerülő rendszerek tágabb értelemben az ICS rendszerek körébe tartoznak. Ezek hibás működése, de főleg működésük redundanciát is érintő megzavarása a villamosenergia ellátás akár súlyos zavarát is okozhatja.

A bevezetőben említett 2015. decemberi ukrán eset szerinti jelentős fogyasztói ellátatlanság a megtámadott alállomási RTU-kon keresztül a megszakítók kikapcsolásával volt előidézhető.

Ennél is jóval súlyosabb következménnyel járhat az alállomások üzemeltetését, a villamosenergia-rendszer üzemirányítását végző SCADA rendszerek sikeres támadása, mivel ezeken keresztül a támadó szélső esetben képessé válhat megszakítók akár több felügyelt alállomáson is történő, azaz tömeges kikapcsolására is, ezzel nagyobb régiót is ellátatlanná téve.

Távlati kockázat, ha az alállomásokon is megjelenik az IIoT[159], melynek sikeres támadása közvetlen hozzáférést adhat az alállomási primer készülékekhez.

A villamosenergia-rendszer működésének gazdasági alapját az adja, hogy a hazai és külföldi termelők, az átvitelt és elosztást végzők, a fogyasztók és az egyéb szereplők (pl. kereskedők) a termelt, fogyasztott, ill. kezelt villamosenergia hiteles, számszerű jellemzőinek az ismeretében számolhassanak el egymással. Ennek mérési feltételét az *elszámolási fogyasztásmérő rendszerek* biztosítják. Az *okos mérők (smart meterek)* terjedésével egyre inkább a kisfogyasztóknál is létrejönnek a digitális méréskezelés, valamint a háztartási méretű energiatermelés és -tárolás feltételei.

A rendszerszinten is helyes működéshez egyes védelmeknek és automatikáknak, továbbá az erőművi, alállomási RTU-knak és az üzemirányító SCADA-knak, az elszámolási fogyasztásmérő rendszer elemeinek, a vagyonvédelmi rendszer érzékelőinek (pl. kameráknak, tűzjelzőknek) és a biztonságfelügyeleti munkahelynek egymással digitálisan kommunikálniuk kell. Ennek megvalósítása az *adatátviteli rendszer* feladata. Nagy üzembiztonsági igénye miatt ez ugyancsak redundáns kialakítású.

Közhely, de *a villamosenergia ellátáshoz is villamosenergiára van szükség*. Ez a segédüzemek feladata. Súlyos rendszerüzemzavar esetén az egyenáramú segédüzemek akkumulátorai, ill. a váltakozóáramú segédüzemek dieselgenerátorai hivatottak néhány óráig villamosenergiát biztosítani az üzemzavar utáni rendszerhelyreállításhoz szükséges alapvető funkciók – azaz az irányítástechnika, az adatátvitel, a védelmek, automatikák működése, a távkapcsolások – fenntarthatóságához, továbbá az alapvető gépek működéséhez.

Különösen speciális eset egy rendszerüzemzavar utáni teljes leállásból a Paksi Atomerőmű és a Mátrai Erőmű újraindítása (ún. *blackstart*-ja). Ehhez egy-egy másik kisebb, könnyebben és gyorsabban indítható erőmű – a Paksi Atomerőmű esetében a Dunamenti Erőmű gázturbinás blokkja, a Mátrai Erőmű esetében a lőrinci gázturbinás erőmű – villamosenergiájára van szükség. Blackstart esetén az energia speciális eljárásrend szerint jut el a két erőműbe.

Rendszerüzemzavarok miatti nagy áramszünetek voltak, vannak és lesznek is. A legtöbb fogyasztót érintő áramszünet 2005. augusztusban, Indonéziában volt, ahol 100 millió (!) ember mintegy 7 órára maradt ellátatlanul. A leghosszabb áramszünet 1999. márciusában Brazíliában volt, amely mintegy 97 millió ember 30 órás (!) ellátatlanságát okozta. Pedig ezek nem is voltak szándékosak…

[158] Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme c. jegyzet V.1-V.3. pontok

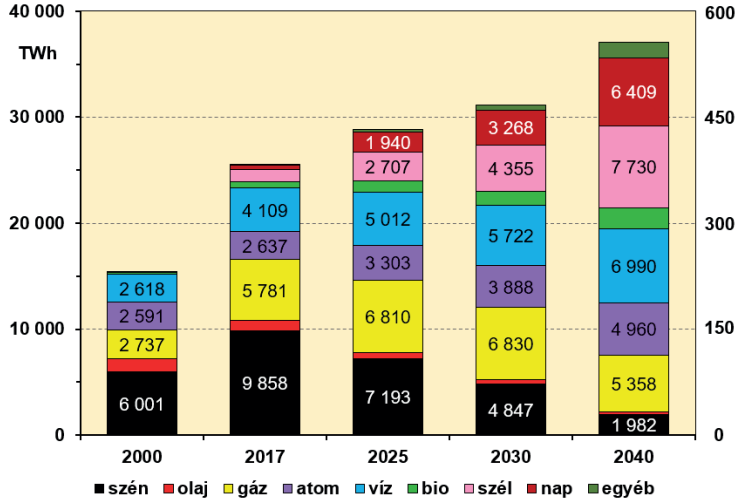
[159] IIoT: Industrial Internet of Things

### *4.3.5. Rendszerirányítás*

A villamosenergia-infrastruktúra csúcsán a rendszerirányítás áll. Ennek kiemelt feladata a villamosenergia-rendszer egyensúlyának a fenntartása, ehhez az előző pontokban ismertetett összetevők összehangolt működésének az irányítása. Feladatai rendkívül összetettek és a nemzeti villamosenergia-rendszerek összekapcsolásával egyre inkább átlépnek az országhatárokon, így kontinentális koordinációt igényelnek. Az európai átviteli hálózati rendszerirányítói együttműködés kerete az ENTSO-E[160].

### *4.3.6. A jövő villamosenergia-rendszerének a struktúrája*

A jövő villamosenergia-rendszerének a struktúrája jelentős mértékben a jövőben gazdaságosan és a klímavédelmi szempontoknak is megfelelően elérhető primer energiaforrások **összetételének, az** *energiamixnek* a függvénye. Ennek 2040-ig várható alakulását az alábbi ábra mutatja:




*10. ábra: A világ villamosenergia-termelésének energiahordozónkénti az alakulása*
*Forrás: Stróbl Alajos közlése – WEO 2018*

Szembetűnő a megújuló energiákon alapuló termelő kapacitások további masszív növekedése (az alig növekedő víz- mellett az egyre olcsóbban elérhető szél- és napenergia). Egyes off-shore szélparkok beépített teljesítménye már a nagyerőművekével vetekszik (pl. Ír tenger, Walney-sziget, 695 MW). Jelentős átrendeződés várható a hagyományos nagyerőművek energiamixében is: a szénalapú termelő kapacitások jelentős visszaszorulását alapvetően a gázalapúak pótolják, az olajalapúak jelentős és az atomalapúak csekély csökkenése mellett. Az energiamixben 2020-ban 48, majd 2040-ben várhatóan 60%-os részarányt képviselő megújuló energiatermelő kapacitások jellegükből adódóan a villamosenergia-rendszer struktúra elmozdulását vetítik előre a decentralizálódó energiatermelés irányába.

> Az átalakuló struktúra fokozott digitális támogatásigénye a villamosenergia-rendszer sérülékenységének a növekedését is előre vetíti.

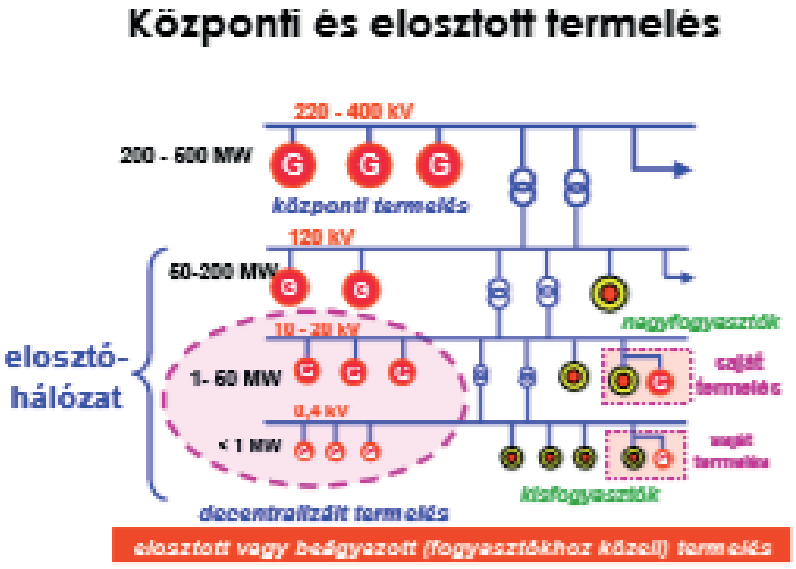
[160] ENTSO-E: Europian Network of Transmission System Operators for Electricity. A szervezet 36 ország 43 rendszerirányítóját tömöríti (2019. augusztusi állapot).

A villamosenergia-rendszer erősáramú elemeit régen alapvetően elektromechanikus elemekből (relékből, mutatós mérőműszerekből, kormánykapcsolókból, valamint egyenáramú jelzőkábelhálózatból) álló szekunder rendszer tartotta kézben. Elvükből adódóan ezek zavarérzékenysége csekély, távoli támadhatósága pedig nulla. Mára egyre elterjedtebbé váltak a digitális védelmek és automatikák, mérők, számítógépes megjelenítők és a mindezek közötti digitális adatkapcsolat. Fokozatosan visszaszorul az erősáramú készülékek és a rohamosan terjedő IED-k[161] közötti jelzőkábelezés. A mindeddig elkülönült erősáramú berendezések maguk is digitális objektumokká, az erőművi, alállomási IIoT hálózat részévé válnak.

Míg régebben az átviteli és 120 kV-os elosztóhálózati alállomások személyzetesek voltak és analóg kapcsolatban álltak az üzemirányítóval, addig ma ezek már kivétel nélkül távkezeltek, digitális rendszerekkel felügyeltek.

> Az ukrán esetekben az RTU-kra jogosultságot szerezve a támadók kizárták az üzemirányítást a támadással okozott fogyasztói ellátatlanságok távoli megszüntetésének a lehetőségéből. Az ellátást végül csak a kezelőknek az alállomásokba való kiküldése után sikerült helyreállítani. Egy az ukránnál kiterjedtebb támadás esetén elsősorban a mozgósítható kezelők száma, másodsorban a velük a tartós áramszünet miatt vélhetőleg egyre inkább akadozó vezetékes és mobil kommunikáció okozhat gondot.

A korábban jellemzően hierarchikus, masszív nagyerőművi energia betáplálási pontokra, az erőművektől a fogyasztók felé irányuló vertikális energiaáramokkal jellemezhető villamosenergia-rendszer struktúrára támaszkodó értéklánc a 4.2.5. pontban írtak szerint komplexszebbé válik. Az energia betáplálási pontok egyre inkább elosztottan, a hálózat alsóbb szintjein, kisebb egységteljesítményekkel (akár kW nagyságrendben), horizontális energiaáramokkal is megjelennek, akár szigetüzembe elkülönülve is.

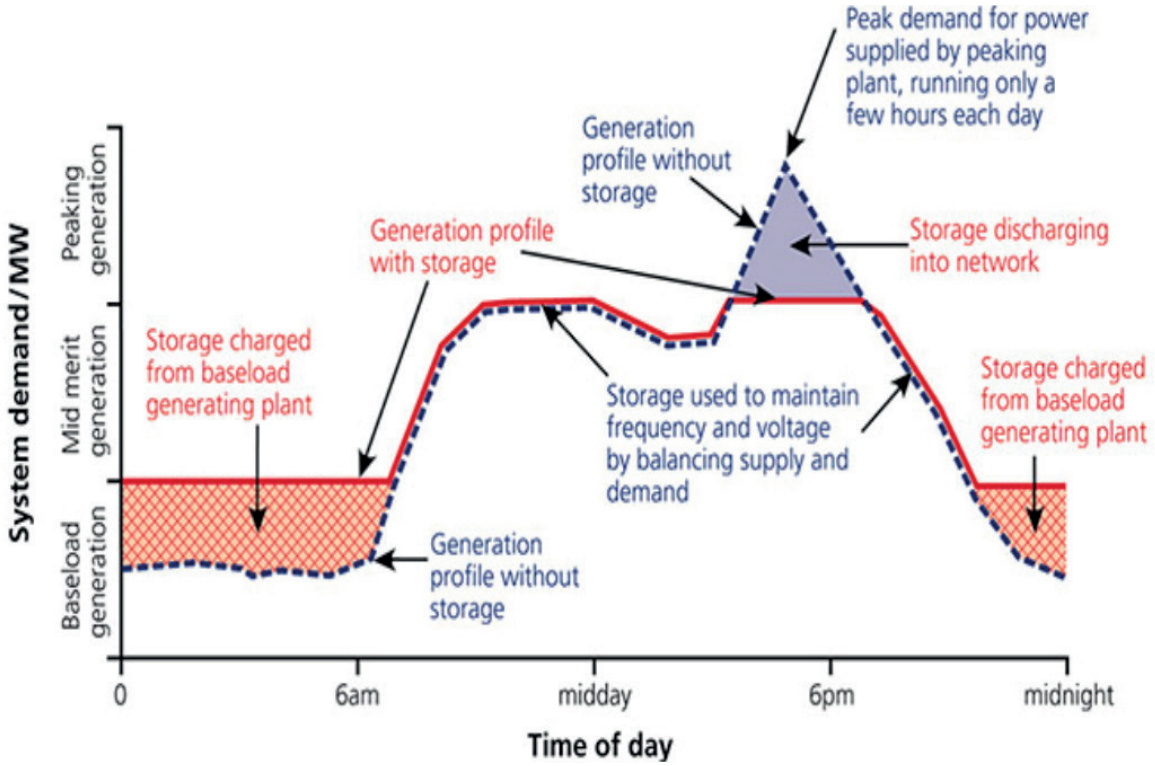



*11. ábra: A villamosenergia-rendszer változó struktúrája*
*Forrás:* http://mavir.hu/documents/10258/107815/szabalyozas20050512.pdf/fd7f0903-53b9-4a3d-83b3-bddc290d652f
*(Utolsó letöltés: 2019. augusztus 28.)*

[161] IED: Intelligent Electronic Device

Az elosztott villamosenergia termelésnek egyre kevésbé van technológiai akadálya: a jól ismert napelemek, szélturbinák mellett gázmotorok, különböző méretű gázturbinák, stb. közül lehet választani. Így az elosztott villamosenergia termelés mértéke nagymértékben politikai akarattól függő szabályozói környezet és gazdaságossági számítás kérdése.

Fokozatosan teret nyernek a különféle közvetlen (pl. akkumulátor, kondenzátor) és közvetett (pl. sűrített levegő, lendkerék) energiatároló berendezések. Elvileg az elektromos autók is részesei lehetnek a villamosenergia tárolásnak, bár ennek hálózati hatásai tekintetében még intenzív szakmai polémia zajlik. Az elosztott energiatárolás terjedése megfelelő tarifális feltételek mellett további lökést adhat a megújuló energiatermelés további térhódításának, mivel hatékonyan képes kezelni az egyes technológiák 4.3.1. pontban taglalt kétségtelen napszak, ill. időjárásfüggése miatti termelési kockázatot. A villamosenergia tárolás alkalmas technológia a villamosenergia-rendszer napi terhelési csúcsainak és völgyeinek a 11. ábra szerinti kiegyenlítésére is (ezzel a rendszeregyensúlyfenntartásához szükséges szabályozási szükségletek csökkentésére), de akár a hálózatra visszatápláló elosztott energiatermelő kapacitások feszültségnövelő hatásának a kezelésében, továbbá egyéb szolgáltatások formájában is.




*11. ábra: A villamosenergia tárolás hatása a napi terhelési görbére*
*Forrás:* https://www.mvmpartner.hu/hu-HU/Szolgaltatasok/Villamos-energia/Erdekessegek/Villamosenergia-taroloklehetsegesfeladataiesrendszerbeilleszthetosege
*(Utolsó letöltés: 2019. augusztus 28.)*

A jövő egyre inkább decentralizálódó termelésű (és tárolású) villamosenergia-rendszerében egyre nagyobb lesz az okos mérők és a rájuk épülő okos hálózatok szerepe. Az okos mérők szofisztikáltabb kialakításuk és kétirányú adatkapcsolatuk révén az eddigi primitívebb, rugalmatlanabb és egyirányú HKV és RKV[162] technológiákhoz képest minden eddiginél nagyobb (intelligensebb, rugalmasabb, kétirányú) lehetőséget biztosíthatnak a fogyasztók direkt és indirekt befolyásolására, szélső esetben

[162] HKV: hangfrekvenciás körvezérlés (vezérlés a villamos vezetéken keresztül a fogyasztókhoz eljutó vezérlő jelekkel); RKV: rádiófrekvenciás körvezérlés (vezérlés rádióhullámokkal a fogyasztókhoz eljutó kódokkal).

akár távlekapcsolására. Csak Magyarországon mintegy 7,3 millió[163] elosztóhálózati felhasználói csatlakozási pont van. Ezek okos mérőkkel való ellátása hatalmas potenciál, egyben esély okos hálózatok fokozatos meghonosodására.

Az okos hálózat az abba integrált okos mérőkre alapozva a pillanatnyi fogyasztás és termelés, a fogyasztói és termelői szokások feldolgozását végzi folyamatos döntési helyzetet biztosítva a fogyasztóknak, termelőknek. Az adatok magán a villamos hálózaton, vagy mobil adatátvitellel áramlanak a végponti eszközök és ezeket felügyelő felügyeleti számítógépek között. Az okos hálózatok képesek lesznek járulékos szolgáltatások széles körét nyújtani a fogyasztóknak.

Az okos hálózat speciális esete a *mikro okos hálózat (microgrid)*. A mikro okos hálózat elkülöníthető, jelentős mértékben hurkolt, jellemzően középfeszültségű hálózatrészt lefedő okos hálózat, melyben a saját termelés és fogyasztás mértéke közel azonos. Jelentős benne a belső koordináció, akár saját belső tarifa rendszer is működhet benne. A környező villamos hálózat felé energiát értékesíthet, ill. onnan energiát vételezhet. Üzemét EMS rendszer irányítja. Az okos és mikro okos hálózatok valamennyi végponti adatáviteli és felügyeleti komponense hálózatba kapcsolt digitális eszköz, ill. rendszer – annak összes előnyével és kockázatával.

Miközben önmagában a villamosenergia-termelő kapacitások decentralizációja, továbbá a tárolókapacitások alapvetően az ellátásbiztonság növekedése irányába hatnak, aközben az új, lényegesen bonyolultabb struktúrát menedzselni hivatott ICS rendszerek (esetlegesen sikeres) támadása növeli a kockázatot. Külön fel kell hívni a figyelmet a különféle ICS rendszerelemek és rendszerek közötti adatkapcsolatot biztosító – szintén masszív számítástechnikai alapokon nyugvó – rendszerek fontosságára. Ezek esetlegesen sikeres támadása nyomán az üzem-, ill. rendszerirányítás jelentős mértékben vakká, süketté és bénává válhat.

A kialakuló új struktúra a jelenleginél is jóval bonyolultabb rendszerirányítási, elszámolási, védelmi, automatikai, stb. problémákat vet fel. A minden eddiginél nagyobb IT háttér sikeres támadása kaotikus állapotot hozhat létre. Ugyanakkor digitális technika nélkül ma már esélytelen a villamosenergia ellátás. Nem kiberbiztonsági téma, de a kitettséget jelzi, hogy egy komolyabb napkitörés, de szélső esetben egy ún. EMP[164] bomba robbantása esetén jelentős zavarok keletkezhetnek a közműszolgáltatásokban, a közlekedésben, a távközlésben, stb. Mindez különösen téli hidegben tragikus következményekkel járhat.

A jövő struktúrájának várható további jellemzője lesz az egyes országok villamosenergia-rendszereinek még szorosabb kapcsolata a *határkeresztező távvezetékek* számának és kapacitásának a növelésével. Ezek a nemzeti villamosenergia-rendszereket kontinensnyi rendszerré kapcsolják össze. A *supergridek* **r**évén távoli rendszerek is rendszerbe foglalhatók, akár kontinensek közötti, főleg nagyfeszültségű egyenáramú villamos kapcsolatokat és energiaszállítást létrehozva, jelentős megújuló alapú energiatermelés mellett. Egy több időzónát is átfogó supergridben az időzónák miatti idő- és terheléseltolódás miatt már érvényesül az eltolódó terhelési csúcsok és völgyek terheléskiegyenlítő hatása. A teljesítményelektronika rohamos fejlődésével a nagy feszültséget és teljesítményt is kezelni képes *egyenáramú betétek* két, akár aszinkron járó váltakozóáramú rendszert is összekapcsolhatóvá tesznek, mivel az illesztésüket megvalósító egyenáramban az eltérő fázishelyzet indifferens, nem is értelmezhető. Emellett nagyobb hatásfokára tekintettel a nagyfeszültségű egyenáramú átvitel várhatóan teret fog nyerni a különösen hosszú, akár 600 km-t is meghaladó távvezetékek esetében.

[163] 2017. évi állapot.

[164] EMP: Electro Magnetic Pulse

## *4.3.7. A villamosenergia-infrastruktúra biztonsága*

Eltekintve esetleges fizikai támadástól a villamosenergia-rendszer működését – bonyolultságából, de különösen egyensúlyi érzékenységéből adódóan – számos villamostechnológiai ok zavarhatja meg. Ezek egyik csoportja a *frekvencia-zavar*, azaz pl. az 50 Hz-es alapfrekvenciától való tartós eltérés (teljesítményhiány esetén lefelé, teljesítménytöbblet esetén fölfelé). Erőművi forráskieséskor az abból fakadható tartósan alacsony frekvencia tovább súlyosbíthatja az egyébként is súlyos teljesítményhiányt, mivel alacsonyabb frekvencián az erőművi keringtető szivattyúk teljesítménye is kisebb, így túlterhelődnek, védelmük kikapcsolja őket, de ezzel további erőművi blokkok is kiesnek, tovább fokozva a forráshiányt. Frekvencia ingadozásokat okoznak a villamosenergia-rendszer egyensúly vesztésével, majd a helyreállítást célzó szabályozásokkal óhatatlanul együtt járó lengések is.

Ha a hálózat két, vagy három eltérő potenciálú eleme egymással, és/vagy a földdel közvetlen kapcsolatba kerül, akkor *zárlat* keletkezik, melyben az üzemi áramok többszöröse lép fel. A zárlat következtében csökken az átviteli kapacitás, ami *stabilitási zavart*, lengéseket okozhat (a frekvenciában, a teljesítményben, a feszültségben).

Az esetleges berendezéskárok miatt veszélyesek a pl. helytelen feszültségszabályozásból, a hatásos-meddőteljesítmény egyensúly megbomlásból fakadó *feszültség túllépések*. A terhelő áram négyzetével arányos melegedés okozta károk miatt veszélyesek a *túlterhelések*. Pl. távvezeték túlterhelése esetén a sodronyok megnyúlnak, amely az átívelési távolság elérése esetén zárlatot és ezzel a távvezeték kiesését okozza. De a túlterhelés okozta melegedés fokozottan igénybe veszi és ezzel öregíti a transzformátorok, generátorok szigetelését is.

A *szakadások* (pl. vezetékszakadás, elmaradó megszakító, szakaszoló működés) többnyire a három fázisból csak egyet (esetleg kettőt) érintenek, azaz a háromfázisú rendszer aszimmetriáját okozzák. Nyomukban csökken az átviteli kapacitás, ami egyensúlyi problémát okozhat.

Feszültség és/vagy áram *aszimmetriát* egyenlőtlen fogyasztói terhelés, ill. a három fázist nem egyformán érintő hálózati hiba (pl. megszakítóberagadás) is okozhat. Ilyen esetben kiegyenlítő áramok indulnak, melyek jelentősen növelik a veszteséget, melegedést idéznek elő a hálózatban, pl. a különösen sérülékeny generátorokban.

A villamostechnológiai kockázatok mellett a villamosenergia ellátás fő folyamatát érintő kockázatokat is célszerű áttekinteni. A primer energia biztosítása többnyire térben is időben is megosztott logisztikai folyamat, elosztott, inhomogén informatikai támogatással, ami nehezebben támadható. A primer energiák villamosenergiává való átalakítása jelenleg még nagyobb hányadban (nagy)erőművekben, jelentős irányítástechnikai támogatással valósul meg, amely leghatékonyabban a SCADA-kon, EMS-eken keresztül támadható. Az átvitel és elosztás – eltekintve egy esetleges kiterjedt fizikai támadástól (pl. több távvezeték oszlopainak egyidejű rongálása) – leghatékonyabban a SCADA-kon és az alállomási RTU-kon keresztül támadható. A fogyasztók is egyre inkább tömegesen támadhatóvá válnak a beépített távkikapcsolási funkcióval is rendelkező okos mérők terjedésével.

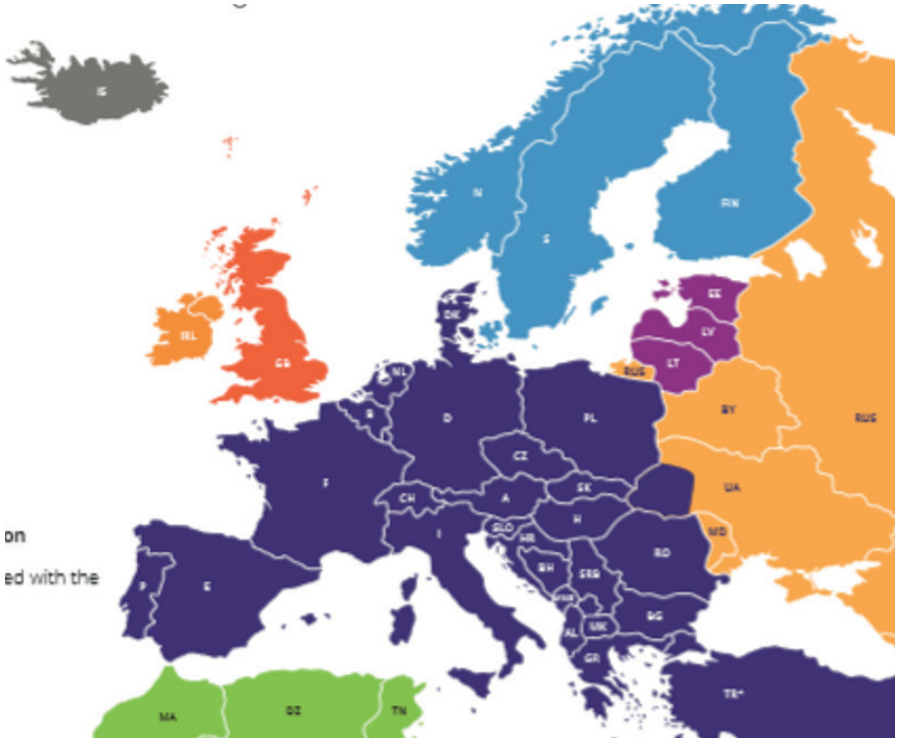
Az általános trenddel összhangban mind az erőművek, mind az átviteli és elosztóhálózati alállomások szekunder és egyéb rendszerei esetében is nő a távoli elérések, a távfelügyeletek száma. Ezek révén gyorsabbá és hatékonyabbá válik e rendszerek üzemeltetése, diagnosztikája. Ugyanakkor a távoli elérések nem kellően gondos kialakítása növelheti a támadási kockázatot.

A 2015-ös 2016-os ukrán esetekben a támadók logikusan a sok fogyasztót ellátó, jellemzően nagyfeszültségű alállomások RTU-it támadták. Csak idő kérdése valamely SCADA sikeres támadása.

Az okos mérők, a belőlük álló okos hálózatok, az EMS-ek, a virtuális erőművek rohamos terjedése egyben a támadási felületek rohamos terjedését is jelenti.

Az elosztott energiatermelés, -tárolás, az okos mérők és hálózatok, a virtuális erőművek – és ezekhez tartozó irányítástechnika – várható térhódításával egyre inkább a közép-, majd kisfeszültségű szint is támadási célponttá válhat.

Bármilyen eredetű is a villamosenergia-rendszer esetleges zavara, az ellátásbiztonság szempontjából az egyre nagyobb és integráltabb *kooperációs villamosenergia rendszerek* egyértelműen előnyösebbek a kisebb és tagolt rendszereknél. A több országot, vagy akár egész kontinenst összefogó kooperációs villamosenergia rendszerek robusztusságuk révén jobban tűrik az zavarokat, nagyobb a stabilitásuk, üzemzavari kisegítéssel rugalmasabban kezelik az átmeneti forráshiányokat.



*13. ábra: Az ENTSO-E villamosenergia-rendszer szinkronterületei, kooperációs rendszerei*
*Forrás:* http://mavir.hu/documents/10258/45985073/MAVIR_VER_2017_web_2.pdf/599179f4-d263-f4d0-b65d-3dd04acbc352
*(Utolsó letöltés: 2019. augusztus 28.)*

Minél nagyobb egy kooperációs villamosenergia-rendszer, annál inkább érvényesülnek legfőbb előnyei, azaz a) a nagyobb egységteljesítményű erőművi blokkok beépíthetősége, b) a kisebb tartalék kapacitás igény, c) a fogyasztói csúcs és völgyidőszakok kiegyenlítése és d) a gazdaságosság.

Ugyanakkor még kontinentális méretű villamosenergia-rendszerben is bekövetkezhet súlyos zavar. Pl. 2006. november 4-én Észak-Németországban tengeri hajó mozgásának a biztonsága érdekében kikapcsoltak egy folyó fölött átívelő 400 kV-os távvezetéket. Szerencsétlen módon a kikapcsolás ideje alatt a régióban jelentősen megváltozott szélerőmű termelés miatt az átviteli hálózaton is megváltozott az energiaáramlás. A kikapcsolt távvezeték hiányában jelentősen túlterhelődött az üzemben maradt párhuzamos távvezeték, melyet végül a védelme kikapcsolt. Emiatt azonban olyan láncreakció indult, melyben a környező, majd egyre távolabbi távvezetékek is sorra túlterhelődtek,

majd kikapcsolódtak. A lavina kontinentális kihatású lett, melynek során mindössze 18 mp (!) alatt a kontinentális hálózat három „szigetre” esett szét. A forráshiányossá vált nyugati „szigeten” a teljes összeomlás („black-out”) megelőzésére jelentős fogyasztói korlátozásokat léptettek életbe. A középső „szigeten” a túltermelés miatt éppen ellenkezőleg, erőműveket kellett leszabályozni, míg a dél-keleti „sziget” megőrizte az egyensúlyát.

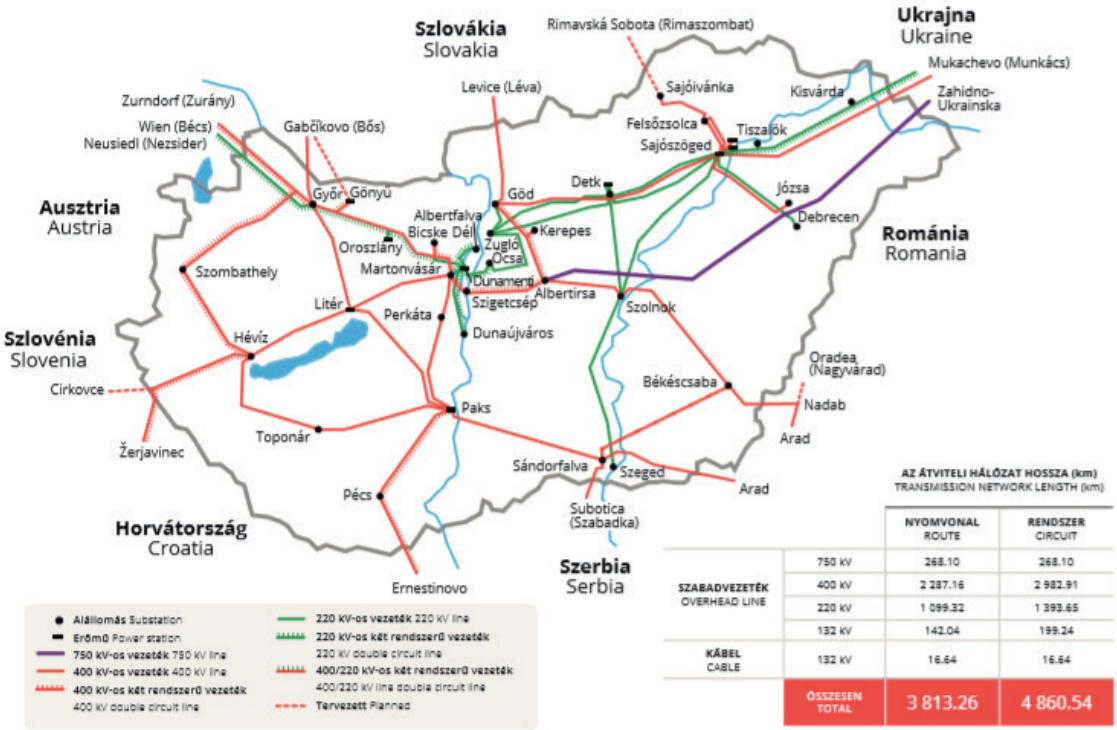
A hatalmas gazdasági károkat okozó 2006. őszi rendszerüzemzavar rámutatott arra, hogy még egy előkészített, szakszerűnek, kockázatmentesnek gondolt beavatkozás is járhat beláthatatlan következményekkel. Hát még egy esetleges gondosan megtervezett, károkozási szándékú…

Ugyanakkor az eset azt is megmutatta, hogy a villamosenergia-rendszer védelmei és automatikái bár jelentős fogyasztói kihatásokkal, de végül képesek voltak megelőzni a rendszer teljes összeomlását.

## 4.4. A magyar villamosenergia-rendszer áttekintése

A magyar villamosenergia-rendszer jelenlegi kialakítását csaknem 130 éves fejlődéssel, az 1949 óta egységesülő rendszerben részben saját fejlődési pályáját bejárva, majd az utóbbi 70 évben egyre inkább a regionális, majd az európai villamosenergia-rendszer részévé válva nyerte el.

A magyar villamosenergia-rendszer meghatározó erőművei, átviteli hálózati alállomásai és távvezetékei, a szomszédos országok villamosenergia-rendszereivel való kapcsolatai az alábbiak szerint alkotják a magyar villamosenergia-rendszer alapját:

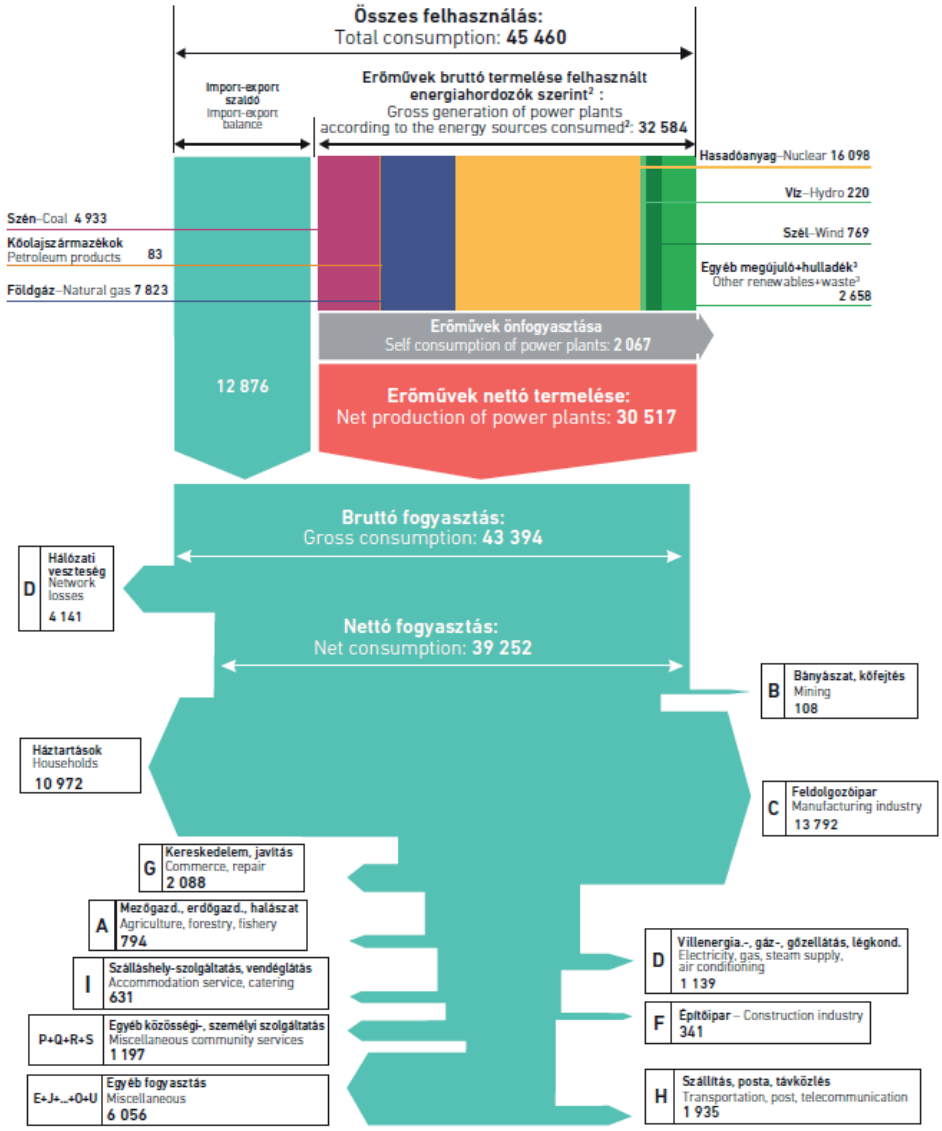



AZ ÁTVITELI HÁLÓZAT HOSSZA (km)
TRANSMISSION NETWORK LENGTH (km)

| | | NYOMVONAL ROUTE | RENDSZER CIRCUIT |
|---|---|---|---|
| SZABADVEZETÉK OVERHEAD LINE | 750 kV | 268.10 | 268.10 |
| | 400 kV | 2 287.16 | 2 982.91 |
| | 220 kV | 1 099.32 | 1 393.65 |
| | 132 kV | 142.04 | 199.24 |
| KÁBEL CABLE | 132 kV | 16.64 | 16.64 |
| | ÖSSZESEN TOTAL | 3 813.26 | 4 860.54 |

*14. ábra: A magyar átviteli hálózat*
*Forrás:* http://mavir.hu/documents/10258/45985073/MAVIR_VER_2017_web_2.pdf/599179f4-d263-f4d0-b65d-3dd04acbc352
*(Utolsó letöltés: 2019. augusztus 28.)*

A magyar átviteli hálózat jellemzően hurkolt, kielégíti az n-1 elv követelményeit. A villamosenergia ellátásbiztonság szempontjából kulcsfontosságú Paksi Atomerőműben termelt energia öt 400 kV-os távvezetéken keresztül kerül kihozatalra, sőt az új blokkok rendszerbe lépése kapcsán a hatodik 400 kV-os összeköttetés is megépül. A magyar villamosenergia-rendszer min. egy 400, vagy 220 kV-os távvezetékkel csatlakozik valamennyi szomszédos ország rendszeréhez, ezzel az európai villamosenergia-rendszerhez. Az átviteli hálózati alállomásokról a szintén hurkolt 120 kV-os elosztóhálózat veszi át az energiát, mely 120/20, vagy 120/10 kV-os transzformáció után a jellemzően 20, vagy 10 kV-os hálózaton keresztül, majd 20/0,4, vagy 10/0,4 kV-os transzformáció után jut el a kisfogyasztókhoz. A nagyobb fogyasztók 10, vagy 20 kV-on, a nagy ipari létesítmények pedig 120, vagy 220 kV-on vételezik az energiát. A magyar villamosenergia-rendszeren átfolyó energiaáram mérlege a 14. ábra szerint alakul (2017. évi állapot).




*15. ábra: Magyarország villamosenergia-termelése és -felhasználása, 2017 (GWh)*[165]
*Forrás:* https://www.mavir.hu/documents/10258/154394509/MEKH+MAVIR+VER+2017_kiadvany_vegleges_20181116.pdf/d345fdb8-7048-4af2-9a63-1d7415bb84c9
*(Utolsó letöltés: 2019. augusztus 28.)*

[165] A háztartási méretű és egyes saját felhasználásra termelő kiserőművek adatai nélkül.

A hazai termelésben a primer energiahordozók között meghatározó a hasadóanyag (2017-ben a hazai termelés 49,4%-a), valamint a földgáz (24,0%) és a szén (15,1%) szerepe. A megújuló alapú termelés (11,2%) mellett jelentős az import hányad. A 2017. évi összes felhasználás 28,6%-a importból volt fedezhető. A legnagyobb fogyasztók a feldolgozóipar (a nettó fogyasztás 35,1%-a) és a háztartások (28,0%). A 2017. évi értékelés szerint is magas import mellett kockázatot jelentenek a szükséges tartalékok nem mindig megfelelő műszaki jellemzői.

### *4.4.1. A magyar erőművek*

A magyar villamosenergia ellátás alapvető pillére a Paksi Atomerőmű. A 2000 MW összteljesítményű I-IV. blokk termelését élettartamuk lejárata után a Paks II. Atomerőmű 2*1200 MW összteljesítményű blokkjai folytatják. A másik alaperőmű, a Mátrai Erőmű blokkjai várhatóan 2023-2025 között élettartamuk végére érnek. A menetrendtartó erőművek közül a korábban legnagyobb Dunamenti Erőműben a 2010-es évek végére három működő blokk maradt (145, 241 és 408 MW teljesítménynyel). A csepeli CCGT[166] erőmű teljesítménye 410 MW, míg a Gönyűi Erőművé 433 MW. A Tisza II. Erőmű szünetelteti villamosenergia-termelését, de befektetői szándék szerint a 2020-as évek első felében két-három 225 MW-os blokkja felújításra kerülhet. A gyorsindítású tartalékként épített, de évek óta tercier szabályozási tartalékként szolgáló három gázturbinás blokk (Lőrinci, Litér, Sajószöged) működési engedélyei 2020-2023 között lejárnak. Élettartam hosszabbításuk tulajdonosi döntés kérdése. További erőművek mintegy 700 MW összteljesítménnyel állnak rendelkezésre.

A jelentős és növekvő import kitettség mellett ez az erőmű kapacitás már jelenleg sem elégséges. Utalva a témában zajló vitákra megállapítható, hogy Magyarországnak az atomenergiára is és a megújuló energiára is szüksége van. Ezek egymás kiegészítői, nem pedig riválisai. A Paks II. Atomerőmű építése a jelenleg működő négy blokk 2030-as években történő leállása ellenére biztosítja hazánkban a nukleáris alapú villamosenergia termelés tartós jelenlétét. 2023-ig mintegy 1900 MW-nyi erőmű állhat le. A pótlás importból és/vagy új termelő kapacitások építésével biztosítható. Ugyanakkor az import a térségbeli erőmű fejlesztések visszafogása miatt kockázattal jár, miközben ekkora új erőműpark létesítése nem tűnik reálisnak. Mindemellett a külföldön létesülő, időjárásfüggő megújuló erőművek (napenergia, szélenergia) egyre olcsóbb áraikkal kiszorítják az ottani hagyományos erőműveket, melynek nyomán számolni kellhet azzal, hogy kedvezőtlen időjárási körülmények esetén a hazánkba importálható villamos energia mennyisége is lecsökken, azaz a hazai forrásokkal együtt sem lesz garantálható a fogyasztói igények maradéktalan kielégítése. A biztonságos ellátáshoz még a Paks II. Atomerőmű blokkjainak üzembe helyezése esetén is szükség lesz rugalmas, piacra és tartalékként is értékesíthető erőművek építésére[167].

A rendszerirányítást végző MAVIR[168] az elmúlt években többször is felhívta a figyelmet az időjárásfüggő termelő kapacitások folyamatos növekedése miatti elégtelen szabályozó kapacitásra. További gond a Paks II. Atomerőmű belépésével rendszerszinten jelentősen megnövekedő blokkméret: a jelenlegi 500 MW-os blokkokhoz képest 1200 MW-os blokkok lépnek üzembe. Ez azért gond, mert a villamosenergia-rendszer stabilitása érdekében a gyorsan mozgósítható tartalék kapacitásokat a mindenkori legnagyobb blokk kiesését feltételezve kell biztosítani. A Paks II. Atomerőmű, mint alaperőmű egyértelmű pozitívuma a villamosenergia-import átmenetileg jelentős csökkentésének a lehetősége. Menetrendtartó erőműként az alább írtak szerinti megszorításokkal lehet tekinteni rá. Viszont az 1200 MW-ra növekedő blokkméretre tekintettel a gyorsindítású (15 perces) rendelkezésre állású tartalék erőművi kapacitás jelentősen, legalább 600 MW-tal megnövelendő. Hiányában viszont

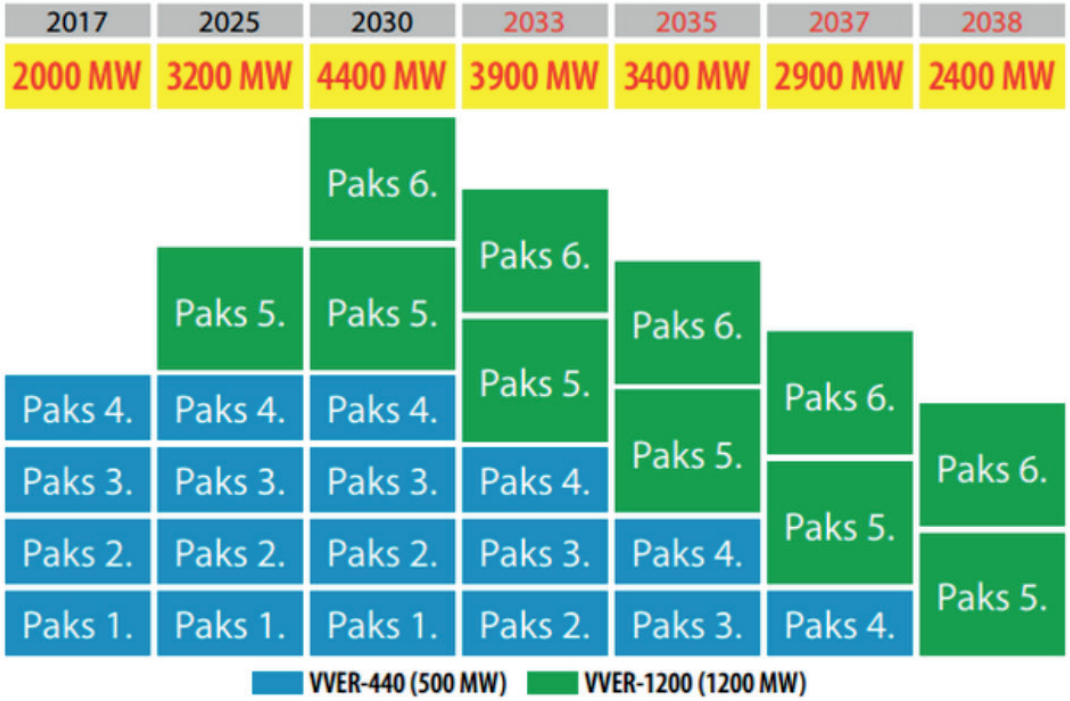
[166] CCGT: Combined Cycle Gas Turbine (kombinált ciklusú gázturbina)

[167] Prof. Dr. Aszódi Attila: Villamosenergia-ellátás hazánkban és a Paks II. beruházás szerepe (Elektrotechnika 2018/9)

[168] MAVIR: Magyar Villamosenergia-ipari Rendszerirányító Zrt.

blokk kiesés esetén nő az import kitettség és annak költsége, hiszen a gyorsan mozgósítható tartalék a villamosenergiapiac speciális, az üzemzavar kiterjedésétől függő mennyiségben rendelkezésre álló, éppen ezért drága „terméke”.

Magyarország meghatározó, nukleáris alapú villamosenergiatermelő kapacitása a Paks II. Atomerőmű belépésével az alábbiak szerint alakul:




*16. ábra: Magyarország nukleáris alapú villamosenergiatermelő kapacitásának az alakulása*
*Forrás:* https://docplayer.hu/3820778-Orosz-atomenergia-technologia-a-tudomany-es-a-versenykepesseg-szolgalataban.html
*(Utolsó letöltés: 2019. augusztus 28.)*

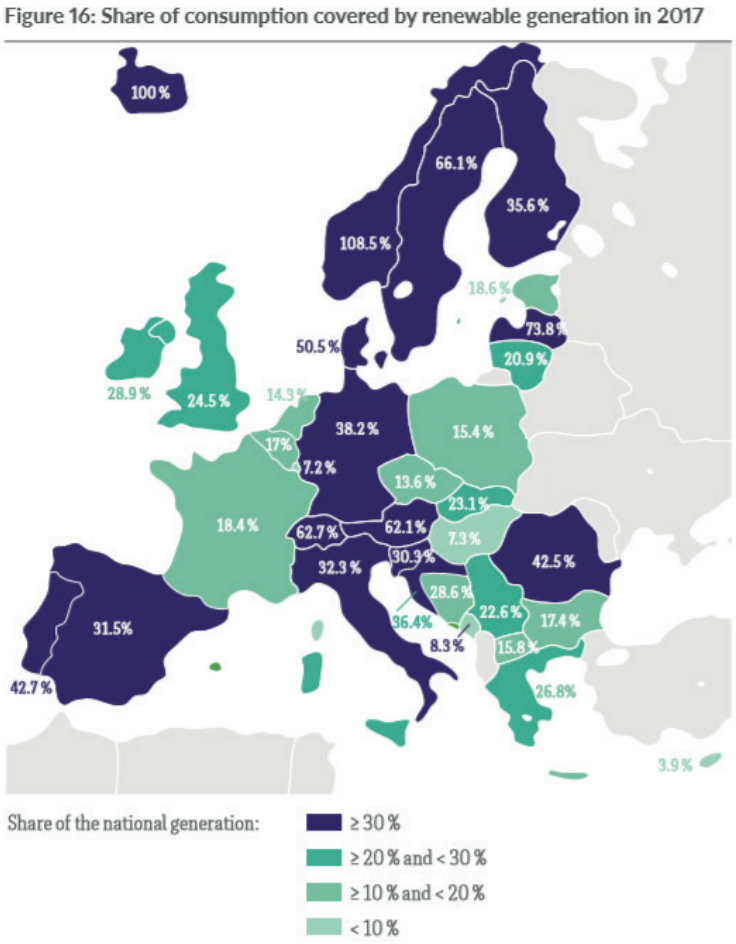
Az ábrából kiolvashatóan nagyjából 2025 és 2037 között a jelenleginél akár jelentősen nagyobb lesz a nukleáris alapú villamosenergia termelés.

> Első alkalommal 2018 augusztusában egy további kockázat jelentkezett. A mind a meglévő, mind az új paksi blokkok hűtésére hivatott Duna extrém alacsony vízállása, továbbá a tartós kánikula miatti magas vízhőmérséklete miatt mindössze tizedfokokon múlott a magyar villamosenergia-termelésben meghatározó erőmű blokkjainak a kényszerű visszaterhelése, ezzel a termelés csökkentése.

Bár a magyar villamosenergia-rendszernek szüksége van többlet (jórészt jól szabályozható) erőművi kapacitásra és az új paksi blokkok a jelenleginél lényegesen jobban lesznek szabályozhatók (pl. 100%-ról 50%-ra és vissza 100%-ra napi kétszer, de heti max. ötször, ill. évi max. kétszázszor lesznek le-, ill. felterhelhetők), azonban messze nem annyira, mint a gázturbinás blokkok.

A következő évtizedekben is dinamikusan tovább növekedő megújuló alapú – így részben időjárásfüggő – termelés is újabb, közte jól szabályozható erőművek létesítését teszi szükségessé. A magyar villamosenergia-rendszernek nagy szüksége van a 2010-es évek végének tervei szerint a Tisza II. erőműben 1215 MW, Szegeden 920 MW, Almásfüzitőn pedig 800 MW CCGT erőművek megépülésére.

Az új erőművi kapacitások azért is szükségesek, mert Magyarország jelentős lemaradást mutat a megújuló alapú villamosenergia termelésben, de a növelésre csak a szabályozható erőművi kapacitás jelentős mennyiségi és – az igénybe vehető teljesítmény-változtatási sebesség tekintetében – minőségi fejlődés esetén van biztonságos mód.




*17. ábra: A megújuló energiával fedezett villamosenergia fogyasztás aránya 2017-ben*
*Forrás:* https://docstore.entsoe.eu/Documents/Publications/Statistics/electricity_in_europe/entso-e_electricity_in_europe_2017_web.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

2017-ben Európában a megújulóval fedezett fogyasztás aránya 34.1%, a vízerőművek termelése nélkül 19,1%. Magyarország a maga 7,3%-os arányával európai szinten a 3. legkisebb arányban támaszkodott megújuló energiatermelésre. Míg a szélalapú energiatermelő egységek száma nem gyarapodott, addig a 2010-es évek második felében jelentős fejlődésnek indult a napenergia hasznosítása. A Mátrai Erőmű területén 16 MW, majd később további 20 MW, Pécsett 10 MW, Felsőzsolcán 20 MW, Pakson 20,6 MW, Füzesgyarmaton, Tiszaújvárosban és a Százhalombattai Finomítóban 18,38-18,38 MW, a Százhalombattai Erőműben 17,6 MW napelemkapacitás létesült. Kínai beruházásban Kaposvár mellett az eddigi legnagyobb, 100 MW-os erőmű létesül. Ezek mellett egyre jelentősebb (2017 végére összességében 221,19 MW) a napenergia alapú *háztartási méretű kiserőművek*[169] teljesítőképessége. A rendszerirányítás erre is tekintettel olyan üzembe helyezési előírásokat javasolt, amely támogatja az új kapacitások kiegyenlítő szabályozását. Általánosságban is az egyensúly megőrzése érdekében minden évszak- és időjárásfüggő villamosenergia-termelést az eddigieknél is nagyobb erőművi kapacitásokkal kell kompenzálni.

[169] Ebbe a kategóriába az 50 kVA-t meg nem haladó csatlakozási teljesítményű energiatermelő kapacitások tartoznak.

A 2010-es évek második felében jól szabályozható gázturbinás kapacitásként a Dunamenti Erőmű G3 blokkja (407,7 MW), avagy a Gönyűi Erőmű (433 MW) állt rendelkezésre. Gyorsindítású (15 perces) gázturbinás kapacitásként a litéri (155 MW), a sajószögedi (155 MW), a lőrinci (173 MW), az ajkai (116 MW) blokkok voltak igénybe vehetők. Ezeket a kapacitásokat a paksi blokkméret növekedés említett kompenzálási kényszerétől függetlenül is jelentősen bővíteni szükséges.

A 2010-es évek végén a magyar villamosenergia-rendszerben is megjelentek az első akkumulátoros hálózati villamosenergiatárolók: az ELMÜ 6,1 MWh, az Alteo 4 MWh tárolókapacitású, a Mátrai Erőmű pedig 5 MW teljesítményű akkumulátoros energiatárolókat helyezett üzembe.

### *4.4.2. A magyar távvezetékek*

A magyar átviteli hálózatot 3813 km nyomvonalhosszon 4861 km távvezeték alkotja. Magyarország jellemzően 400 kV-os feszültségszinten kapcsolódik a szomszédos országok villamosenergia rendszereihez. Az elosztóhálózati távvezetékek és kábelek nyomvonalhossza 161.107 km. A közép- (jellemzően 20, 10 kV-os) és kisfeszültségű (0,4 kV-os) elosztóhálózaton vidéki, ill. családiházas környezetben jellemzően légvezetékek, városokban pedig kábelek látják el a fogyasztókat. A gyakoribb időjárási szélsőségek, valamint környezetvédelmi szempontok is indokolnák a jelenlegi kb. 1/3-2/3 kábel/légvezeték arány javítását a kábelek javára, de magasabb költségük miatt ennek üteme elmarad a kívánatostól.

Pedig az időjárási szélsőségek mind gyakrabban okoznak súlyos károkat – és ezzel járó fogyasztói ellátatlanságokat – főleg a közép- és kisfeszültségű légvezetékeken. A tények tükrében főleg az egyidejű hó (vagy ónos eső) és szélvihar jár komoly károkkal. Mint pl. a 2013. március 14-én kezdődött erős lehűlés, havazás, ónos eső és szélvihar esetében. A ráfagyott több cm vastag jég miatt eleve túlsúlyos távvezetéki sodronyok és az azokat meg is lengető viharos szél többlet terhei főleg Kelet-Magyarországon tömeges vezetékszakadást, sőt oszloptöréseket, kidőléseket okoztak a közép- és kisfeszültségű vezeték hálózatban, nagy kiterjedésű és helyenként 4-5 napra is elhúzódó, mintegy 100.000 fogyasztót érintő ellátatlanságokkal. Még a MAVIR egy-egy 400 és 220 kV-os távvezetéke is súlyosan károsodott.

*18. ábra: Kidőlt 220 kV-os távvezeték 120 és 20 kV-os távvezetékekre szakad sodronyai (2013. március 15.)*
*Forrás: MVM OVIT Zrt. üzemzavari dokumentáció*

Zárlati kioldásokkal további távvezetékek is kiestek, de szerencsére még a többszörös kiesés sem okozott fennakadást az n-1 elvnek megfelelő átviteli hálózat működésében. A szélsőséges időjárásra visszavezethető szaporodó távvezeték sérülések konstrukciós változtatásokat, szerkezeti megerősítéseket tettek szükségessé.

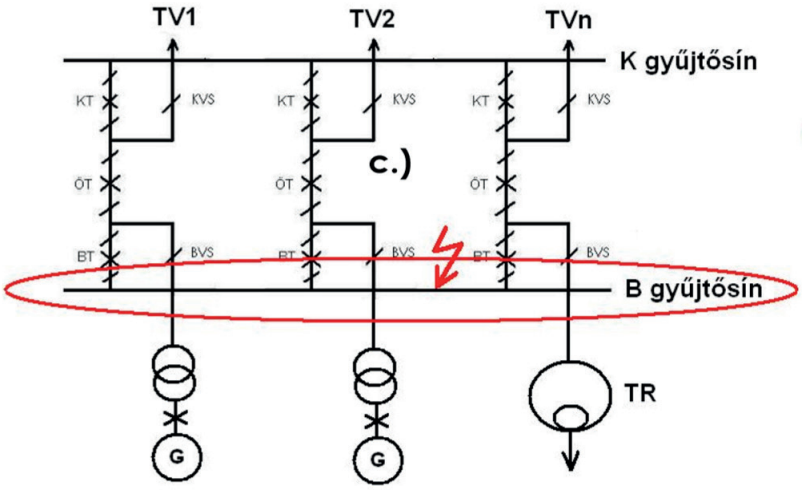
Főleg a magyar közép- és kisfeszültségű elosztóhálózat jelenét és jövőjét érintő körülmény az elosztott energiatermelés, tárolás, valamint az e-mobility *(elektromobilitás)* terjedése. A korábbi egyirányú energiaáramlás és jól tervezhető fogyasztás helyébe eshetőleges helyű és számú be- és kitápláló pontok közötti eshetőleges irányú és mennyiségű energiaáramok lépnek. Ezért, valamint a villamosenergia ellátás minőségi paramétereinek a tarthatósága érdekében a csatlakozási pontok megváltozó paramétereinek a hálózati hatásai esetileg mérlegelendők. Az elosztott technológiák terjedése idővel közép- és kisfeszültségű elosztóhálózati fejlesztéseket és megerősítéseket tehet szükségessé.

A korszerűbb kapcsolókészülékek révén a korábbi helyi, kézi működtetés helyébe középfeszültségen is egyre inkább a távműködtetés lép. Ennek, valamint a szenzortechnika fejlődésének köszönhetően középfeszültségen is jelentősen javulnak az esetleges üzemzavarok gyors és pontos észlelésének, majd a szolgáltatás helyreállításának a feltételei. Természetesen mindez fejlett digitális irányítástechnikát is feltételez.

### *4.4.3. A magyar alállomások*

A magyar átviteli hálózat csomópontjait 34 alállomás, a 120 kV-os elosztóhálózat csomópontjait pedig több, mint 250 alállomás alkotja[170]. Az átviteli hálózati alállomások közül számos az új építésű, a többi pedig rekonstrukción esett át, melynek keretében egyebek mellett korszerű digitális védelmeket és irányítástechnikát kaptak, melynek révén nagy tömegű távjelzés, távmérés és távműködtetés támogatja, hogy személyzet nélkül, távkezeléssel legyenek működtethetők. Ellátásbiztonsági szerepükre, a beépített nagy értékre, valamint a nagyfeszültségre tekintettel az alállomásokat fejlett vagyon- és tűzvédelmi rendszerek védik. Számos korszerű 120 kV-os elosztóhálózati alállomás is épült, ill. került korszerűsítésre, melynek nyomán szintén korszerű digitális védelmeket és irányítástechnikát kaptak.

A villamosenergia-ellátás biztonsága egyebek mellett az alállomások felépítésének, *topológiájának*[171] a függvénye. A magyar átviteli hálózati alállomások döntő többsége ún. *másfél-megszakítós* kialakítású, azaz a gyűjtősíneket összekötő mezőben két leágazást három megszakító szolgál ki.




*19. ábra: Másfél-megszakítós alállomási topológia*
*Forrás:* http://www.eszk.org/attachments/l49/ea/Nagy_rendszeruzemzavarok-restauralas_2010-03-18.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

[170] 2019. augusztusi állapot.

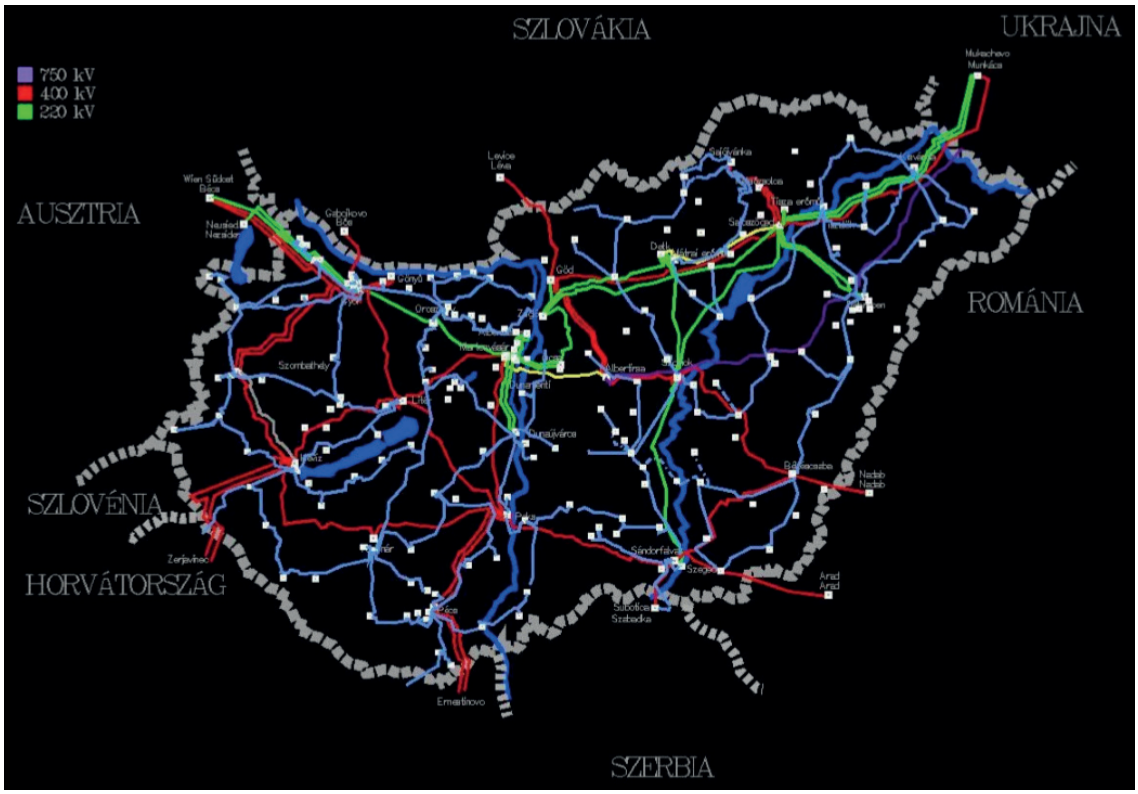
[171] Topológia: 1) helyekkel foglalkozó tudomány; hely meghatározása, bemutatása, 2) a számítógépek összekötésének kialakítása, 3) a matematikának a folytonossággal foglalkozó ága.

A másfél-megszakítós elrendezés tökéletesen megfelel az n-1 elvnek, hiszen pl. az egyik gyűjtősín zárlata esetén a másik gyűjtősínen, avagy a három közül az egyik megszakító hibája esetén a másik két megszakítón keresztül fenntartható az üzem.

A 120 kV-os elosztóhálózati alállomások topológiája igen változatos. Egy- és kétgyűjtősínes, két gyűjtősín plusz segédsínes, H és Π kapcsolású, egy- és többtranszformátoros egyaránt megtalálható.

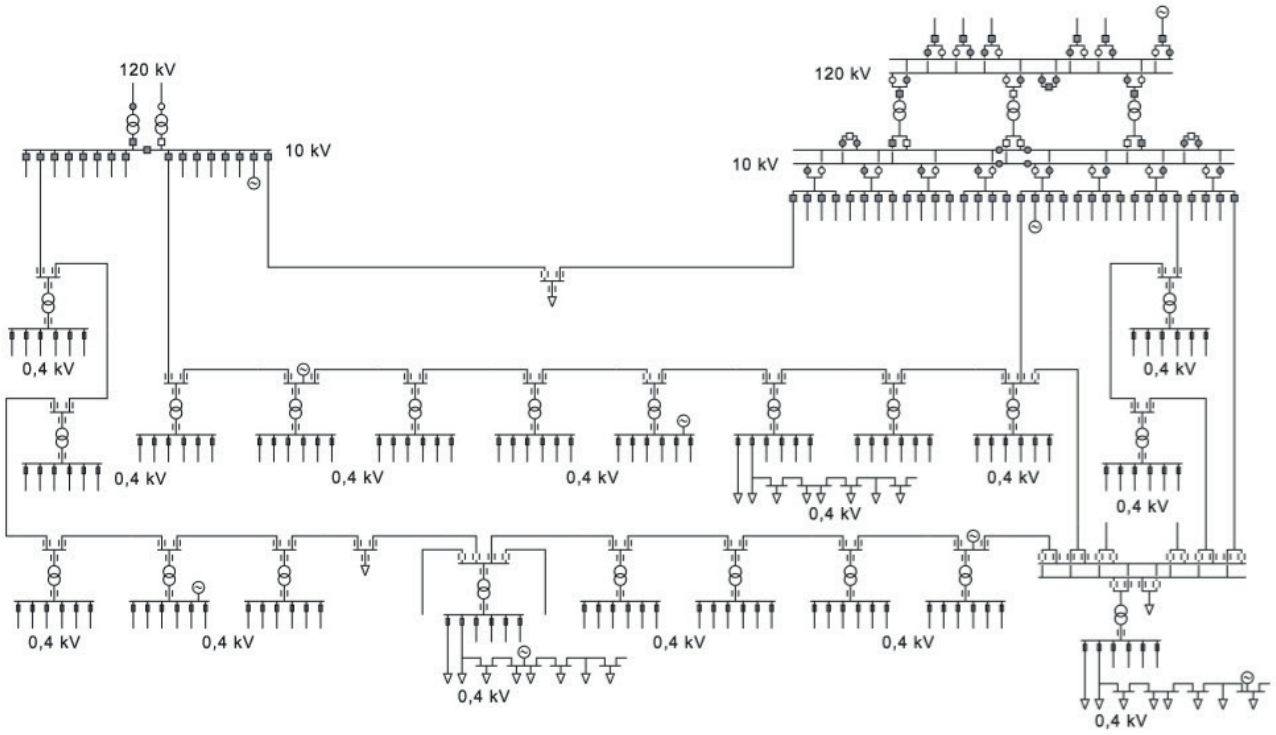
### *4.4.4. A magyar villamosenergia-hálózat*

Az erőművek, alállomások, távvezetékek – és persze az ezek üzemét felügyelő, az adatok átvitelét biztosító, stb. digitális rendszerek is – hálózatokat alkotnak. Az elosztóhálózati feszültségszinteken fölfelé haladva és eljutva az átviteli hálózatig az egyre magasabb üzembiztonsági elvárások miatt a hálózatok erősebben hurkoltak, egyre több redundanciát tartalmaznak.




*20. ábra: A magyar átviteli és 120 kV-os elosztóhálózat*
*Forrás:* http://www.eszk.org/attachments/l293/ea/Tihanyi_Zoltan_ESZK_20160505.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

Az ábra jól mutatja az átviteli és a 120 kV-os elosztóhálózat erős hurkoltságát. A redundáns alállomási és a távvezetéki topológia együttese hivatott biztosítani az áramutak magas rendelkezésre állását. A nagy-, közép- és kisfeszültségű hálózat topológiájára az alábbi ábra mutat példát.




*21. ábra: Középfeszültségű hálózat topológiája*
*Forrás:* ftp://ftp.energia.bme.hu/pub/Energiaellatas%20es%20-gazdalkodas%20-%20B/Nagyvarosi_villamos_halozatok_Eloadasabrak__2013_okt.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

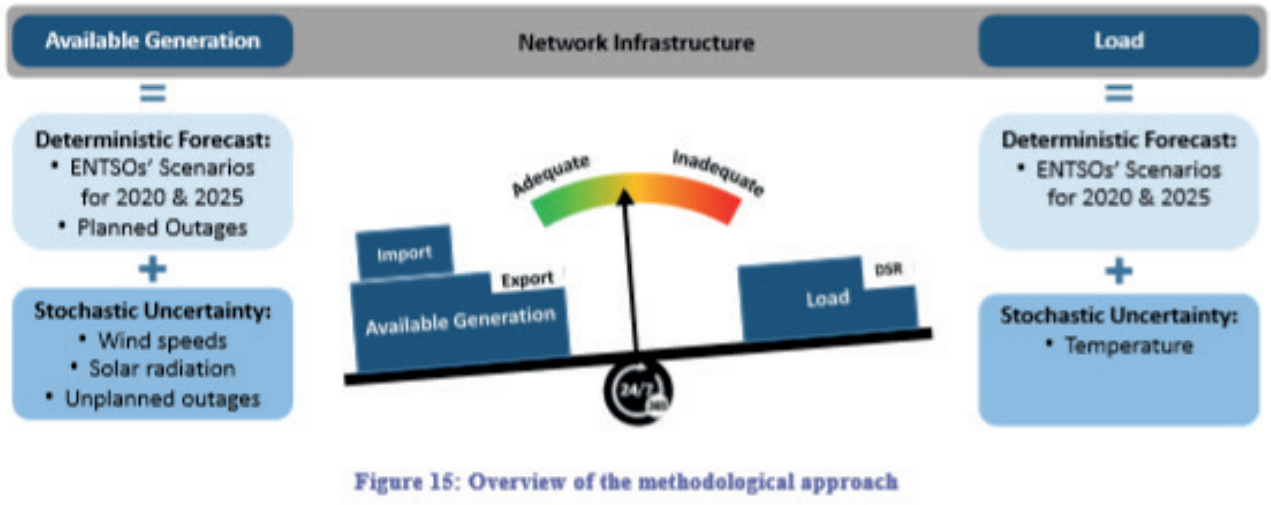
Míg az átviteli és a 120 kV-os elosztóhálózaton a redundancia inkább az alállomások közötti „pókhálószerű" közvetlen távvezetéki kapcsolatokon, addig középfeszültségen az egy-egy 120/középfeszültségű alállomás közötti ívekre (vagy ugyanabban a 120/középfeszültségű alállomásban záródó *gyűrűkre*) felfűzött közép/kisfeszültségű állomásokon keresztül valósul meg. Mind az íves, mind a gyűrűs topológia alkalmas arra, hogy egyszeres hiba (pl. valamelyik középfeszültségű távvezeték szakasz) kiesése ne okozzon tartós ellátási szünetet.

A redundáns hálózati topológia csak szükséges, de nem elégséges előfeltétel a magas rendelkezésre állású villamosenergia ellátáshoz, amely kizárólag a villamos erőművek, hálózatok, alállomások, stb. megfigyelhetőségét és irányíthatóságát biztosító digitális védelmi, automatika, irányítástechnika, méréstechnika, adatátviteli, stb. berendezések és rendszerek rendelkezésre állásával egyetemben értelmezhető.

A rendszerek szoros összefonódása miatt a villamosenergia-rendszer digitális alrendszerei bármelyikének az esetleges támadása magának a villamosenergia rendszernek támadását jelenti.

### *4.4.5. A magyar és az európai villamosenergia-rendszer kapcsolatai*

A villamosenergia-rendszer egyensúlyának, a villamosenergia tárolhatóságának, a termelés tervezhetőségének, stb. a problematikája természetesen európai szinten és hosszú távon is jelentkezik.




*22. ábra: Az ENTSO-E középtávú tervezési metodológiája*
*Forrás:* https://docstore.entsoe.eu/Documents/SDC%20documents/MAF/MAF_2017_report_for_consultation.pdf
*(Utolsó letöltés: 2019. augusztus 28.)*

A középtávú tervezésben mind a termelési, mind a fogyasztási oldalon vannak jól tervezhető és sztochasztikus összetevők. Nem meglepő módon az utóbbiak az időjárásból, a nem tervezhető blokk és távvezeték kiesésekből fakadnak. Ahogy a pl. a hálózat hurkolása, egy-egy főberendezés duplikálása, stb., azaz a beépített redundanciák mértékének a növelése egy-egy ország esetében növeli a villamosenergia-rendszer megbízhatóságát, úgy kontinentális léptékben a nemzeti villamosenergia-rendszerek lehető legtöbb ponton való összekötése teszi robosztussá az európai szintű rendszert. Ehhez Magyarország 17 db határkeresztező távvezetékkel járul hozzá (400 kV-on 13 db, 220 kV-on 4 db távvezetékkel).[172] A biztonsági szempont mellett Magyarország esetében ezeknek az elégtelen erőművi kapacitások miatt szükséges import lebonyolításában is nélkülözhetetlen szerepük van.

### *4.4.6. A magyar villamosenergia rendszerirányítás*

A hálózat korábban sorolt digitális rendszereken keresztül megvalósuló „megfigyelése" és „irányítása" a hierarchikusan felépülő rendszerirányítás feladata. Magyarországon az átviteli hálózat rendszerirányítását a MAVIR, az elosztóhálózatét a KDSZ-ek[173] végzik.

Rendszerirányítóként a MAVIR feladatai igen összetettek. Csak címszó szerűen a fontosabbak: a magyar villamosenergia-rendszer teljesítmény-egyensúlyának a fenntartása; az átviteli hálózatba tápláló erőművek irányítása; az átviteli hálózat üzemeltetése (pl. tervezése, fejlesztése, karbantartása, távkezelése); karbantartások, kikapcsolások tervezése, engedélyezése; folyamatos operatív kapcsolattartás külföldi rendszerirányítókkal; a villamosenergia-piac működtetése; szabályozási és üzemza-

[172] 2018. évi állapot.
[173] KDSZ: Körzeti Diszpécser Szolgálat

vari tartalék kapacitások beszerzése; folyamatos operatív kapcsolattartás KDSZ-ekkel; a rendszerirányítás számítógépes támogatásának üzemeltetése; stb. A KDSZ-ek a fenti feladatok többségét végzik, értelemszerűen a saját ellátási körzetük szerinti terjedelemben.

Mindennemű rendszerirányítói tevékenység elsődleges – hangsúlyosan a MAVIR-t terhelő – feladata a villamosenergia-rendszer egyensúlyának a fenntartása. Amennyiben a 4.2.4. pont szerint szabályozási mechanizmusok, avagy a 4.2.5. pont szerint FTK automatika sem képes biztosítani az egyensúly helyreállítását, akkor a rendszerirányító rendelkezésére álló további speciális eszköz a *rotációs kikapcsolási rend* (RKR). A villamos energia forrásoldal és a fogyasztás egyensúlyának jelentős megbomlása esetén működő automatikus vagy elrendelhető kikapcsolásokat az átviteli rendszerirányító, valamint az elosztó legfeljebb 6 órás időtartamra alkalmazhatja. Ennél hosszabb zavar esetén a vonatkozó rendelet[174] értelmében az átviteli rendszerirányító a fogyasztók kikapcsolására az RKR alkalmazását köteles elrendelni. Az RKR a villamosenergia-felhasználók különböző csoportjainak a villamos energia egyensúly megőrzése céljából a hiánnyal arányos, előre tervezett módon, különböző időben, az egyenlő elbánás és az indokolatlan megkülönböztetés tilalmának elvein történő kikapcsolását és a kikapcsolásának gyakoriságát meghatározó eljárás. Az RKR elrendelése esetén országosan 18, hozzávetőlegesen egyforma terhelési csoport felváltva, 3-3 órát meg nem haladó időtartamokban kerül kikapcsolásra, nem érintve az alapvető felhasználók[175] folyamatos ellátását.

A villamosenergia-rendszer egyensúlyi követelményének az elsődlegességéből egyebek mellett az is következik, hogy az ezt biztosítani hivatott rendszerirányítói infrastruktúra (pl. SCADA, távközlés) is rendelkezik redundanciával. A MAVIR rendelkezik olyan földrajzilag is elkülönített tartalék irányítási hellyel, ahonnan az elsődleges irányítási helyen való munka bármely okú ellehetetlenülése esetén fenn lehet tartani a rendszerirányítást. A fejlett hálózatos megoldások révén a KDSZ-ek is rendelkeznek tartalék irányítási hellyel.

### *4.4.7. A magyar villamosenergia-rendszer energetikai biztonsága*

Kiterjedt hálózati kapcsolatai révén általánosságban a magyar ellátás biztonsága azonos annak a villamosenergi-rendszeregyesülésnek (VERE) az ellátás biztonságával, amelyhez tartozik. Magyarország a rendszerváltás előtt a KGST[176] VERE része volt. A politikai változások előszeleként a ’80-as években létrejöttek az első – a szinkronjárás nélkül még csak egyenáramú átalakítással megvalósuló – hálózati kapcsolatok a KGST VERE és a nyugati országok villamosenergia rendszereit összefogó egyesülés, az UCPTE[177] között. A KGST felbomlása után hazánk, Lengyelország, Csehország és Szlovákia együttműködő rendszerei és a nyugat-európai együttműködő rendszerek szinkronjárása 1995-ben kezdődött. A nemzeti villamosenergia-rendszerek együttműködésének alapelvei szerint minden nemzeti rendszer felel a saját ellátásbiztonságáért, miközben minden nemzeti rendszer kölcsönösen segíti a másikat, de csak időlegesen. Az európai szintű együttműködés 2009 óta az ENTSO-E keretei között zajlik.

A nagy rendszerméret és az ENTSO-E együttműködés együttesen jelentősen növeli az ellátásbiztonságot. Ugyanakkor a nagyobb arányú megújuló alapú villamosenergia ellátás irányába több országban történő súlypont eltolódás biztonsági kérdéseket is felvet. Az egyre gyakoribb és akár több országot is sújtó szélsőséges időjárásnak (pl. az északi országokban is megjelenő hőhullámok-

[174] 280/2016. (IX. 21.) Korm. rendelet a villamosenergia-rendszer jelentős zavara és a villamosenergia-ellátási válsághelyzet esetén szükséges intézkedésekről

[175] Alapvető felhasználók: pl. gázfogadó és nyomásfokozó állomások, földgáztárolók, katasztrófavédelmi irányító központok, kijelölt üzemanyag töltőállomások, közszolgálati televízió- és rádió, kórházak, közforgalmi repülőtér, radioaktív hulladéktároló.

[176] KGST: Kölcsönös Gazdasági Segítség Tanácsa

[177] UCPTE: Union for the Coordination of Production and Transmission of Electricity.

nak), a roppant károkat okozó szélviharoknak, avagy a vízerőből való energiatermelést, de akár az (atom)erőművek hűtését is korlátozó aszályoknak ellátásbiztonsági kockázata, vagy akár konkrét hatása is lehet.

2018 nyarán a Paksi Atomerőműre vetült fokozott figyelem a Duna alacsony vízszintje és a kánikula miatt. Az atomerőmű hűtővízigényét kielégítő Duna hőmérséklete erősen megközelítette azt a határértéket, amelytől termelési korlátozásokat kellett volna életbe léptetni. A magyar villamosenergia rendszer meghatározó, teljes üzeme esetén 2000 MW teljesítménnyel termelő alaperőművéről lévén szó a korlátozásnak súlyos következménye lehetett volna.

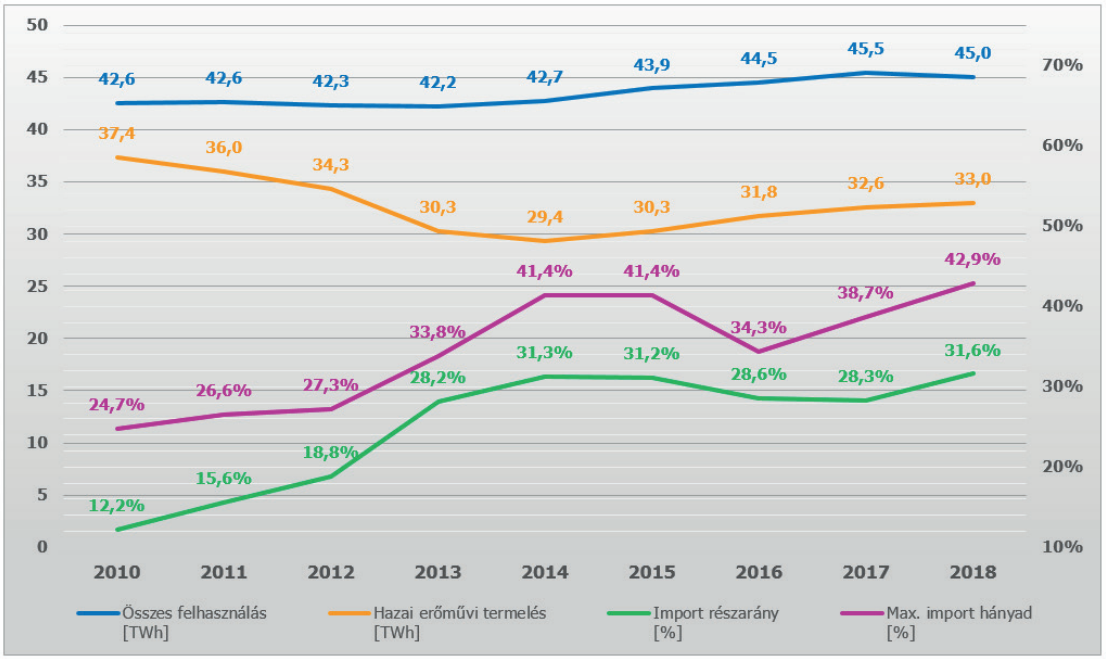
A szélsőséges időjárás Magyarországon további ellátásbiztonsági kockázatokat is felvet. Pl. tartós és kemény fagy esetén több esetben is befagytak a Mátrai Erőmű, mint a Paks utáni második legnagyobb alaperőmű lignittárolói, megakadályozva a fűtőanyag utánpótlást, az erőmű termelésének kényszerű korlátozását okozva. Pl. 2017. január közepén Európában nagy hideg volt, mely miatt a német széltermelés is drasztikusan visszaesett. A Mátrai Erőműben a lignit összefagyott, az erőmű termelése jelentősen csökkent. Ráadásul meghibásodott a Dunamenti és a Bakonyi Erőmű egy-egy blokkja, a Gönyűi Erőműben pedig előre tervezett leállás volt. Önmagában a mátrai és dunamenti kiesések együttesen elérték az 1000 MW-ot. A kényszerű pótlás kapcsán a határkeresztező távvezetékek teljes kapacitással üzemeltek. Ugyanakkor ugyanezen időszakban a külföldi termelés visszaesése, ezzel a villamosenergia árának a jelentős emelkedése miatt a pótlás rendkívül drága volt. A szélsőséges időjárás miatti villamosenergia-ellátási zavarok emlékezetes példája volt a 4.4.2. pontban részleteiben ismertetett 2013. március 14-én kezdődött erős lehűlés, havazás, ónos eső és szélvihar miatti kiterjedt fogyasztói ellátatlanság is.

A magyar villamosenergia rendszer import kitettsége az esetleges erőművi forráshiányok pótlásán kívül is jelentős. Pl. 2017-ben az ENTSO-E 34 tagországából importáló 20 ország közül Magyarország villamosenergia import-export szaldója volt a 4. legnagyobb (Olaszország, Finnország és Nagy-Britannia után).

Ráadásul ahogy a 22. ábra mutatja, az import kitettség – a 2015-2017 időszak részbeni stagnálásától, ill. csökkenésétől eltekintve – jellemzően évről-évre nő.[178] Nagyjából ezt a tendenciát mutatják a maximum import hányadok is. A vizsgált időszakban a villamosenergia felhasználás csak mérsékelten nőtt, így a növekvő import részarány oka inkább a rendelkezésre álló hazai erőművi teljesítőképesség jelentős leépülése (a 2011. évi mintegy 9100 MW-ről 2016-ra 7000 MW-ra)[179].

[178] Ennek egyik oka, hogy a villamosenergia-fogyasztás szinte évről évre új rekordokat dönt. (Forrás: https://www.origo.hu/itthon/20190109-sorra-megdolnek-a-hazai-villamosenergiafogyasztasi-rekordok.html)

[179] http://www.mekh.hu/download/e/99/60000/a_magyar_villamosenergia_rendszer_2017_evi_adatai.pdf (Utolsó letöltés: 2019. augusztus 28.)




*23. ábra: A magyar villamosenergia-rendszer import-export energia szaldó részarányok Szerkesztette a szerző.* [180]

A 4.4.1. pontban írtak alapján a Paks II. Atomerőmű blokkjainak a belépése ezt a helyzetet csak átmenetileg fogja orvosolni, azaz elkerülhetetlenek a további erőművi beruházások.

Az ENTSO-E tagság jelentős biztonságot ad a magyar villamosenergia-rendszernek. Ugyanakkor a) a hazai erőművi kapacitás csökkenése, b) a jól szabályozható termelő kapacitások szükségesnél kisebb mennyisége, ezekből következően c) a jelentős villamosenergia-import kitettség, d) az időjárásfüggő megújuló alapú energiatermelés, valamint e) a villamosenergia-rendszer irányításának, védelmének, stb. egyre nagyobb mértékű digitalizáltsága – ezzel hekkerek általi támadhatósága – növekvő kockázatot jelent. Különösen olyan esetben, ha pl. valamely nagy kiterjedésű időjárási szélsőség miatt Magyarország mellett több más ország villamosenergia-rendszerében is lecsökkennek a tartalékok, a mozgósítható kapacitások. Amennyiben pl. korábban végrehajtott social engineering[181] révén a támadó már támadási helyzetben van, akkor idővel adódhat olyan időpillanat, amikor az az ellátásbiztonságot is érintően kihasználhatja a villamosenergia-rendszer sérülékenységét.

[180] A felhasznált források
https://www.mavir.hu/web/mavir/import-export-energia-szaldo-reszaranya
http://www.mekh.hu/download/e/99/60000/a_magyar_villamosenergia_rendszer_2017_evi_adatai.pdf
http://mavir.hu/web/mavir/reszletes-havi-brutto-energi-adatok
http://mavir.hu/documents/10258/45985073/MAVIR_VER_2017_web_2.pdf/599179f4-d263-f4d0-b65d-3dd04acbc352 8. o. (Utolsó letöltések: 2019. augusztus 28.)

[181] Social engineering: támadási forma, amelyben a támadó megtévesztéssel vesz rá ismerettel, jogosultsággal rendelkező személyt hozzáférési információ átadására, vagy a rendszerhez való illetéktelen személy általi hozzáférés lehetővé tételére.

# 5. DR. DANYEK MIKLÓS: A VILLAMOSENERGIA-SZEKTOR MINT KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA

## 5.1. Bevezető gondolatok

A következő fejezetben csak a közép- és nagyfeszültségű (> 1 kV) villamosenergia rendszer védelmi és irányítástechnikai rendszerével foglalkozunk, a kisfeszültségű rendszereket a [182] jegyzet 4. alfejezete ismerteti.

## 5.2. A villamosenergia-rendszer irányítástechnikai rendszerei

*A villamosenergia-rendszert – hasonlóan más műszaki rendszerekhez – felügyelni szükséges az üzembiztos, gazdaságos és folyamatos működéséhez. Az ehhez használt mérő, adatgyűjtő, beavatkozó elemekből felépülő rendszert a villamosenergia-rendszer irányítástechnikájának nevezzük. Az alállomásokon, erőművekben lévő az energiairányok kijelölésére használt nagyfeszültségű (>1 kV) eszközöket kapcsolókészülékeknek nevezzük (szakaszolók, megszakítók, földelőszakaszolók)*. A villamosenergia hálózat felügyeletéhez ezeknek a kapcsolóelemeknek az állapotát (pl. kint, bent, üzemkész, meghibásodott) valós időben ismernünk kell, valamint távolról beavatkozást kell rajta végeznünk (pl. ki/be kapcsolás). A villamosenergia-áramlás felügyeletéhez – az előbb említetthez hasonlóan online – mérni kell számos helyen (főleg a csomópontokban) a villamosenergia jellemzőit (feszültség, áram, frekvencia). A kapcsolóelemek és a mért jellemzők ismeretében lehet a villamosenergia áramlását (termelő -> fogyasztó) irányítani és a fogyasztás – termelés egyensúlyát fenntartani (lásd. [183] jegyzet 4.2.2. ábrája) és olyan üzemállapotok irányába terelni a villamosenergia rendszert, hogy az energiaveszteséget minimalizálhassuk, amely együtt jár a költségek csökkentésével és a környezet kisebb mértékű szennyezésével és terhelésével.

A nagyfeszültségű kapcsoló készülékeknek (megszakító, szakaszoló, földelőszakaszoló) és készülékeknek (pl. transzformátor, generátor) két részét különböztetjük meg:

- *primer rész: a villamosenergia szállítását végző / biztosító elemek összessége, amelynek a feszültségszintje 1 kV vagy annál nagyobb*
- *szekunder rész: a primer rész működtetését, állapotfelügyeletét, mérését biztosító elemek összessége, amelynek a feszültségszintje kisebb, mint 400 V.*

---

[182] „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

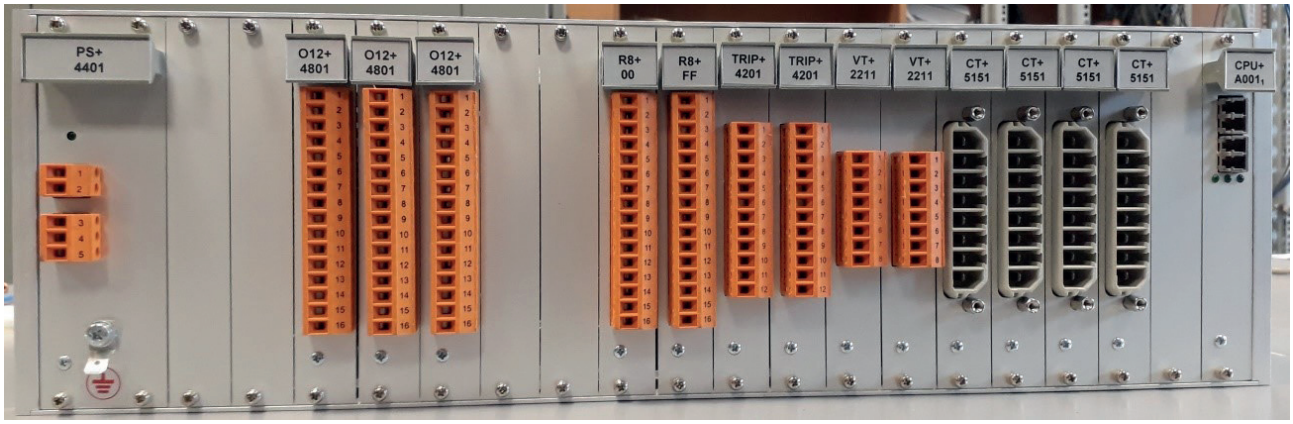
[183] „Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme” című jegyzet

## *5.2.1. Az irányítástechnikai rendszer elemei*

Annak függvényében, hogy milyen funkciót lát el az irányítástechnikai rendszerben egy-egy elem, illetve hol helyezkedik el, különböző részegységekről beszélünk. Vannak - az előző fejezetben ismertetett – kapcsolókészülékekhez illetve mérő elemekhez közvetlenül csatlakozó eszközök, az ezektől gyűjtött információkat feldolgozó elemek, valamint az irányító személyzet számára a szűrt/teljes információszerzést és beavatkozást biztosító HMI[184]-k. Az alábbiakban ezek az elemek kerülnek ismertetésre.

### 5.2.1.1. Mezőgép

*Az állapotismereti és mérési funkciókat úgy lehet biztosítani, hogy adatgyűjtőket/végrehajtókat – összefoglaló nevükön mezőgépeket - telepítünk a szükséges pontjaira a villamosenergia hálózatnak.* Ezek a helyszínek: alállomások, erőművek illetve bizonyos feszültségszinteken (jellemzően 20 kV) szabadvezetékeknél a távvezérelhető oszlopkapcsolók. A mezőgépek tipikus felépítésére mutat példát az 1. ábra.




*1. ábra - Adatgyűjtő mezőgép felépítése*

A mezőgépek feladata, hogy a nagyfeszültségű kapcsolókészülékektől (megszakító, szakaszoló, földelőszakaszoló), készülékektől (pl. transzformátor, generátor) kapott – szekunder köri - erősáramú (12V, 24V, 48V, 230 V DC[185] vagy AC[186]) állás- és állapotjelzéseket illetve az áramváltóktól[187] vagy feszültségváltóktól[188] kapott mért értékeket összegyűjtsék és átalakítsák adatgyűjtésre alkalmas digitális (0/1) jelekké. Ezen felül a távvezérelhető nagyfeszültségű (> 1kV) kapcsolóelemeket - az előbb említett 12V, 24V, 48V, 230 V DC vagy AC - szekunder köri - feszültségszinteken vezérelniük kell annak érdekében, hogy a villamosenergia rendszert irányítani tudjuk. Ez a vezérlés hasonló az otthoni villanykapcsolóhoz, csak ebben az esetben a kapcsolt feszültség 1000 ÷ 750.000 V-ig terjed, a kapcsolást pedig nem a kezünkkel, hanem az előbb említett szekunder köri feszültséggel végezzük a legtöbb esetben jelentős távolságról (>10 km) valamelyik villamosenergia irányító központból (lásd. 5.2.2. fejezet).

A mezőgépek minden esetben külön, független tápfeszültséget (12V, 24V, 48V, 230 V DC vagy AC) igényelnek attól, amellyel vezérlik/érzékelik az általuk felügyelt kapcsolókészülékeket. Cserélhető/bővíthet modulos (amit kártyának nevezünk) rendszerűek, felépítésük pedig attól függ, hogy

184 HMI = Human Machine Interface = ember – gép kapcsolati eszköz

185 DC = Direct Current = egyenáram

186 AC = Alternate Current = váltakozó áram

187 Áramváltó = A nagyfeszültségű készüléken/távvezetéken folyó áram mezőgépbe/védelembe csatlakoztatható értékűre csökkentését és biztonságos potenciál leválasztását biztosító mérőkészülék.

188 Feszültségváltó = A nagyfeszültségű készülék/távvezeték feszültség értékét (750.000 ÷ 500 V) mezőgépbe/védelembe csatlakoztatható értékűre (< 300 V) csökkentését és biztonságos potenciál leválasztását biztosító mérőkészülék.

milyen készülékeket kell felügyelniük. A beépíthető kártyák lehetnek: tápellátást biztosító, adatfeldolgozó (processzor), kommunikációs, bemeneti (input), kimeneti (output) és mérőkártyák. Annak függvényében, hogy melyik gyártó készíti az adott mezőgépet ezek kombinációját is alkalmazni szokták (pl. integrált adatfeldolgozó és kommunikációs kártya). A mezőgépek buszos kivitelűek (így lehetséges a modularitás biztosítása), amely – jellemzően - gyártófüggő kialakítású, így más gyártó kártyája nem helyezhető be ugyan abba a mezőgépbe. Minden kártyának szüksége van tápfeszültségre és egy kommunikációs irányra, amely - a legtöbb esetben - manapság Ethernet alapú, ezeket biztosítja a belső buszrendszer. A buszrendszer azt az adatcsere elvet jelenti, hogy az adott kártyáról (buszmegálló 1.) érkező adat felszáll az adatátviteli csatornára (buszjárat) és leszáll a célállomását jelentő kártyán (buszmegálló 2.). A busz kapacitása (utasszám) elegendő arra, hogy egyszerre többen (nagy számban) utazhassanak adatok (utas) rajta.

A mezőgépek külső kommunikációja (más mezőgépek, adatkoncentrátorok irányába lásd. 5.3. fejezet) Ethernet[189] alapú TCP/IP[190] protokollon történik, réz vagy optikai szálas fizikai közegen. Régebbi technológiák esetében (<2005) egyedi gyártófüggő protokollok kerültek alkalmazásra. Ilyen mezőgépek beépítve még számos helyen előfordulnak, mivel a korszerűsítések, cserék tulajdonosi szemléleti, finanszírozási vagy üzemeltetési okból nem vagy csak részlegesen történtek(nek) meg. A korábban és a jelenleg alkalmazott kommunikációs hálózatokkal/protokollokkal részletesen az 5.4. fejezet foglalkozik.

A mezőgépeknek el kell látniuk az általuk felügyelt készülékek adatgyűjtését és vezérlését is – szűkebb funkcionalitással – akkor is, ha a külső kommunikációjuk megszakad. Ebben az esetben a nem saját információk hiányában csak olyan mértékű felügyeletet tud a mezőgép ellátni, amely a saját információkból megoldható. Amennyiben egy automatika (lásd. 5.2. fejezet) van beleprogramozva, akkor autonóm módon végzi ezt, vagy a saját – általában érintőképernyős – megjelenítő felületén keresztül lehet emberi beavatkozással (kézzel) irányítani. Ez utóbbi felület a mezőgép saját HMI-je, amelyen a megjelenített információk annak függvényében változnak, hogy milyen kapcsolókészülékeket/készülékeket felügyel. Kommunikáció megszakadás nélkül ezen HMI kezelési jogosultságát (ki és honnan kapcsolhatja az adott készülékeket) a rendszerirányítás során alkalmazott kezelési jogosultsági rendszer határozza meg, amely biztosítja, hogy egy kapcsolóelemet egyszerre csak egy helyről lehessen irányítani a téves működtetések kizárása végett (lásd. 5.2.2.4. fejezet).

### 5.2.1.2. Fejgép (RTU)

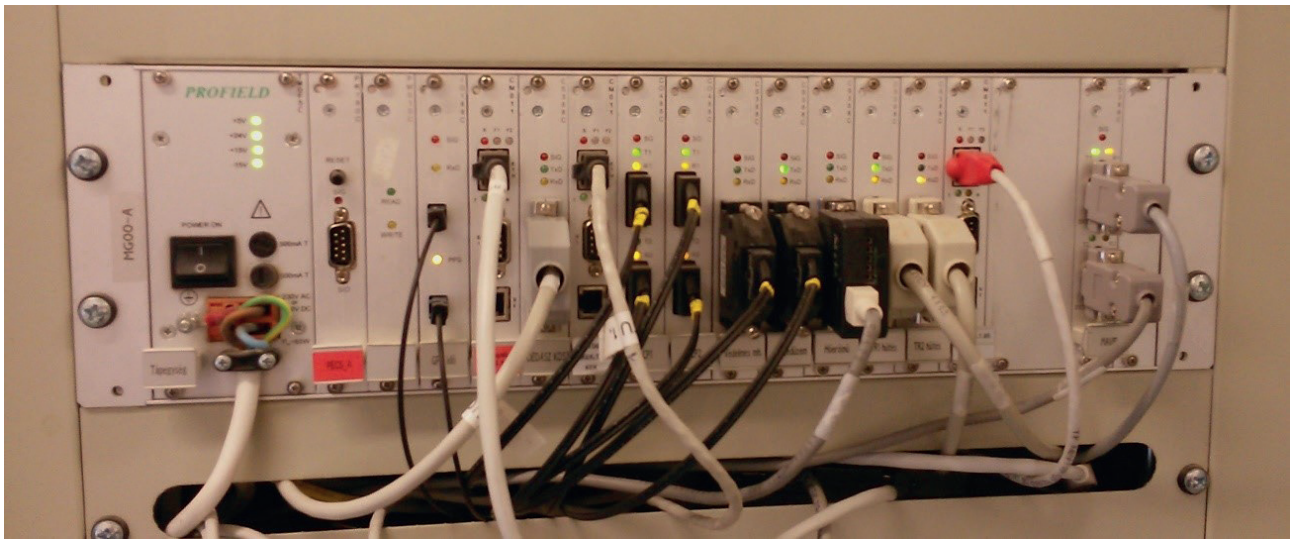
*Minden villamosenergetikai csomópontban (erőmű, alállomás) szükség van egy olyan eszközre, ami az itt elhelyezett mezőgépek adatait összegyűjti, futtatja azokat az automatika funkciókat, amelyeket a mezőgépek magukban nem képesek megtenni, illetve kiszolgálja a további (alállomáson kívüli) kommunikációs irányokat. Ezt az eszközt nevezzük fejgépnek (RTU[191], vagy amennyiben duplikálva van akkor duál[192] fejgépeknek)*. A fejgépek felépítésére mutat példát a 2. ábra.

[189] Ethernet = A DEC, Intel és 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. Hasonló az IEEE 802.3 szabványhoz. www.wikipedia.org

[190] 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. https://www.ipcomm.de/protocols_en.html

[191] RTU = Remote Terminal Unit, itt fejgép

[192] Duál fejgép = azonos funkciót ellátó, de fizikailag különálló fejgépek, amelyek tartalékai egymásnak. Céljuk az üzembiztonság/rendelkezése állás növelése.




*2. ábra – Fejgép felépítése*

A fejgépek minden esetben saját külön (független) tápfeszültséget igényelnek (12V, 24V, 48V, 230 V DC vagy AC), cserélhető/bővíthet modulos (amit kártyának nevezünk) rendszerűek, felépítésük attól függ, milyen kommunikációs irányokat kell biztosítaniuk. A beépíthető kártyák lehetnek: tápellátást biztosító, adatfeldolgozó (processzor) és kommunikációs. Gyártótól függően ezek kombinációja is előfordulhat (pl. integrált adatfeldolgozó és kommunikációs kártya). A fejgépek belső buszos kivitelűek (így lehetséges a modularitás biztosítása), amely gyártófüggő kialakítású. Minden kártyának szüksége van tápfeszültségre és egy belső kommunikációs irányra, amely manapság – a legtöbb esetben – Ethernet alapú. Ezeket biztosítja a belső buszrendszer, hasonlóan a mezőgépekhez. Létezik olyan gyártó is, akinek a fejgépe ki- és bementi kártyákat is tud fogadni, ebben az esetben hibrid mezőgép/fejgép készülékről beszélünk.

A fejgépek külső kommunikációja réz vagy optikai szálas fizikai közegen keresztül történik. Egyre gyakoribb a teljesen Ethernet alapú TCP/IP protokollt alkalmazó kivitel, de nem kizárólagos. A felügyelt mezőgépek típusától, gyártójától, gyártási idejétől függően különböző protokolloknak megfelelően gyűjtik az adatokat és továbbítják a vezérléseket (lásd. részletesebben az 5.4. fejezetben). A fejgépben annak függvényében, hogy kapják vagy adják a vezérléseket megkülönböztetünk alsó (slave)[193] és felső (master)[194] irányokat. Jellemzően a mezőgépek alsó iránynak minősülnek, a külső kommunikációs irányok pedig felső iránynak. Elő szokott fordulni olyan eset duál fejgépek alkalmazása során, hogy a csatlakoztatott slave nem képes egyszerre két master-t kiszolgálni, ezért egy bővítő fejgépet iktatunk be, amely fogadja ezt az egy irányt és osztja ketté a duál fejgépek számára. Ez a korlát lehet fizikai (pl. IEC 60870-5-101 protokoll = pont – pont soros kommunikációs irány) vagy szoftveres (pl. csak egy master klienst programozott be a slave készülék gyártója). Jogosan merül fel a kérdés, hogy miért nem lehet átalakítani a nem megfelelő slave irányt. Az esetek túlnyomó részében meglévő rendszereket kell bővíteni, átalakítani úgy, hogy a környező (korábban már csatlakoztatott irányok) változatlanok és nem lehet változtatni rajtuk, mert más tulajdonában vannak vagy nem része az adott munkának.

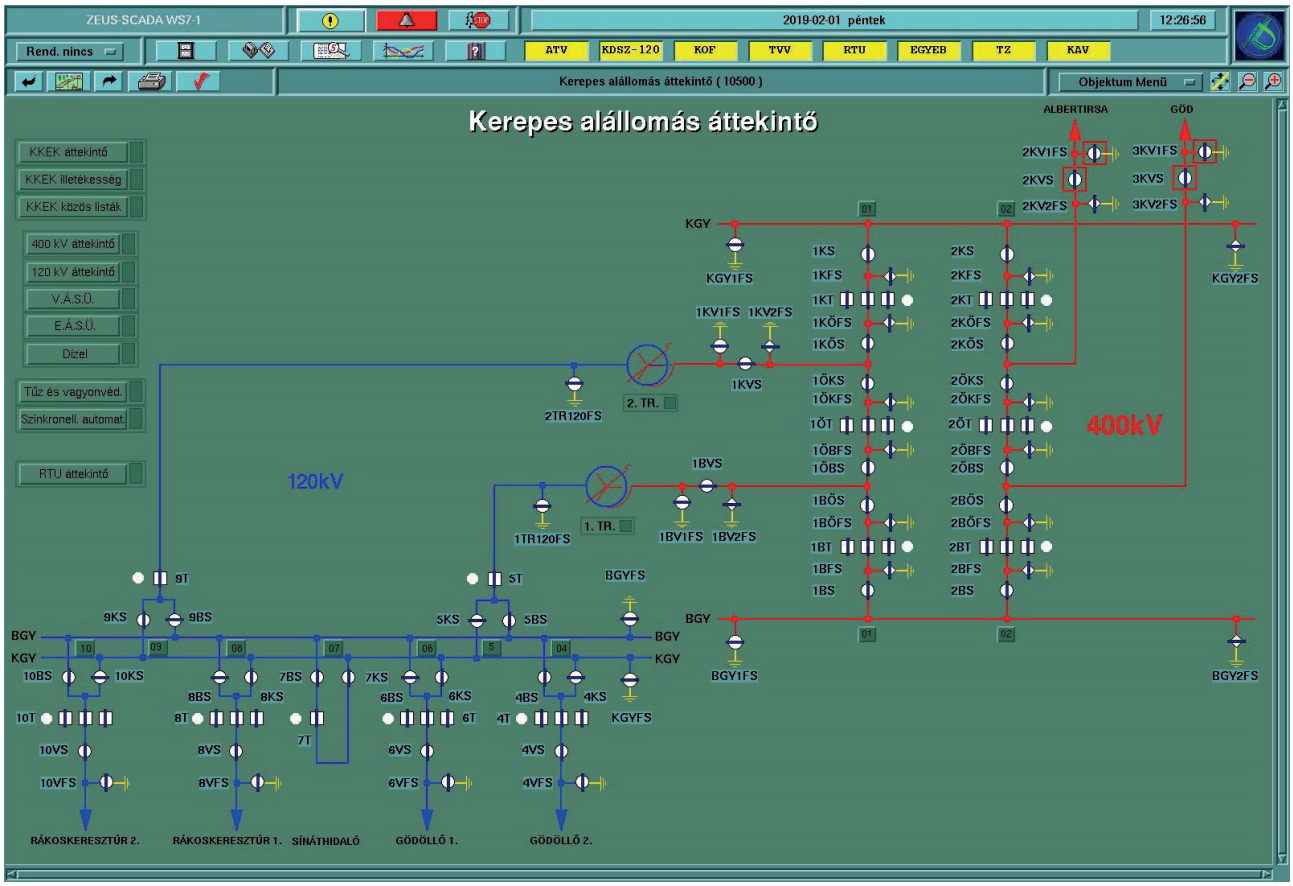
A fejgépek szolgálják ki azokat a külső kommunikációs irányokat, amelyek vagy a csatlakozó távvezetékek túlsó végére biztosítandó információadás vagy nemzetközi egyezmények vagy a központi rendszerirányítás miatt szükségesek. Ezek jellemzően: Áramszolgáltató (ÁSZ), tisztán villamos vagy kapcsolt villamos- és hőerőmű, MAgyar VIllamos Rendszerirányító (MAVIR), nagyobb ipari fogyasztó (pl. ipari/termelő üzem/gyár, vízmű, szennyvíz átemelő telep, olajfinomító, gázellátó te-

[193] Slave = kiszolgáló, szerver irány ebben az estben
[194] Master = fogadó, kliens irány ebben az esetben

lep), ENSTO-E[195] központ. Annak függvényében, hogy az előbb említett partnerek milyet preferálnak a fizikai átviteli közeg és a protokoll (lásd. részletesen az 5.4. fejezetben) is változik, amiből az következik, hogy a fejgépnek protokoll konverter (gateway)[196] funkciót is el kell látnia.

### 5.2.1.3. HAM (Helyi Alállomási Megjelenítő)

A fejgépek egyik feladata, hogy az alállomáson/erőműben a központi felügyeletet biztosító HAM[197]-ot kiszolgálja a mezőgépektől gyűjtött és feldolgozott adatokkal. Egy tipikus HAM képet mutat a 3. ábra.




*3. ábra – Tipikus nagyfeszültségű alállomási HAM kép*

*A HAM feladata, hogy a helyszínre kiérkező (vagy folyamatosan ott tartózkodó) szakemberek számára gyorsan és könnyen áttekinthető képet adjon az alállomás/erőmű helyzetéről, állapotáról. Ebbe beleértendő teljes körűen az alállomás vagy erőmű nagy- és kisfeszültségű villamos rendszerének állapota, a fő és kiszolgáló berendezések mérési értékei, kapcsolási képe, eseménylistája (event list vagy log). Gyakori még, hogy – az üzemeltető kérésére – a terület vagyonvédelmi és tűzjelző berendezéseinek (szűkített körű) jelzéseit is meg kell jeleníteni a HAM-on.*

Erőművi vagy egyéb olyan helyszínen, ahol egy alállomáson belül több tulajdonos is van (pl. MÁV[198] / ÁSZ közös alállomás) a másik tulajdonoshoz tartozó kapcsolókészülékek/mérőváltók[199]

[195] ENTSO-E = European Network of Transmission System Operators for Electricity

[196] Gateway = átjáró, konverter eszköz, különböző protokollon kommunikáló eszközök között

[197] HAM = Helyi Alállomási Megjelenítő = az alállomáson lévő komplex HMI, amely a helyben kezelt villamos berendezések teljes körű felügyeletére alkalmas

[198] MÁV = Magyar ÁllamVasutak

[199] mérőváltó = áram- és/vagy feszültségváltó

egy részét és mérési értékeit, (vagy amennyiben a rendszerirányítás miatt szükséges) vezérlését is integrálni kell a megjelenítőre. Ebben az esetben egyértelműsíteni kell (általában üzemviteli megállapodás keretében), hogy ki az adott nagyfeszültségű rész/kapcsolókészülék üzemeltetője, kinek van joga vele kapcsolni vagy átadhatóvá kell tenni a kapcsolási jogot a felek között. Ez utóbbi megvalósítása történhet szoftveres (HAM-on keresztül végzett) vagy erősáramú megoldással (fizikai kapcsolóval), azonban mindkét esetben egyértelmű visszajelzés és reteszelés (= működtetés letiltás) szükséges mindkét fél részére.

Gyakori, hogy online eseménynaplót (log fájlt) és annak archiválását illetve egyszerűbb SCADA[200] funkciókat is integrálnak a HAM-ra (pl. mérési értékekből trend rajzolása és archiválása). A trendeknek, log fájloknak, kapcsolási eseményeknek visszanézhetőnek kell lenniük, olyan szempontból is, hogy az adott kapcsolóelemet (kapcsolókészüléket) ki és mikor működtette milyen jogosultsággal és melyik helyszínről. Ennek egy utólagos üzemzavar elemzés / hibakeresés / felelősség megállapítás esetén kulcsfontosságú a jelentősége.

Mivel a HAM-ról teljes körűen felügyelhetők és kapcsolhatók a felügyelt területen lévő és a villamosenergia rendszer részét képező készülékek, így a HAM kezelési jogosultságát is (ki és honnan kapcsolhatja az adott készülékeket) a rendszerirányítás során alkalmazott kezelési jogosultsági rendszer határozza meg.

## *5.2.2. Villamosenergia irányító központok*

Mivel Magyarországon a villamosenergia rendszerben - szinte kizárólag - csak állandó személyzet nélküli alállomások vannak, ezért szükséges ezek teljes körű távoli felügyelete és üzemirányítása. Ezt a feladatot a KDSZ[201]-ek és a MAVIR közösen végzi. Utóbbi feladata ezen felül, hogy a villamosenergia rendszerben a (a még nem megoldott nagy mennyiségű és gazdaságos tárolhatóság miatt szükséges) kereslet – kínálat egyensúly fennálljon, ahogyan a [202] jegyzet IV. fejezet is bemutatja.

### 5.2.2.1. Körzeti Diszpécser Szolgálat (KDSZ)

A KDSZ-ek az áramszolgáltatókhoz tartoznak és regionális elhelyezkedésűek, feladatuk a 120 kV-os és az alatti névleges feszültségű távvezetékek és alállomások felügyelete és üzemirányítása. Minden egyes alállomással, amely hozzájuk tartozik legalább egyszeres, folyamatos adatkapcsolatuk van, amely a távközlési hálózat kialakításából adódóan kvázi redundánsak tekinthető (részletesebben lásd. az 5.4.4. fejezetben). Ezek az adatkapcsolatok szerverekben végződnek, amelyekre a KDSZ-ben dolgozó operátorok HMI-jei rácsatlakoznak, és innen irányítják a hozzájuk rendelt körzeteket. Ugyan ezekre az adatszerverekre csatlakoznak az adatfeldolgozást és a SCADA funkciókat végző szerverek, amelyek gyakran már virtuálisak és felhő alapú megoldásokat használnak. A szerverek maguk is redundánsak. Ezen felül az adatközpontoknak egy földrajzilag külön álló helyen teljes körű tartalék is ki van alakítva az alábbi módon: a hat áramszolgáltatói terület[203] mindegyike rendelkezik legalább egy-egy saját adatközponttal, amelyek egymás tartalékaiként is funkcionálnak. Minden azonos

---

200 SCADA = Supervisory Control and Data Acquisition = adatgyűjtő, elemző és irányító rendszer (itt villamosenergia rendszerre vonatkoztatva)

201 KDSZ = Körzeti Diszpécser Szolgálat = Az ÁSZ-ok által használt kezelőközpont a 120 kV-os és annál kisebb névleges feszültségű rendszerekhez

202 „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

203 ÉDÁSZ = Észak Dunántúli Áramszolgáltató, DÉDÁSZ = Dél Dunántúli Áramszolgáltató, ELMŰ = Elektromos Művek, ÉMÁSZ = Észak Magyarországi Áramszolgáltató, DÉMÁSZ = Dél Magyarországi Áramszolgáltató = NKM Áramhálózati Kft, TITÁSZ = Tiszántúli Áramszolgáltató

tulajdonban lévő áramszolgáltató (ELMŰ-ÉMÁSZ, E.ON, NKM) minden KDSZ-e teljes körűen át tudja venni egymás szerepét egy tulajdonosi körön belül. A földrajzilag elhatárolt ÁSZ-ok esetében mindegyik KDSZ a saját körzetét kezeli alapból, de megoldott minden területnek a másik helyszínről való kezelése is, mind technológiai (HMI), mind humán erőforrás szempontjából. Ez utóbbi azt jelenti, hogy az operátorok folyamatos képzésével és vizsgáztatásával biztosított a nem saját KDSZ körzetben lévő villamosenergia rendszer felügyelete (pl. Dél-Dunántúli KDSZ-ből a Tiszántúli régió felügyelete). Az ÁSZ-ok folyamatosan arra törekszenek, hogy mind a humán, mind az IT állományukat fejlesszék, korszerűsítsék és egyre költséghatékonyabbak legyenek a biztonsági előírások betartásának figyelembe vételével.

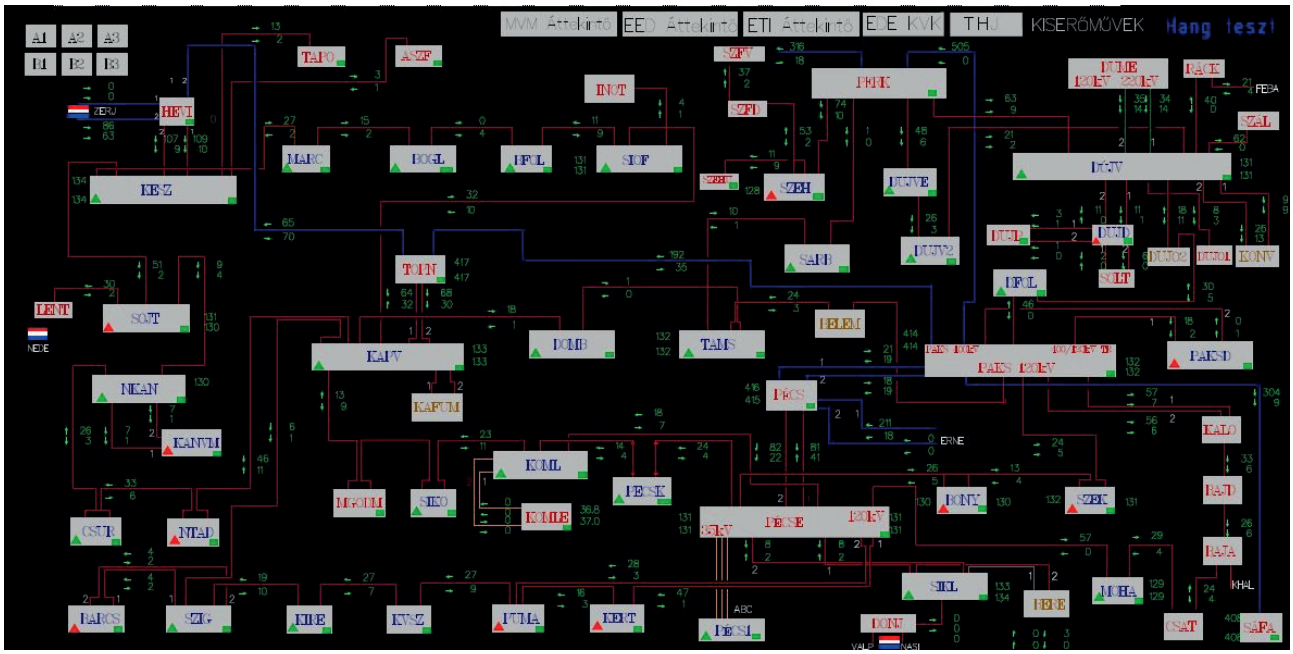
A SCADA és EMS[204] rendszerek közül a leggyakrabban használt a Siemens gyártmányú - nemzetközi termékként elérhető – Spektrum rendszer. Ez egy komplex szoftver melynek testreszabása minden egyes ÁSZ esetében a saját igényekhez történik, valamint a folyamatos terméktámogatása nemzetközi szinten megoldott.

A KDSZ-ek (mivel pl. az ELMŰ-ÉMÁSZ által felügyelt 20 kV-os hálózat több ezer km hosszúságú) felhasználják a térinformatikai eszközöket (pl. = GIS[205]) - amelyre alapulva a középfeszültségű hálózatot térképre vetítve tudják megjeleníteni az üzemeltető operátoroknál használt HMI-ken – a pontosabb és minél gyorsabb hibabehatárolás, kapcsolási helyszín behatároláshoz. A rendszer hatékony működése elsősorban a GIS és az üzemeltetetett hálózat adatbázisának folyamatos frissítésén, pontosságán és összehangolásán múlik, amelyet minden érintett ÁSZ saját hatáskörben végez el.

A 20 és a 0,4 kV-os hálózatok felügyeletét korábban az ÜIK[206] látták el (kijáró szakemberek vezénylése stb.), de ezek manapság (irányítástechnikai szempontból) integrálódtak a KDSZ-be. A KDSZ-es operátorok számára - az előbb említett térinformatikai rendszerbe integrálva – a szolgálati autókban lévő GPS jeladók is megjelennek, így pontosan látják, hogy melyik helyszínen vannak a kijáró szakemberek ezzel is csökkentve a hibaelhárítás idejét és az élőmunkaidő igényt.

A korszerű technológiák közül – egyelőre csak kísérleti jelleggel - elkezdték használni az AR[207]-t, amely egy adott helyszínen belül a helyismerettel nem rendelkező kijáró szakember munkáját könnyíti meg, valamint szintén csökkenti az élőmunka időt.

[204] EMS = Energy Management System = energia menedzsment rendszer (itt villamosenergia rendszerre vonatkoztatva)
[205] GIS = GeoInformatics System
[206] ÜIK = ÜzemIrányító Központ = 0,4 kV-os hálózat és a kijáró szakember állomány felügyeleti és irányító központja
[207] AR = Augmented Reality




*4. ábra – KDSZ séma*

A KDSZ-ek üzemirányítása alá tartoznak a beépített teljesítmény tekintetében kiserőműi kategóriába tartozó (50 kW < X < 500 kW) megújuló erőművek. Ezek lehetnek szél, bio és a 2017-ben elkezdődött és jelenleg is igen nagy fejlesztési népszerűségnek örvendő naperőművek. Ezek üzemirányítása folyamatosan növekvő megterhelést jelent az ÁSZ-oknak és KDSZ-eknek, mivel jelentős (és egyre növekvő) számban, területileg elszórtan helyezkednek el és az általuk termelt villamos energia csak az időjárástól és napállástól függ, befolyásolni/szabályozni nem lehet, ellentétben a többi (pl. gáz, víz, szén, atom alapú) erőművel. Egy naperőmű esetében a felhősödés akár 60-70 %-os teljesítmény visszaesést jelent, amelyet kompenzálni kell a kiesési időszakban a villamosenergia egyensúlyfenntartása miatt (lásd. [208] jegyzet IV. fejezete). A másik véglet pedig, hogy több esetben csak azért kell(ett) egy-egy új 120/20 kV-os alállomást építeni az egymás közelébe telepített naperőművek hálózati csatlakoztatásához, mert a meglévő 20 kV-os hálózat - túlterhelődés nélkül - nem bírja(ta) volna elvezetni az egyszerre megjelenő energiamennyiséget.

Minden ilyen erőmű rendelkezik saját fejgéppel (RTU), amelynek direkt adatkapcsolata van az adott KDSZ szervereihez. Mivel ezek tulajdonlás szempontjából az ÁSZ-tól függetlenek, ezért a KDSZ-nek csak üzemirányítási joga és feladata van (termelhet, nem termelhet) az erőmű üzemeltetetést (karbantartás, állagmegóvás, felügyelet/távfelügyelet stb.) az erőmű tulajdonosának kell ellátnia.

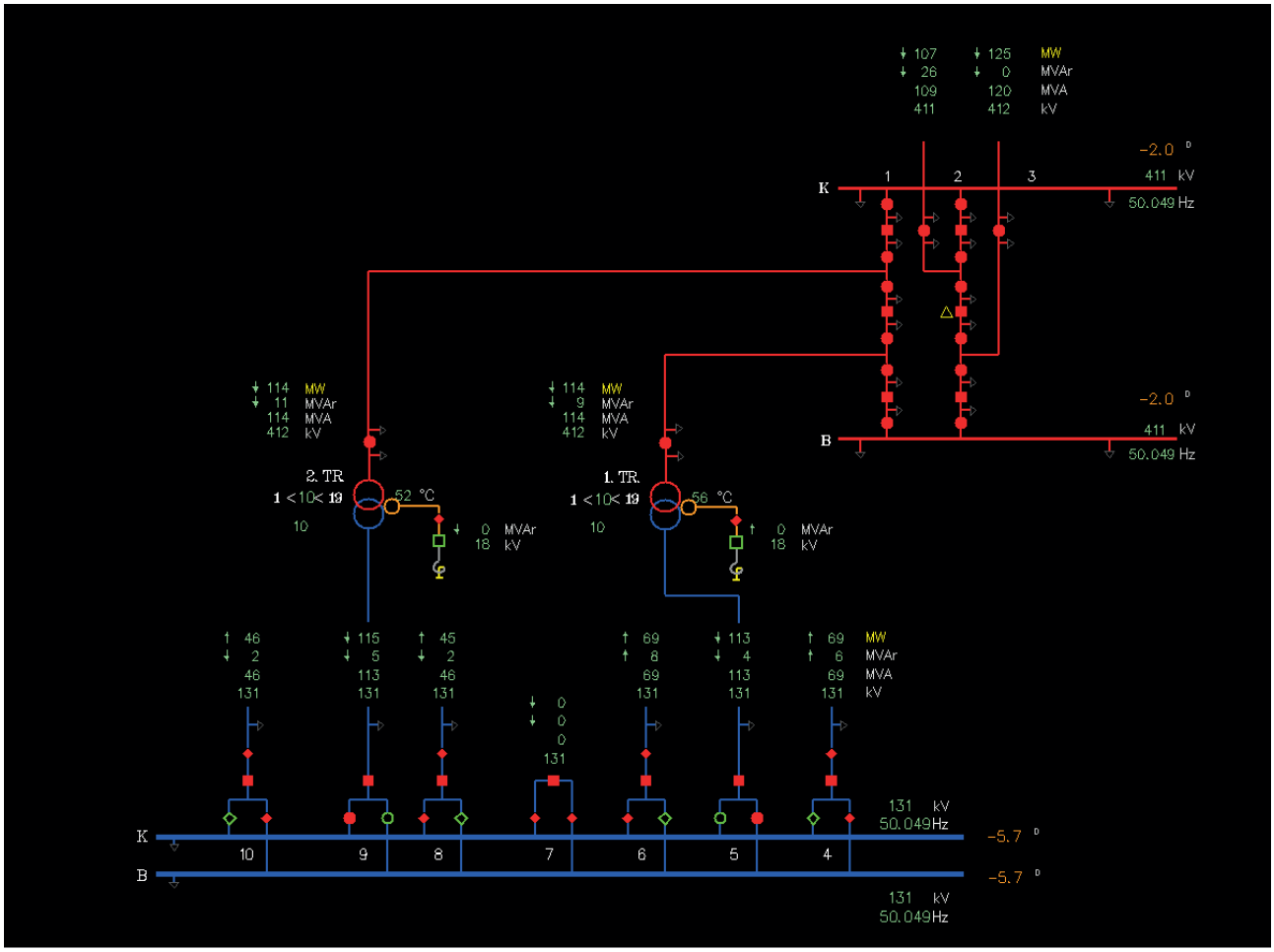
Az előbb említetthez hasonló a helyzet azon nagyfogyasztók esetében (pl. MÁV, nagyobb ipari üzem pl. nyíregyházi LEGO gyár) ahol az alállomás egyik része az ÁSZ, a másik fele pedig a nagyfogyasztó tulajdonában van. Ekkor a teljes 120 kV-os alállomási hálózat üzemirányítója az ÁSZ, üzemeltetésileg (karbantartás, állagmegóvás, felügyelet/távfelügyelet stb.) viszont a tulajdoni határ a döntő. Ez a leggyakrabban a fogyasztói leágazás felé menő 120 kV-os gyűjtősín szakaszoló, ami már a nagyfogyasztó tulajdona, az alállomás többi nagyfeszültségű berendezése (és azok kiszolgálását végző szekunder részek) az ÁSZ tulajdona, az előbb említett üzemeltetési feladatokkal együtt.

[208] „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

### 5.2.2.2. Magyar Villamos Rendszerirányító (MAVIR)

A 750, 400 és 220 kV-os alállomások és távvezetékek felügyeletét és üzemirányítását a MAVIR végzi, valamint a 0,5 MW feletti beépített teljesítményű erőműveknél az üzemirányítást. Mindegyik üzemirányított egységben el van helyezve a MAVIR-nak saját tulajdonú fejgépe vagy külön felső iránya(i) van(nak) az erőművi tulajdonú fejgépben. Azt, hogy egy adott helyszínen a MAVIR melyik megoldást alkalmazza, egyéni elbírálással dől el figyelembe véve a beépített teljesítményt, a tulajdonosi háttért és a villamosenergia rendszerbeli stratégiai szerepét. Mindegyik helyszínről a MAVIR fő és tartalék szerverek irányába saját dedikált távközlési irányokon keresztül kommunikálnak a felső irányok.

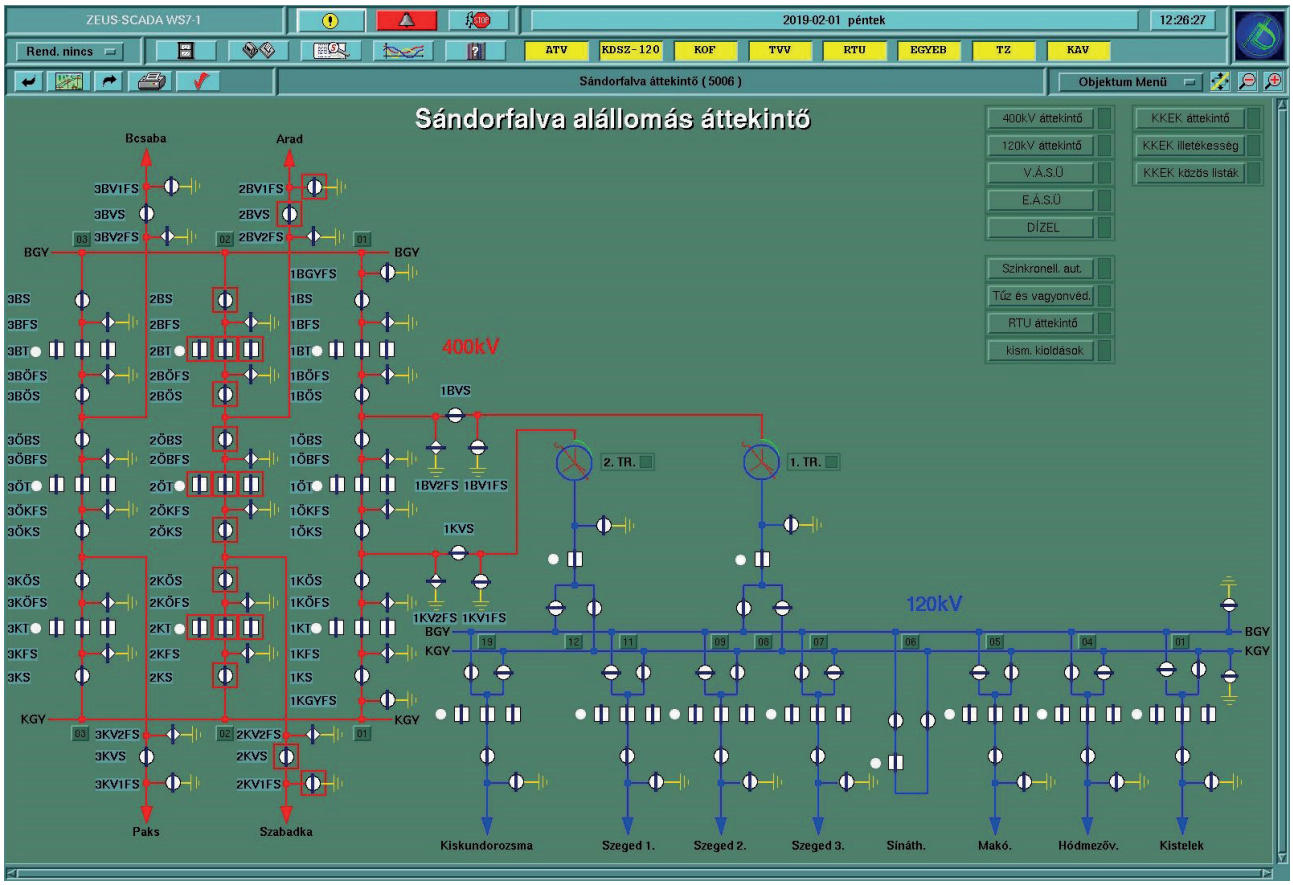
Meg kell különböztetni a MAVIR esetében az országos és nemzetközi energiaegyensúly felügyeletét és a terhelésbecslést biztosító SCADA-t és EMS-t kiszolgáló Siemens[209] gyártmányú - nemzetközi termékként elérhető – Spektrum rendszert és a Prolan Zrt.[210] által gyártott ZEUS alapú üzemirányítási és felügyeleti rendszert. Ezen rendszereknek külön-külön saját központi szervereik vannak, amelyek helyben is és földrajzilag is tartalékoltak.




*5. ábra – Nagyfeszültségű alállomás Spektrum sémája*

[209] Siemens = nemzetközi multicég, amely többek között villamosenergia rendszer felügyeletére képes SCADA rendszert is gyárt és forgalmaz (Spektrum)

[210] PROLAN Zrt. = magyar tulajdonú alállomási felügyeleti rendszert (ZEUS) gyártó és forgalmazó cég




*6. ábra – Nagyfeszültségű alállomás ZEUS sémája*

Az 5. ábra a Spektrum, a 6-os ábra a ZEUS rendszerhez tartozó áttekintő HMI képét mutatja ugyan annak a nagyfeszültségű alállomásnak. A Spektrum kép láthatóan egyszerűbb kialakítású, mivel az energiaegyensúlyfenntartáshoz elegendő az alállomás kapcsolókészülékeinek és mért értékeinek megjelenítése. A ZEUS alapú V.6-os ábra részletesebb megjelenítésű, mivel az alállomás teljes körű felügyeletét kell biztosítania. Ehhez több sémakép is rendelkezésre áll, amely az összes energiaátviteli és segédüzemi feszültségszintet (jelen esetben 400, 120, 18 és 0,4 kV) megjelenítve valamint az összes kiszolgáló rész (egyen és váltakozó áramú segédüzem, vagyon, beléptető és tűzjelző rendszer) távkezeléséhez szükséges információt.

A Spektrumot és a ZEUS-t használó ODSZ[211] és KKEK[212] operátorok számára alkalmazott HMI-k mindegyik szerverre fel tudnak csatlakozni (egyszerre két szerverrel állnak kapcsolatban, amelyikből az egyik a tartalék irány), ugyan így a földrajzilag eltérő helyen lévő tartalék ODSZ-ben és TKKEK[213]-ben lévő HMI-k is. A munkahelyek kialakítása lehetővé teszi, hogy az országot flexibilisen osszák fel egymás között az operátorok, illetve egymás feladatainak az ellátására is képesek.

Nemzetközi együttműködés:

A Spektrum rendszer és az azzal dolgozó operátorok feladata, hogy a nemzetközi ENSTO-E tagság következtében a magyar villamosenergia rendszer által biztosított és a közös rendszerből igényelt villamosenergia pillanatnyi egyensúlyát megtartsák, az előzetesen megállapított villamosenergia áram-

211 ODSZ = Országos Diszpécser Szolgálat, itt a villamosenergia rendszerre vonatkoztatva
212 KKEK = Központi Kezelő Központ
213 TKKEK = Tartalék Központi Kezelő Központ

lási menetrendeket kövessék (hazai és nemzetközi viszonylatban is). Az előbbire a [214] jegyzet IV.3. fejezetében bemutatott folyamatos egyensúly miatt van szükség, utóbbira pedig azért, mert a fogyasztók villamosenergia igénye (időben és térben is!) folyamatosan változik számos tényező (pl. időjárás, napszak, munka/munkaszüneti nap, nagyobb társadalmi esemény stb.) függvényében. Emellett az erőművek által termelt villamosenergia is változik (menetrend, karbantartás, meghibásodás miatt) az energiaáramlások pedig ezek folyományaként alakulnak ki. Az előzetesen becsült és az energiapiacon (energiatőzsdén) szerződésekkel lefixált menetrendek tartása azért is lényeges, mert az ettől való eltérés (többlet és hiány esetén is) jelentős többletköltséget jelent az erőművek, a szolgáltatók (ÁSZ, MAVIR) és az ipari fogyasztók számára is. Amennyiben az eltérés egy adott időablakon belül egy magadott mértéket meghalad (többlet vagy hiány irányban is!), akkor jelentős büntetést kell fizetnie az adott erőműnek/fogyasztónak, mivel a MAVIR-nak ezt ki kell kompenzálnia: túltermelés esetén a fölös energia elvezetésével, alultermelés esetén a hiányt pótolva más forrásból. Mindkét esetnek anyagi vonzata is van.

Tartalék Telemechanikai Rendszer (TTMR[215]):

Az előbb említett Spektrum és ZEUS rendszerektől függetlenül a MAVIR-nak van még egy független – TTMR elnevezésű - mérési rendszere, amely a főbb alállomási csomópontokba, erőművekbe és nemzetközi távvezetékre kerül felszerelésre. Ezek az adatgyűjtők közvetlenül az áram- és feszültségváltókra csatlakoznak (a mezőgépektől függetlenül) és dedikált távközlési vonalon keresztül továbbítják az adatokat a MAVIR tartalék üzemirányító központjában elhelyezett szerverre. A gyűjtött adatokat az energiaegyensúlyt felügyelő operátorok (ODSZ) használják, mint tartalék rendszert.

### 5.2.2.3. Villamosenergia fogyasztásmérés

A trendek, amelyekből a menetrendek követése vagy az ezektől való eltérés látható a SCADA rendszerből nyerik az információt. A tényleges (utólagos) villamosenergia termelés/fogyasztás elszámolása viszont külön - a MEKH[216] által hitelesített - villamosenergia fogyasztásmérőkkel történik. Tipikus elszámolási pontok: erőművek blokktranszformátorainak 120, 220 vagy 400 kV-os oldala (erőmű - MAVIR), 400/120 kV-os transzformátorok 120 kV-os oldala (MAVIR - ÁSZ), 120, 35, 20 kV-os távvezetéki gyűjtősín szakaszolók (ÁSZ - nagy ipari fogyasztók pl. SAMSUNG SDI[217] Göd), 0,4 kV-os csatlakozási pontok (kisebb ipari létesítmények, háztartási fogyasztók). Annak függvényében, hogy mely felek között történik az elszámolás (pl. MAVIR – erőmű, ÁSZ – háztartási fogyasztó, ÁSZ – ipari üzem) eltérő típusú és funkcionalitású fogyasztásmérőket alkalmaznak. Itt kapcsolódik be a smart metering / smart grid (okos mérés / okos hálózat) fogalma a villamosenergia rendszer irányításába (lásd. részletesebben a [218] jegyzet III. fejezetében).

Amennyiben mérőváltó alkalmazása szükséges a fogyasztásmérő bekötésére, akkor külön áram- (az áramváltó szekunder körének fogadásához) és feszültségbemenete (a feszültségváltó szekunder körének fogadásához) van a készüléknek. A nagyfeszültségű elszámolási pontokon (erőművek, MAVIR – ÁSZ, nemzetközi távvezetékek, ipari fogyasztók) használt fogyasztásmérőknek több digitális és erősáramú ki- és bemeneti pontja van abból a célból, hogy mindegyik elszámoló fél le tudja kérdezni a mérőket a saját adatgyűjtő rendszerében. Szintén ezeknél a mérési pontoknál egy fő és egy

[214] „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

[215] TTMR = Tartalék Telemechanikai Mérés = a MAVIR által üzemeltetett független mérési ponttal és távközlési kapcsolattal rendelkező adatgyűjtő rendszer

[216] MEKH = Magyar Energetikai és Közmű-szabályozási Hivatal (MEKH)

[217] SAMSUNG SDI = SAMSUNG SDI Magyarország Gyártó és Értékesítő Zrt.

[218] „Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme” című jegyzet

ellenőrző mérőt is alkalmaznak (független mérőváltó körökről megtáplálva), hogy az elszámolásban egyszeres meghibásodás esetén is a kiesés mentesség biztosítva legyen. Lakossági fogyasztók esetében az utóbbi kettőzést és a mérőváltókat nem alkalmazzák, mivel a 0,4 kV feszültségszintű és jellemzően 63 A-t nem meghaladó fogyasztási helyek direktben beköthetők a fogyasztásmérőkbe.

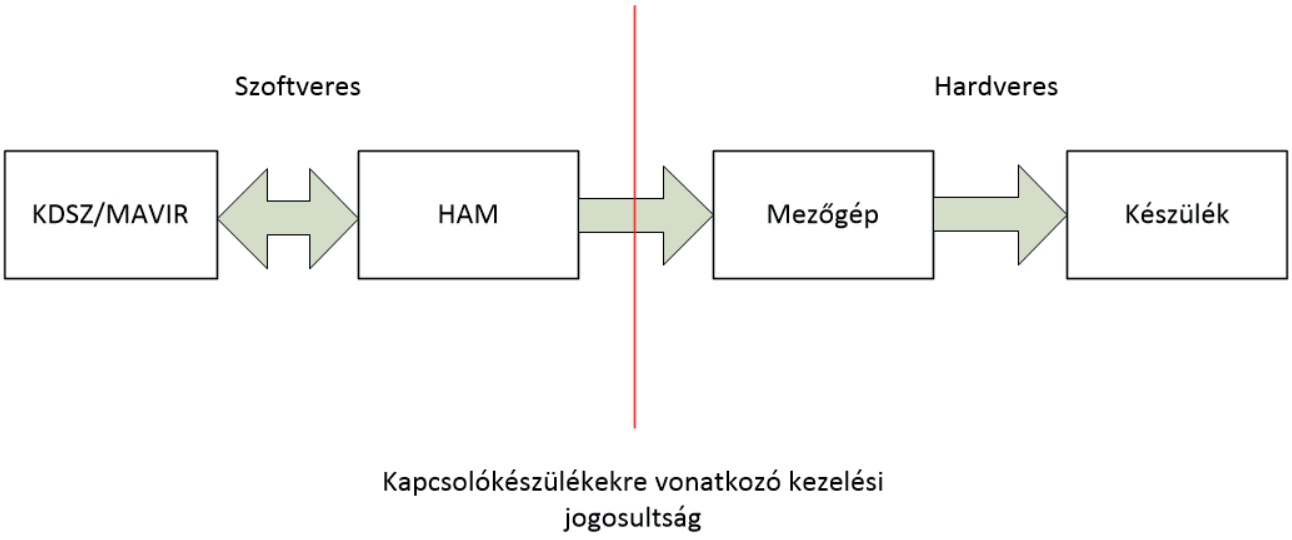
### 5.2.2.4. Üzemirányító operátorok képzése

Az operátorok képzése / tréningezése mindegyik irányító központban (MAVIR, KDSZ) folyamatos, mivel a humán erőforrás változik, illetve a hálózaton is folyamatos bővítések, átalakítások vannak. Ezeknek a változásnak a begyakorlását és az operátorok tudásának naprakészen tartását tréningszimulátor szoftver használatával végzik, amellyel valós üzemi és üzemzavari helyzeteket tudnak szimulálni, így éles beavatkozás nélkül reális körülményeket teremtenek a gyakorláshoz, az üzemzavarok közben kialakuló stresszes, gyors, határozott döntéseket igénylő helyzetek kezelésének elsajátításához. Az adatbázist, amit a tréningszimulátor használ a villamosenergia rendszer on-line SCADA adatbázisból frissítik rendszeresen, így biztosítva a naprakészségét.

A képzésekkel és vizsgákkal válik az lehetővé, hogy az operátorok számos területet tudjanak felügyelni, irányítani illetve üzemzavari és más szükséghelyzetben egymás munkáját segíteni. A tréningszimulátor, az operátor HMI és a szerverek összehangolásával a legújabb generációs szimulátorok esetén lehetővé vált az, hogy az operátor ugyan annál a munkahelynél, mint ahol a szolgálata alatt dolgozik - szimulációs üzemmódban - gyakorol/vizsgázik az oktató/vizsgáztató által irányítva. Ezáltal még inkább a normál üzemi körülmények biztosítottak a tréningezés idejére.

### 5.2.2.5. Kapcsolókészülékek kezelési jogosultsága

Az 5.2. fejezetben szó volt arról, hogy a kapcsolókészülékeket lehet mind a mezőgépről mind a HAM-ról kezelni (ki/be kapcsolni). Az, hogy ki kezeli az adott kapcsolókészüléket rendkívüli jelentőségű egy olyan földrajzilag jelentősen elosztott (Magyarország és az egész kontinens!) és kritikus infrastruktúra esetén, mint a villamosenergia rendszer. Alapvető elv, hogy minden kapcsolókészüléknek egy adott időpontban csak egy felelős kezelője lehet, az összes többi lehetőséget vagy szoftveres vagy fizikai retesszel ki kell zárni. A kezelési lehetőségek egy alállomási készülék esetében az alábbiak.




*7. ábra – Kezelési jogosultságok egy kapcsolókészülékre*

A legalsó szint (az adott kapcsolókészüléktől kiindulva a hozzá fizikailag legközelebb eső) a kapcsolókészülék szekunder szekrényében lévő kezelőszervek (nyomógombok). Amennyiben ezen engedélyezve van a távkapcsolás (egy erősáramú kapcsoló által) akkor innen nem lehet működtetni, hanem átkerül az őt kezelő mezőgéphez. Itt vagy az érintőképernyőn/készüléken lévő nyomógombbal vagy kulccsal (ez az adott gyártótól függ) van lehetőség a mezőgép által kezelt összes kapcsolókészülékre vonatkozóan a mezőgépen tartani vagy felsőbb irányba (HAM) továbbadni a kapcsolási jogosultságot. A HAM – KDSZ/MAVIR viszonylat esetén nem csak egységesen (egy egész alállomás) kapcsolási jogosultságait lehet átadni, hanem szegmensekét külön – külön (pl. erőátviteli transzformátor/távvezeték és kapcsolókészülékei). Ez azért előnyös, mert ha az egyik alállomási transzformátoron hibajavítást végeznek így az alapból a KDSZ/MAVIR-ban lévő kapcsolási jog az alállomáson tartózkodó üzemviteli személyzetnél van, aki jobban át tudja tekinteni a helyszíni munkavégzést. Ebben az esetben is érvényes, hogy csak egy felelős kezelője van az adott kapcsolókészüléknek. Annak függvényében, hogy erőművi, alállomási, ÁSZ, MAVIR, MÁV kapcsolókészülékről van szó a leírt (7. ábra szerinti) jogosultsági rendszer változhat, de az alaplevek megegyeznek.

A felsőbb szintű kezelési jogosultság átadások (KKEK, alállomási HAM) szoftveresek, az alsóbb két szinten (mezőgép, készülék a helyszínen) viszont fizikai beavatkozás történik (kapcsoló átállítása). Mindegyik jogosultsági szint legalább a sajátját és az alatta lévőt megjeleníti, így a helyszínen és a felsőbb szinteken is egyértelmű, hogy az adott készülék kezelése joga hol van. A KDSZ/MAVIR-ban és az alállomási HAM-on is be kell jelentkeznie (egyértelmű azonosítással) az adott helyen lévő kezelő operátornak. Naplózásra kerül minden elvégzett művelet (készülék jogosultság átadás-átvétel, kapcsolás) a kapcsolókészülékek által szolgáltatott jelzésekkel, mérésekkel közös (utólagosan szűrhető, visszakereshető) naplófájlba, így egyértelműen azonosíthatók az elvégzett műveletek és azok hatásai, következményei egy esetleges üzemzavar, téves kapcsolás, fogyasztói kiesés esetén.

### 5.2.2.6. Terhelésbecslés, menetrend

Az 5.2.2.2. fejezetben említett energiaáramlások előzetes meghatározása a rövid (órás), közepes (néhány napos, hetes) és hosszú távú (havi, éves) terhelésbecslések (fogyasztási becslések) illetve az erőművek előzetes termelési menetrendje alapján történik. Ezt a munkát kiszolgáló infrastruktúrát nevezzük EMS-nek, amelynek az alapja a - Magyarországon - Spektrum alapú SCADA adatgyűjtő rendszer kiegészítve számos információforrással (pl. elszámolási fogyasztásmérés, TTMR). Mind a MAVIR, mind az ÁSZ-ok végeznek terhelésbecslést és menetrend készítést a saját területükre, feszültségszintjükre vonatkozóan. A MAVIR nemzetközi és országos viszonylatban végzi ezt, az áramszolgáltatók pedig saját területükre vonatkozóan. Ehhez kölcsönösen (törvényileg és nemzetközi előírásokban rögzített) adatszolgáltatást köteles minden résztvevő (erőművek, ÁSZ-ok, MAVIR, nagyobb és kisebb ipari fogyasztók) nyújtani az érintett partnere számára. A kapott adatok, a korábbi trendek és a kiegészítő körülmények (időjárás, nagyobb társadalmi események, ünnepek, munkanap, munkaszüneti nap, TV műsor, napszak, tervezett karbantartások, tervezett ki- és bekapcsolások) figyelembevételével készülnek el az energiamenetrendek, amelyek az alapját képezik az online energiaegyensúlyi szabályozásnak. Üzemzavarok esetén ettől eltérés alakul(hat) ki az üzemzavar nagyságának függvényében, ekkor a beépített tartalék termelő egységek (pl. Magyarországon a gyors indítású gázturbinás erőművek) indításával lehet a villamosenergia hiányt kiküszöbölni. Amennyiben túltermelés következik be, akkor a szabályozható termelésű erőművek (gázturbinás, fosszilis erőművek) visszaterhelésével lehet az egyensúlyt fenntartani (lásd. [219] jegyzet IV. fejezetében), kritikus esetben pedig az 5.3. fejezetben bemutatásra kerülő védelmek avatkoznak be, automatikusan.

Magyarország pillanatnyi energiaáramlási viszonyai a MAVIR honlapján folyamatosan elérhetők (http://mavir.hu/web/mavir/adatpublikacio).

[219] „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

## 5.3. A villamosenergia-rendszer védelmi és automatika rendszerei[220]

### *5.3.1. A villamosenergia rendszerben lévő védelem és automatika fogalma*

*A védelmeket szokták relévédelmeknek is nevezni, ami még az első generációs készülékek idejéből megmaradt elnevezés. A villamosenergia rendszerben használatos védelmi relé olyan készüléket jelent, amelyet az általa érzékelt fizikai mennyiség adott értékhatárának átlépése esetén működik, és amely működésekor kapcsolókészüléke(ke)t vezérel.*

Ezek a készülékek arra szolgálnak, hogy megszüntessék a zárlatokat (nem kívánt meghibásodásokat) a villamosenergia rendszerben. Ilyen meghibásodás lehet, ha pl. egy faág ráhull a szabadvezetékre és rövid időre (< 1 másodperc) összezár két eltérő potenciálú részt (pl. az egyik fázisvezetőt és a szabadvezeték oszlopot) ezáltal zárlatot okozva. A védelmek és a bennük lévő automatikák feladata, hogy kb. 10 milliszekundum alatt ezt érzékeljék távolról (áram és feszültség méréssel) majd a hibás távvezetéket – amennyiben a hálózatkép olyan mindkét végén – ki- és visszakapcsolják (1-2 másodperc alatt), ezáltal megszüntetve a zárlatot. *A védelmi funkció, ami érzékeli a zárlatot, az automatika pedig, ami - ebben az esetben - a ki- és visszakapcsolást vezérli. Ez utóbbit nevezzük üzemzavari automatikának.* A ki- és visszakapcsolásból otthonainkban általában egy villanást érzékelünk a lámpa fényében és mást nem. *Amennyiben sikerült a zárlatot a rövid 1-2 másodperces ki- és visszakapcsolással elhárítani, akkor a szabadvezeték üzemben marad, ha nem akkor, végleges kikapcsolás történik,* és részletesebben ki kell vizsgálni a hibát, mivel nem múló zárlatról (meghibásodásról) van szó. Az előbb említetten felül számos más zárlati, meghibásodási lehetőség van a villamosenergia rendszerben, ezek mindegyikére van megfelelő védelmi funkció, amelyeket az 5.3.2 - 5.3.5. fejezetek mutatnak be. *A nem üzemzavarok esetén működő, de automatikus beavatkozó funkciókat végző üzemviteli automatikákat a 5.3.5.3. fejezet ismerteti.*

*A védelmi készülékek és automatikák nem megfelelő működése – amely lehetséges nem szándékos (pl. nem megfelelő beállítás, meghibásodás) vagy szándékos (külső „megzavarás”, fizikai vagy kiberbiztonsági behatolás) okból – okozhat nagyobb kiterjedésű villamosenergia kiesést (pl. városrészek, városok, nagyobb földrajzi területek). Amennyiben szándékosan előidézett működési zavarról van szó akkor tartós több órás / napos kiesés is lehet belőle. Ez utóbbi jelenséget nevezzük black out-nak, amely rendkívül komoly (akár végzetes!) humán és anyagi károkat tud okozni (pl. víz-, gáz- és szennyvízszolgáltatás, nagy- és kissebességű tömegközlekedés leállása és ezek következményei).*

Az egyre gyakrabban előforduló extrém időjárási körülmények (szélsőséges meleg/hideg, extrém mennyiségű eső, hó, jegesedés) is okozhat tartós (több órás – több napos) villamosenergia kimaradást kisebb (1-2 település) / nagyobb (10-20 település, országrész) területeken, de ezt nem nevezzük black out-nak, mert nem szándékos emberi beavatkozás okozta.

### *5.3.2. A védelmek és automatikák generációs fejlődése, felépítése*

A villamosenergia-rendszer kialakulásával, folyamatos fejlődésével egy időben a védelmek is változtak, így a védelmi és automatika berendezéseknek három nagy generációja van. A villamosenergia-rendszer kialakulásakor (1940-1950) először elektromechanikus relévédelmeket alkalmaztak. Ezekben a védelmekben a számításokat, időzítéseket, méréseket, működtetéseket elektromágneses és mechanikus elven működő szerkezetek végezték, innen ered az elnevezésük. A készülékek hosz-

[220] Forrásanyag: Dr. Danyek Miklós, Kovács Miklós, Woynárovich András: Nagyfeszültségű hálózati védelmi elvek és megoldások, Elektrotechnika, 2015. április, 5-10. oldalak

szú évtizedekig voltak (és a mai napig vannak még néhány helyen) üzemben. Utánuk jelentek meg az analóg elektronikus eszközök (1970-s évek vége, 1980-as évek eleje), melyeket sokkal rövidebb ideig alkalmaztak. Végül a digitális technika, számítástechnika elterjedésével a digitális védelmi- és automatika készülékek kerültek előtérbe (2000-től). A mai világban csak digitális védelmeket és automatikákat (más néven numerikus- vagy processzoros védelmeket és automatikákat) fejlesztenek, és ezek a készülékek folyamatosan váltják fel a régebbi, még üzemben lévő elektronikus, illetve elektromechanikus készülékeket az egész világon.

A különböző generációjú készülékek majdnem azonos mérési elveken alapulnak, ugyanakkor alapvetően eltérnek egymástól kivitelükben, a fizikai mennyiség érzékelésében, a belső működésükben, és felépítésükben. A fejlődést alapvetően azok a tényezők indokolták, amelyek a mindennapokban is körbevesznek bennünket: információadás (éhség), távoli elérés, automatizálás, információ feldolgozás, MI[221] terjedése. Ezen tényezőknek csak a digitális adatot szolgáltatni és fogadni képes készülékek tudnak megfelelni, így a villamosenergia-rendszerek védelmi és automatika készülékei is ebbe az irányba fejlődtek(nek). Nem szabad elfeledkezni arról a tényezőről sem, hogy a „koros" készülékek (>15 év) javítása, karbantartása is problémás, mivel az alkatrész utánpótlás, szoftverfejlesztés körülményes ezekre a készülékekre, hasonlóan a mindennapjainkat körülvevő digitális eszközökhöz (pl. tablet, mobiltelefon).

A XXI. században alkalmazott védelmi és automatika készülékek felépítésüket, kinézetüket tekintve teljesen megegyeznek az 5.2.1.1. fejezetben ismertetett mezőgépekkel, azaz modulos rendszerűek, belső busszal és TCP/IP alapú külső kommunikációval. A különbség a beléjük programozott funkciókban van: a védelmek feladatukból kifolyólag önálló ki- és visszakapcsolásokat végeznek az általuk felügyelt berendezésen, a mezőgépeknek pedig adatgyűjtő és továbbító feladatuk van kisebb volumenű önálló döntési funkcióval. Az előzőből következik, hogy a kártyakiosztásukban is van különbség, de alapvetően táp-, processzor-, kommunikációs-, mérő-, ki/bemeneti kártyákból épülnek fel. A védelmekben alkalmazott adatgyűjtési protokollokat az 5.4. fejezet ismerteti.

A következő részben bemutatjuk, hogy milyen védelmi és automatika rendszerek üzemelnek napjainkban az átviteli- és főelosztóhálózaton.

### *5.3.3. A villamosenergia rendszerben kialakított védelem-automatika rendszer alapelvei*

Az átviteli és a 120 kV-os hálózat primer kialakítását tekintve hurkolt (=nincs az egyik végén csak termeléssel, a másik végén csak fogyasztóval rendelkező távvezetéke, lásd. [222] jegyzet 4.4.7. ábrája). A védendő primer objektumok (távvezetékek, transzformátorok, gyűjtősínek, amelyek nagyságrendekkel nagyobb értékűek, mint a védelmi berendezés) védelmi funkcióját szolgáló védelem-automatika rendszerek kialakítása, felépítése a hálózati diszpozíció és a primer környezet által megkövetelt igényeket szolgálja ki a rendelkezésre álló műszaki eszközbázis figyelembevétele mellett.

A távvezetékek és transzformátorok védelmi rendszerét az egyszeres – vagy az átviteli hálózaton kettős – alapvédelmi rendszer és visszakapcsoló automatika, valamint a tartalékvédelmek alkotják. Az alkalmazott védelmi rendszer kialakítása a védendő primer objektum feszültség szintjétől, a villamosenergia rendszerben betöltött stratégiai szerepétől, a helyétől, jellegétől, annak elrendezésétől függ.

[221] MI = Mesterséges Intelligencia = Artificial Intelligence

[222] „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme" című jegyzet

## *5.3.4. Az átviteli hálózat védelem-automatika rendszere*

*A magyar átviteli hálózat távvezetékein, és transzformátorain (750 kV/400 kV; 400 kV/220 kV; 400 kV/120 kV; 220 kV/120 kV) kettős alapvédelmi rendszert alkalmaznak, ami azt jelenti, hogy két külön álló készülék (általában ugyanolyan alapfunkcióval) egymástól függetlenül, és egymással párhuzamosan védi a nagyfeszültségű berendezést.* Az elmúlt évtizedek gyakorlata szerint a két alapvédelmi készülék más-más gyártótól származik, de működési elvük ugyanaz: mindkettő *távolsági védelem, vagy transzformátor különbözeti védelem. Előbbi a mért feszültség és áram hányadosának hirtelen változásából (a feszültség értéke hirtelen lecsökken, az áram értéke megnő), utóbbi pedig a transzformátor különböző feszültségű oldalain mért áramok különbségéből (ha zárlat van a transzformátorban, akkor a különbség jelentősen megnő) detektálja a zárlat meglétét.*

### 5.3.4.1. 400 kV-os és 220 kV-os távvezetékek védelem-automatika rendszere

Az átviteli hálózat 220 kV és afeletti feszültség szintű távvezetékei védelmére általánosan távolsági védelmet alkalmaznak. A távolsági védelem egy irányított impedancia elvű (irányított = a mért áram és a feszültség egymáshoz képesti irányából kiindulva meg tudja mondani, hogy felszerelési helyéhez képest a távvezetéken előtte vagy mögötte van-e a zárlat, impedancia = a mért feszültég és áram hányadosa) védelem több impedancia fokozattal: feszültség és áram hányadosának értékétől függően több lépcsőben/fokozatban (időbeli késleltetéssel) való kioldás a védett távvezetékre vonatkoztatva.

Jelentős eltérés a 120 kV-os távvezetékeken alkalmazott távolsági védelmekhez képest (lásd. 5.3.5.1. fejezet), hogy a szabadvezeték két végén lévő alállomások között - nem csak védelmi jelátviteli funkciójú (lásd. 5.4. fejezet) - kommunikációs csatorna van, így az információátvitel lehetősége minden esetben biztosított. Utóbbi funkciót a védelmi jelátviteli készülékek látják el, amelyek feladata a védelmi gyorsító parancsok, valamint másfél megszakítós elrendezés esetén a megszakító beragadás elleni védelmi távkioldó parancs átvitele az ellenkező oldali védelmi készülékek számára. A védelmi gyorsító parancs a távvezeték végén lévő zárlatok gyorsabb hárítását szolgálja, a második fokozatos (időben késleltetett) kioldás késleltetését csökkenti le alapidős (= a készülék önidős ~ 25-40 ms) kioldásra. Ez azért lényeges, mert a minél gyorsabb zárlathárítás a kiesés idejét és ezáltal a nagyobb kiterjedés esélyét is lecsökkenti.

A normál üzemállapot mielőbbi visszaállítását visszakapcsoló automatika alkalmazásával valósítjuk meg, mely funkciót a két alapvédelmi készülék integráltan foglalja magába. A hiba típusától (fázis - nulla, 2 fázisú, 3 fázisú stb.) függően egyfázisú, illetve háromfázisú visszakapcsolási (EVA[223], illetve HVA)[224] ciklust alkalmazunk, amely - ahogyan a nevében írva van - vagy csak egy fázisban vagy mind a három fázisban ki- és visszakapcsolja a távvezetéket. Amennyiben csak egyfázisú a zárlat az a kedvezőbb, mivel a távvezeték két vége a másik két fázison keresztül összeköttetésben marad.

Minden NAF[225] távvezeték rendelkezik AZT0[226] védelemmel. Ez a – magyar fejlesztésű és csak Magyarországon alkalmazott – védelem nem igényel külső tápfeszültséget, a zárlat energiájának segítségével kapcsolja ki a megszakító (amelyet az áramváltó szekunder körén keresztül vételez), abban az esetben, ha sem az alap, sem a tartalék védelem nem oldott ki. Ennek a védelemnek a legnagyobb a beállított késleltetése, meg kell várnia, amíg minden alap- és tartalék védelem lefut.

[223] EVA = Egyfázisú Visszakapcsoló Automatika
[224] HVA = Háromfázisú Visszakapcsoló Automatika
[225] NAF = Nagyfeszültségű >=120 kV
[226] AZT0 (ejtsd: AZTnull) = földzárlat érzékelésű Autonóm Zárlati Túláramvédelem

### 5.3.4.2. NAF/NAF transzformátorok védelmei és automatikái

Az átviteli hálózati (750/400 kV, 400/220 kV, 400/120 kV, 220/120 kV) transzformátorokat 2 db különbözeti elvű villamos védelemmel látják el (lásd. 5.3.4. fejezet). Ezek háromlábúak (= a transzformátor három különböző feszültségszintjét jelenti (pl. 400/120/18 kV), a harmadik láb az alállomás segédüzemét tápláló tercier KÖF tekercsen van lezárva. A védelem önidős, késleltetés nélküli működésű, transzformátor bekapcsolási áramlökésre reteszelő funkcióval kiegészített készülék. Minden transzformátort külön fázis (AZT[227]) és külön földzárlatot érzékelő (AZT0 tip.) tartalékvédelmek is védenek. Hasonlóan a 120 kV/KÖF[228] transzformátorokhoz (lásd. 5.3.5.3. fejezet) mechanikus elvű védelmeket is használunk: gáz és olajlökés relé (Buchholz relé), több ponton mért olaj- és tekercshőmérséklet érzékelés, nyomáscsökkentő szelep. Mindegyik mechanikus védelem rendelkezik előjelző és kioldó fokozattal is. Amennyiben külön olajterű a transzformátor fokozatszabályzója, akkor az is rendelkezik saját mechanikus védelmekkel: gáz és olajlökés relé, nyomáscsökkentő szelep. A mechanikus védelmek nem a villamos paraméterek mérésével (feszültség, áram) detektálják a zárlatot, hanem a transzformátor szigetelőolajában a zárlat miatt létrejövő kémiai reakciók hatására kialakuló gázbuborékot (Buchholz relé) vagy a zárlat miatt bekövetkező olajnyomás hullámot (olajlökés) érzékelik és adnak kioldást. Ezek a transzformátorok az átviteli hálózat legösszetettebb és legnagyobb koncentrált értékű berendezései, így a villamos és mechanikai károsodásuk megakadályozása kiemelten fontos. A felsorolt védelmek a zárlatok megszűntése mellett az említett károsodások ellen is védik a transzformátorokat.

### 5.3.4.3. 400 kV-os és 220 kV-os gyűjtősínek védelmi rendszere, valamint a megszakító beragadás elleni védelem

Az átviteli hálózati csomópontok – az alállomásokban lévő gyűjtősínek (lásd. pl. [229] jegyzet 4.4.2. ábrája „K” és „B” gyűjtősín) – kiemelt fontosságúak a villamosenergia rendszer egésze szempontjából, ugyanakkor itt nagyon kicsi a valószínűsége zárlatok kialakulásának, így egyszeres alapvédelmi rendszerük van tartalék védelemmel.

Az alapvédelmi funkciót a különbözeti elvű gyűjtősínvédelmi berendezések látják el, amelyek a csomópontba (gyűjtősín) be- és kifolyó áramok összegzéséből határozzák meg, hogy van-e a zárlat vagy sem. Amennyiben az összegzés értéke meghalad egy határértéket, akkor kiold az összes erre a gyűjtősínre csatlakozó megszakító. Az eszköz kivitelét tekintve lehet centralizált, amely egy központi helyre telepített berendezést jelent (pl. DGYD[230], EGYD[231] tip.), vagy decentralizált (pl. OGYD[232] tip.), a leágazások saját mezejében történt érzékelést (leágazási egységben), optikai kábelen történő adatátvitelt, majd egy központi egységben történő kiértékelést megvalósító. Utóbbi elterjedését az optikai összeköttetés lehetősége és a numerikus elvű berendezések alkalmazása tette lehetővé. Az átviteli hálózaton kizárólag ilyen védelmek működnek. Jelentős előnye a centralizált védelmekhez képest, hogy mérőváltók áramát és feszültségét nem kell egy helyre kábelezni az alállomás területén, így jelentős költségmegtakarítást lehet elérni.

A gyűjtősínre csatlakozó leágazások valamely megszakítójának esetleges beragadása esetén a megszakító beragadás elleni védelem az összes mögöttes zárlati betáplálást leválasztja, megakadályozva a zárlat okozta romboló hatás továbbterjedését. Ezzel nagyobb terület lesz kikapcsolva, mintha az eredeti megszakító működött volna csak, de az anyagi kár mérséklése és az így kisebb visszaállítási idő jelentősebb tényező ebben az esetben, mint a rövidebb időre történt nagyobb méretű kiesés.

---

227 AZT = fáziszárlat érzékelésű Autonóm Zárlati Túláramvédelem

228 KÖF = Középfeszültségű

229 „Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára - Kritikus információs infrastruktúrák védelme” című jegyzet

230 DGYD = Digitális Gyűjtősín Differenciál védelem

231 EGYD = Elektronikus Gyűjtősín Differenciál védelem

232 OGYD = Optikai Gyűjtősín Differenciál védelem

A tartalékvédelmi funkciót a gyűjtősínekhez kapcsolódó távvezetéki leágazásokba telepített távolsági védelmek gyűjtősín fele néző ún. hátra pillantó fokozata (irányított impedanciavédelem), és a transzformátor leágazásokba telepített impedancia elvű védelmek látják el (lásd. 5.3.4.1. fejezet).

## *5.3.5. A 120 kV-os főelosztóhálózat védelem-automatika rendszere*

A hazai 120 kV-os főelosztóhálózat a stratégiai kapocs szerepét tölti be az országos átviteli hálózat (400 kV, 220 kV) és a középfeszültségű (35 kV, 20 kV, 10 kV) elosztóhálózat között. Ez a szerepe csak az elmúlt évtizedek folyamán alakult ki, de még mindig vannak olyan 120 kV-os hálózati részek (távvezetékek), amelyek átviteli hálózati (pl.: Sajószöged – Felsőzsolca 120 kV, Felsőzsolca – Sajóivánka 120 kV), illetve ipari ellátási (pl.: Sajószöged – Tiszai Vegyi Kombinát 120 kV) funkciókat töltenek be.

### 5.3.5.1. 120 kV-os távvezetékek védelem-automatika rendszere

A 120 kV-os főelosztóhálózatot szabadvezetéki és kábelhálózatok alkotják. A 120 kV-os kábelhálózatok, illetve a sűrűn lakott területek (városok) fölött haladó szabadvezeték védelme kettős alapvédelmi rendszerű, míg a többi távvezetéken egyszeres alapvédelem van kialakítva. A 120 kV-os automatikák GVA[233] és LVA[234] ciklust is alkalmaznak, az EVA és a HVA mellett. Az alapvédelmi rendszer hibája esetén a tartalékvédelem feladata a hibás hálózatelem szelektív (minél kisebb területet érintő) leválasztása, aminek működés elmaradásakor az AZT0 tip. tartalékvédelem ad – a legtöbb esetben – nem szelektív kioldást.

#### Hurkolt távvezetékek

Hurkolt távvezeték meghibásodása esetén a nagy zárlati teljesítmények miatt a zárlatos hálózatrészt késleltetés nélkül le kell választani, a hálózati zavartatást megszüntetni, a hiba fellépése előtti normál üzemi állapot minél előbb helyre kell állítani, hasonlóan a NAF távvezetékek esetén.

#### Rövid távvezetékek (L<10 km)

Rövid távvezetékek szelektív védelmi funkcióinak ellátására különbözeti elvű szakaszvédelmek szolgálnak, amelyek működési elve hasonló a transzformátoroknál alkalmazottal = amennyiben a távvezeték két végén folyó áram közötti különbség meghalad egy értéket, akkor zárlat van a távvezetéken és kikapcsolja azt. A szakaszvédelem előnye a zárlathárítás során a gyors (önidős) kioldás megvalósítása, hátránya viszont a két végpont közötti összeköttetés (információ átvitel) biztosításának igénye. Erre a funkcióra korábban erősáramú jelzőkábeles (M-R tip.), majd telefonvonalas (SZVPIZ tip.) összeköttetéssel rendelkező szakaszvédelmeket alkalmaztunk. Ezek jelentős hátránya, hogy védelmi jelátvitelt szolgáló rezes összekötetést kellett kiépíteni a működésükhöz. Az optikai kábelek jelentős térhódítása nyomán (amely az árcsökkenés miatt következett be) ma már optikai kábel felhasználásával direktben kötik össze a numerikus elvű védelem-automatika (pl.: DSZV, DTVA-OX) berendezéseket a távvezeték két végén. A felhasznált optikai kábel (48-96 db) szálszámmal (és így többször 10 Gbps sávszélességgel) rendelkezik, így nem csak a védelmi berendezések jelzéseit képes továbbítani, hanem más médiumok (pl. kábeltv, internet, telefontársaságok stb.) részére is bérbe lehet adni (lásd. 5.4. fejezet).

[233] GVA = Gyors Visszakapcsoló Automatika, amelynek a visszakapcsolási ideje jellemzően 2-4 másodperc

[234] LVA = Lassú Visszakapcsoló Automatika, amelynek visszakapcsolási ideje több tíz másodperc, jellemzően 60

**Hosszú távvezetékek (L>10 km)**

A hosszabb távvezetékek szelektív védelmi funkcióinak ellátására távolsági védelmek szolgálnak. A távolsági védelem előnye, hogy nem igényel összeköttetést a távvezeték másik végén lévő berendezéssel. Hátránya, hogy - a megvalósított lépcsős impedancia (mért feszültség és áram hányadosa) karakterisztika elvéből adódóan - a vezeték mentén fellépő hibák helyétől függően nem minden esetben történik meg a zárlatos távvezeték önidős leválasztása hasonlóan a NAF hálózati távvezetékekhez. A távvezeték végi hibák késleltetés nélküli leválasztását az ún. „Túlfedés" funkcióval valósítjuk meg, ami esetenként a védendő távvezetéken túl fellépő hibákra nem szelektív „járulékos" működést okozhat, mivel önidővel kikapcsolásra kerül az alapértelmezetten késleltetett védelmi részen lévő vezeték/fogyasztó. Ezen funkció használata attól függ, hogy az adott vezeték esetében a gyorsaság vagy a szelektivitás (csak a minimálisan szükséges hálózatrész kikapcsolása) a nagyobb prioritású, amelynek eldöntése a távvezeték által ellátott fogyasztó(k)tól illetve a hálózati struktúrától függ.

**Sugaras távezetékek**

A sugaras távvezetékek kialakításukat tekintve lehetnek végponti vagy „T" (kettős „T") fogyasztói transzformátorral rendelkező leágazások [235]. Az alakzat végpontján ún. „C-védelem" elv látja el a védelmi-automatika funkciót azért, hogy a távvezetéken egyfázisú visszakapcsoló automatika működhessen. Ennek az érzékelési elvnek az alkalmazásával lehetséges a hibás fázis kiválasztása, majd ki – és visszakapcsolása EVA és GVA automatika funkciók alkalmazásával.

### 5.3.5.2. 120 kV-os gyűjtősínek védelmi rendszere

A 120 kV-os gyűjtősínek védelmét az átviteli hálózatnál már ismertetett (lásd. 5.3.4.3. fejezet) kombinált gyűjtősín és megszakító beragadás elleni védelmek látják el. Eltérően az átviteli hálózattól vegyesen, centralizált (EGYD, DGYD) és decentralizált (OGYD) elvű berendezések is vannak a főelosztó hálózaton, attól függően, hogy az alállomás milyen tulajdonosi felépítésű és milyen korú szekunder berendezésekből épül fel.

A gyűjtősínek tartalékvédelmi funkcióját a leágazásokba telepített távolsági védelmek gyűjtősín irányába érzékelő ún. „visszapillantó fokozata" látja el. Ez a funkció az ún. „természetes gyűjtősínvédelem", hasonlóan az átviteli alállomásokhoz (lásd. 5.3.4.3. fejezet).

### 5.3.5.3. 120 kV/KÖF transzformátorok védelem-automatika rendszere

A főelosztóhálózaton alkalmazott transzformátorok teljesítménye 16 MVA, 25 MVA, 40 MVA és 63 MVA. A transzformátor teljesítményétől függően $S_n$<40 MVA egyszeres alapvédelemként, $S_n$>40 MVA kettős alapvédelemként differenciál elvű védelmek vannak telepítve.

A 120 kV/KÖF transzformátorok védelmi feladatainak ellátására villamos és mechanikus elvű védelmeket használunk. A transzformátor alapvédelme a differenciálvédelem, tartalékvédelmi funkcióját a 120 kV-os késleltetett túláramvédelem látja el, valamint az AZT típusú tartalékvédelem. Az átviteli hálózatnál már ismertetett (lásd. 5.3.4.2. fejezet) mechanikus elvű védelmek közül a gázvédelem, az olajáramlás védelem és a túlmelegedés elleni védelmek működnek a 120 kV/KÖF transzformátoroknál.

A középfeszültségű gyűjtősín alapvédelmét és a leágazások távoli tartalékvédelmét független késleltetésű, kétlépcsős túláramvédelem vagy impedanciavédelem és visszakapcsoló automatika végzi. A középfeszültségű leágazások beragadási védelmi funkciója szintén a transzformátor védelmi rend-

[235] Végponti leágazás: egy irányból táplált (sugaras) távvezeték legtávolabbi végpontja. „T" vagy kettős „T" leágazás: egy irányból táplált (sugaras) távvezeték közbenső (nem legtávolabbi) végpontja.

szerébe integrált. A középfeszültségű földzárlatvédelmi feladatokat a FÁVA[236] automatika látja el, amely a zárlat idejére (mivel mesterségesen le van csökkentve a zárlati áram értéke) megnöveli azt, hogy a védelem ki tudja választani, hogy melyik gyűjtősín leágazásban van a zárlat. A mesterségesen lecsökkentett zárlati áram értéke nem azt jelenti, hogy tartósan fennállhat, hanem, hogy megadott határértéken belülre van korlátozva, hálózati követelmények miatt.

Üzemelő transzformátor meghibásodása, üzemzavara esetén a rendelkezésre álló tartalék transzformátor vagy sínbontó feltétel-ellenőrzött, azonnali bekapcsolását az üzemzavari ETRA[237] automatika végzi el. Ez automatikusan bekapcsolja – bizonyos hálózati, készülék rendelkezésre állási és üzemeltetési feltételek megléte esetén – a tartalék transzformátort, hogy a kiesés idejét minimalizálni lehessen. Ez a funkció stratégiai szempontból fontos alállomások / csomópontok / fogyasztók esetén működik, mivel jelentős beruházási előkészítést és fokozottabb üzemviteli készültséget igényel.

Üzemviteli automatikák

Az üzemviteli automatikák feladata a hálózati viszonyokban bekövetkező, üzemszerű, tartós változások automatikus kezelése, hálózati jellemzők (pl.: feszültség, hálózati kompenzáltság mértéke) paramétereinek szabályozása.

A feszültségszabályozó automatika feladata az, hogy a transzformátor menetszámának változtatásával az alállomási gyűjtősín feszültségszintje olyan értéken legyen, hogy a fogyasztók csatlakozási pontjain a feszültség a szabvány által meghatározott értékhatáron belül maradjon, különben a túl alacsony feszültség esetén a készülékek nem tudnak működni, túl magas feszültség esetén pedig meghibásodhatnak. Ez 0,4 kV-on (háztartási fogyasztók csatlakozási szintje) 230-240 V körüli értéket jelent. Ezt a funkciót az FHA[238] és az ATSZ[239] automatika együtt valósítják meg.

A transzformátor üzemközbeni túlmelegedését a transzformátor hűtésautomatika funkció gátolja meg a transzformátor hűtőventillátorok megfelelő vezérlésével. Jelenleg ezen funkciók numerikus elvű mezővezérlőkkel valósulnak meg (DTSZ-HA, ITSZ tip.). Az 5.3.4.2. fejezetben bemutatott NAF/NAF transzformátorok esetében is alkalmaznak hűtésautomatikát, amely nem csak a ventillátorokat, hanem az olaj áramlásáért felelős szivattyúk működését is vezérli. Ezen felül figyelembe veszi a ventillátorok és a szivattyúk üzemidejét, így egyenletesebb lesz a kopás/elhasználódás mértéke is, amely üzemidő növekedést és költségmegtakarítást eredményez.

Az ISZA[240] feladata, hogy (a középfeszültségű kompenzált hálózat mindenkori üzemállapotának megfelelően) a földzárlati hibahely kapacitív földzárlati áram kompenzálását úgy végezze el az induktív tekercs szabályozásával, hogy a szabvány által meghatározott értékhatárok között legyen a kialakuló maradékáram szintje. Jelenleg már ezt a funkciót is numerikus elven működő automatikák alkalmazásával oldjuk meg (DRL[241]).

Az 5.3. fejezetben ismertetett védelmi és automatika elvek részletesebb ismertetése az [242] irodalomban található meg.

---

236 FÁVA = Földzárlati Áramnövelő (FÁVA) ellenállást Vezérlő Automatika

237 ETRA = Eseményvezérelt TRanszformátor átkapcsoló Automatika

238 FHA = Feszültség Határoló Automatika

239 ATSZ = Automatikus Transzformátor Szabályozó

240 ISZA = Ívoltó Szabályozó Automatika

241 DRL = Digitális RL kör szabályozó automatika

242 Póka Gyula: Védelmek és automatikák a villamosnergia-rendszerekben

## 5.4. A villamosenergia-rendszer kommunikációs hálózata

### *5.4.1. A kommunikációs hálózat története napjainkig*

A villamosenergia rendszer kialakulása során – az akkori kor technológiai fejlettségének megfelelően - elektromechanikus védelmi és irányítástechnikai készülékeket használtak, amelyeket vagy közvetlenül a készülék mellől vagy egy épületen belül kialakított erősáramú (24, 48, 110, 230 V AC vagy DC) átjelzések alapján kezeltek, felügyeltek. Minden alállomásban és erőműben folyamatos üzemeltető személyzet volt, amely – amikor odáig jutott a telefonhálózat elterjedtsége – telefonon keresztül egyeztetett az üzemviteli és üzemzavari eseményekről. A villamosenergia hálózat országon belül is széttagolt volt, nemzetközi (határkeresztező) távvezetékek nem léteztek. A ténylegesen mechanikus elven működő védelmi és automatika készülékekre mutat példát a 8-as ábra.

*8. ábra – Elektromechanikus védelmi és automatika készülék*

Ez a berendezés a kornak megfelelő mennyiségű információt volt képes szolgáltatni a készülékről: kioldott/indult-e a védelem, ha igen akkor melyik fokozata, valamint üzemképes-e a készülék. A helyszínen vizuálisan minden információ könnyen leolvasható volt a készülékről, mivel minden mechanikus tárcsákkal, fogaskerekekkel és mágnestekercsekkel működött. A védelem beállítása is ezekkel a finommechanikai eszközökkel történt.

Irányítástechnika szempontjából az erőművekben és a terhelésbecslésben (lásd. 5.2.2.6. fejezet) alkalmaztak először analóg, majd digitális számítógépeket. Ezek a gépek csak az adott helyszínen rendelkezésre álló adatokkal dolgoztak (on-line távközlési hálózat ekkor még nem létezett), így teljesen lokális működésűek voltak.

Amikor az elektronika fejlettsége, megbízhatósága és integráltsági foka elérte azt a szintet (1970-es évek vége), hogy a védelmi és automatika készülékeket is lehettet belőlük gyártani elkezdődött az elektronikus működési elvű készülékek gyártása és beépítése (lásd. 9. ábra).


*9. ábra – Elektronikus működési elvű védelmi és automatika készülék*

Ezek a készülékek csak belső működésükben (és kis mértékben mérési elvükben) különböztek az elektromechanikus készülékektől, de külső kommunikáció szempontjából nem szolgáltak plusz információval. Modulos (kártyás) kivitelűek voltak, korai elvű buszrendszerrel rendelkeztek. Analóg és digitális elvű távméréseket alkalmaztak már ekkoriban, de a beavatkozás továbbra is csak lokálisan történt, a helyszínen lévő üzemviteli személyzet által. Mivel a humán felügyelet folyamatos volt, így az a külső kommunikációs információ amelyet ezek a készülékek biztosítani tudtak, megfelelő volt. A telefonos egyeztetés, majd utóbb a fax-os információ csere elegendőnek bizonyult a megfelelő üzembiztonságú villamosenergia-rendszer fenntartásához.

Az 1990-es évek elején kezdődött el az ÜRIK[243] program, amelynek keretében az átviteli és főelosztóhálózati alállomásokról és erőművekből célzott adatgyűjtés indult meg az akkori kornak megfelelő processzoros mezőgépekkel. Ez volt a digitális irányítástechnika és védelmi adatgyűjtés kezdete. Minden fejlesztő és gyártó a saját maga számára legmegfelelőbb (gyakran saját maga által fejlesztett) protokollt használta a centralizált és decentralizált adatgyűjtés megvalósításához (pl**:** SPA[244], LON[245], Protecta[246] hurok, egyszeres vagy kétszeres Prolan[247] hurok, IEC-60870-5-101[248]). Amikor több gyártótól származó védelmi és irányítástechnikai berendezések kerültek telepítésre egy alállomásba vagy erőműbe, akkor mindegyiknek szüksége volt a saját gyártójától származó adatgyűjtő rendszerre (csatolókra és ezek összeköttetésére). A különböző gyártók protokolljai között pedig konvertereket (gateway) kellett alkalmazni, minden összeköttetés esetében külön-külön. Erre mutat példát a 10. ábra.

243 ÜRIK = Üzemirányító Rendszer Irányítástechnikai Központ Korszerűsítése

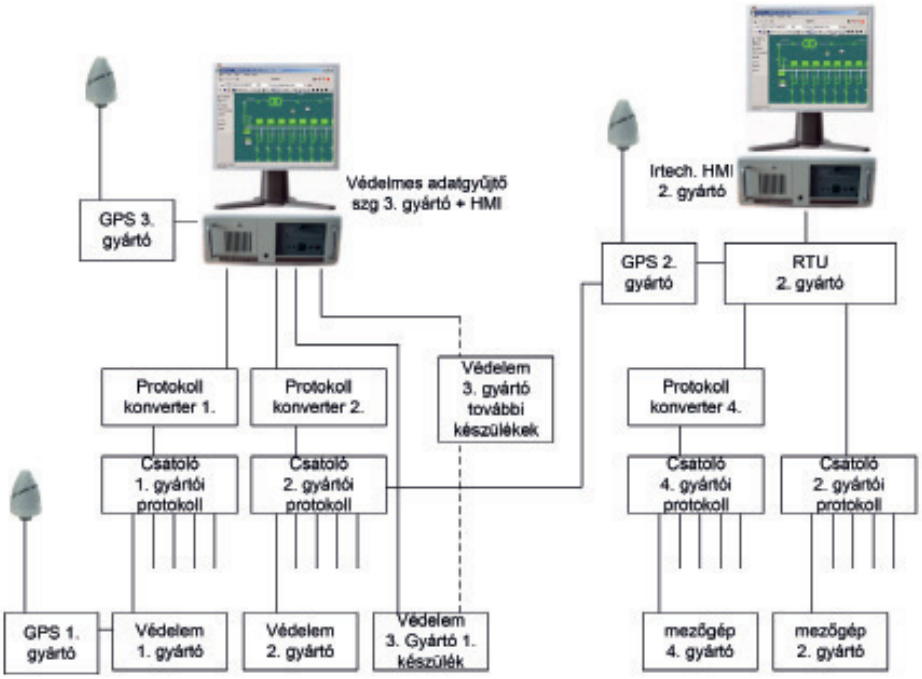
244 SPA = ABB licenszű irányítástechnikai adatgyűjtő protokoll

245 LON = ABB licenszű védelmes adatgyűjtő protokoll

246 Protecta Kft. = villamosenergia rendszer védelmi és irányítástechnikai készülék gyártó és forgalmazó (magyar)

247 Prolan Zrt. = villamosenergia rendszer irányítástechnikai készülék gyártó és forgalmazó (magyar)

248 IEC 60870-5-101 = International Electrotechnical Commission (IEC) által létrehozott nemzetközi szabvány (klasszikus pont – pont soros összeköttetés) https://www.ipcomm.de/protocols_en.html




*10. ábra – : Saját protokollos, adatgyűjtők, gateway-ek pont – pont kapcsolattal*

Az ábrát tekintve látható, hogy például a „Védelem 2. gyártó" készülékétől az információ a saját „Csatoló 2. gyártói protokoll" csatolón és a „Protokoll 2. konverter" gateway-en keresztül jut el a „Védelmes adatgyűjtő szg. 3. gyártó + HMI" eszközhöz. Minden készülék pont – pont kapcsolattal rendelkezik, redundancia nincs kialakítva az összeköttetésekben (ez alól kivételek voltak pl. Prolan hurok, Protecta hurok), ami nem üzembiztos megoldás egy távkezelt alállomáson vagy erőművi villamos elosztóban. Abból a szempontból viszont jó megoldás volt, hogy az adott gyártó sajátosságát ismerni kellett hozzá bármilyen jellegű beavatkozáshoz, így a szándékos meghibásodás/kiesés okozása nem volt egyszerűen kivitelezhető.

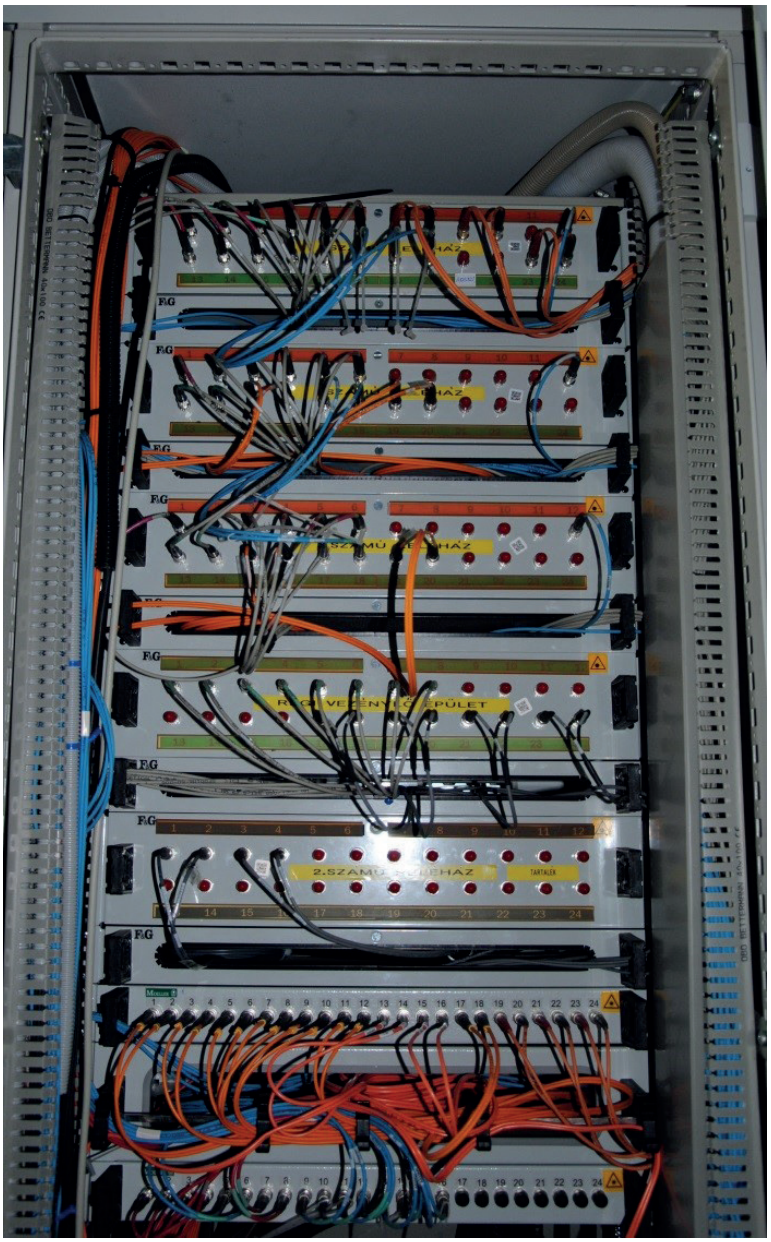
*Ezzel szemben a jelen korban alkalmazott Ethernet alapú hálózatok sokkal inkább támadhatók, mivel nem egyedi fejlesztések, hanem univerzálisak, amelynek alapjai bárki számára hozzáférhetők.*

A trend abba az irányba fordult, hogy az ÁSZ-ok, a MAVIR, a nagy ipari fogyasztók és az erőművek minél kisebb létszámú személyzettel (vagy személyzet nélkül akarták(ják)) üzemeltetni a villamosenergia hálózatukat/rendszerüket, így kellettek olyan technológiai megoldások, amelyek a távolról való elérést/felügyeletet lehetővé tették, nem engedve az üzembiztonsági szintből.

A 2000-es évektől kezdett el terjedni az optikai hálózatok (lásd. 11. ábra) alkalmazása a kommunikációs rendszerekben mind lokális (alállomáson/erőművön belül), mind a távolabbi irányokba (KDSZ, MAVIR, másik alállomás), mivel ez a technológia is egyre olcsóbb lett. Távolság szempontjából a multimodusú[249] optikai összeköttetést (<1 km) az előbbi, a monomodusú[250] optikai összeköttetések (1÷40 km) az utóbbi esetben alkalmazzuk (lásd. 5.4.3. fejezet).

[249] Multimódusú optikai kábel = üvegszál vezető anyagú fénykábel jellemzően rövidebb < 1 km adatátvitelre

[250] Monomódusú optikai kábel = üvegszál vezető anyagú fénykábel jellemzően rövidebb > 1 km adatátvitelre



*11. ábra – Optikai kapcsolatok alkalmazása egy alállomáson*

Az optikai kapcsolat alkalmazásának jelentős előnye, hogy EMC[251] (elektromágneses kompatibilitás) szempontjából leválasztja az eszközöket, azaz ilyen összeköttetésen keresztül nem terjednek az elektromágneses zavarok.

Üzemeltetés szempontjából jelentős előrelépés volt az Ethernet alapú IEC 60870-5-104[252] protokoll bevezetése, ami már lehetővé tette a pont-pont kapcsolatok megszüntetését, de a gyártóspecifikusságot nem szüntette meg, mivel ez a szabvány csak a kommunikációs felületet határozta meg, de konkrétabb előírást nem tartalmaz (pl. védelmi és irányítástechnikai funkciók), mivel az ez a szabvány az egyszerű soros protokoll (IEC 60870-5-101) Ethernet hálózatra való átültetése.

[251] EMC = ElectroMagnetic Compatibility definíciója: Az elektromos eszköznek működnie kell tudnia a saját maga által generált elektromágneses környezetben, miközben nem bocsáthat ki olyan elektromágneses zavart, amely más eszköz működését zavarja. https://www.emtest.com/what_is/emv-emc-basics.php

[252] IEC 60870-5-104 = International Electrotechnical Commission (IEC) által létrehozott nemzetközi szabvány (TCP/IP alapú soros összeköttetés) https://www.ipcomm.de/protocols_en.htm

*Az így bevezetett Ethernet alapú hálózatok magukkal hoz(nak)tak számos előnyt (flexibilitás, könnyű bővíthetőség, szélesebb körű kompatibilitás), de magukban hordozzák azt a lehetőséget is, hogy egy kibertámadás során sokkal egyszerűbb annak kiterjesztése.*

### *5.4.2. Alállomási védelem – automatika és irányítástechnikai rendszerek a 21. században*

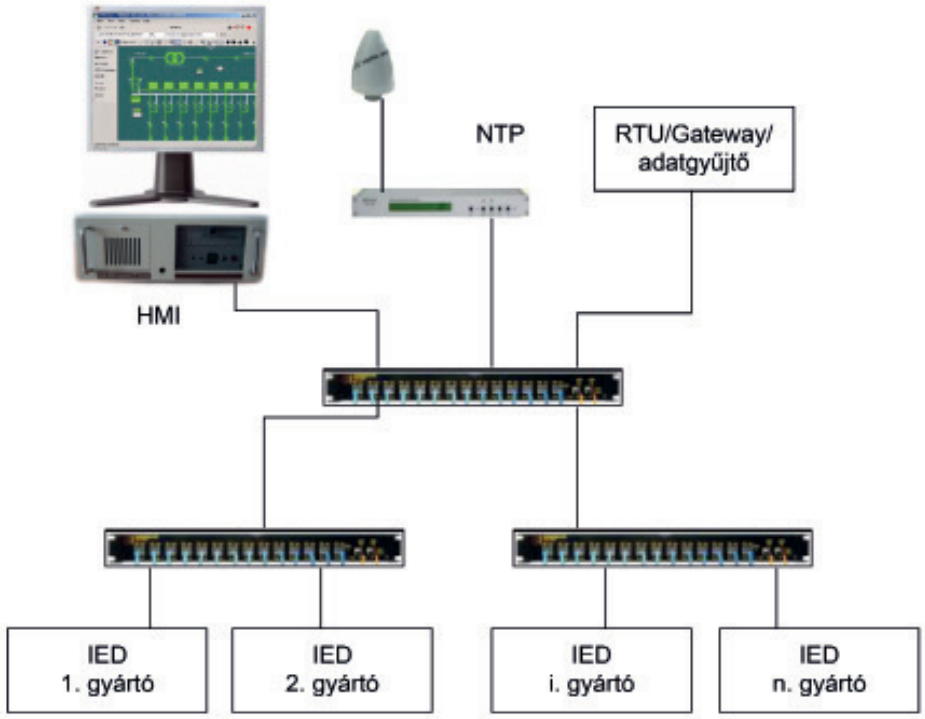
A folyamatosan gyorsuló technikai fejlődéssel a villamosenergia rendszer adatgyűjtése és irányítása is lépést tart, azzal a kikötéssel, hogy ez a rendszer csak azokat a technológiákat alkalmazza, amelyek a tesztelések során már bizonyítottak és üzembiztosak. Ezt a villamosenergia rendszer kritikus infrastruktúra minősítése adja.

Jelenleg hazánkban egy nagyobb átállás zajlik, melynek kitűzött célja a - legkésőbb 2000 környékén - beépített korábbi rendszerű védelmi és irányítástechnikai készülékek cseréje a nemzetközi és magyar területen is általánosan alkalmazott IEC 61850[253]-es szabványnak megfelelőkre. Ez a szabvány egy olyan kompatibilitást biztosító előírás, amely lehetővé teszi, hogy különböző gyártók védelmi és irányítástechnikai készülékei együttműködjenek protokollkonverzió nélkül. Alkalmazásával és egy megfelelően specifikált és kiépített Ethernet alapú adatgyűjtő hálózattal a védelmi és irányítástechnikai készülékek adatgyűjtése (jelzések, mérések, zavaríró felolvasás[254] stb.), vezérlése kialakítható és megnövelt üzembiztonsággal rendelkezik a korábbi rendszerekhez képest. Egy ilyen rendszer kiépítése során jóval kevesebb szekunder erősáramú kábelezésre, körvezetékre van szükség a korábbi szekunder rendszerekhez képest annak függvényében, hogy milyen funkciókat bízunk erre a technológiára. Általánosan elmondható, hogy a rekonstrukciók, új beruházások szinte kizárólag csak ennek a protokollnak megfelelően zajlanak a 6-750 kV feszültségszinteken; valamint már 2007 óta ilyen rendszerek üzemelnek ÁSZ, MÁV, MAVIR alállomásokon valamint az erőművekben, köztük a Paksi atomerőműben is.

Ebben a fejezetben már következetesen védelmi- és irányítástechnikai rendszerről beszélünk, mivel ha az IEC 61850-nek megfelelő szekunder rendszert egészében tekintjük, akkor a kettőt nem lehet szétválasztani. A szabvány pontosan definiálja a készülékek védelmi és irányítástechnikai specifikációit és funkciótól függetlenül megengedi, hogy egy Ethernet hálózatba kerüljenek (lásd. 12. ábra). Nem szükséges, de lehet külön hálózatot alkalmazni, ami annak a függvénye, hogy a megrendelő/üzemeltető milyen rendszert kíván felépíteni.

[253] IEC 61850 = International Electrotechnical Commission (IEC) által létrehozott nemzetközi szabvány a villamosenergia rendszerben alkalmazott védelmekre és irányítástechnikára specializálva https://www.ipcomm.de/protocols_en.html

[254] Zavaríró felolvasás = a digitális védelmek rögzítik - meghatározott feltételek teljesülése esetén (pl. zárlat érzékelése) - az előre meghatározott jelek nagyfelbontású (ms) időbeli lefolyását. Ezek lehetnek mért értékek (áram, feszültség) vagy jelzések (pl. védelem melyik funkciója indult) vagy működtetések (ki- be parancsok). Az így rögzített adatokat zavaríró regisztrátumnak nevezzük, amelyek létrejöttük esetén automatikusan a központi adatszerverekbe továbbítódnak. Ezeknek a regisztrátumoknak nélkülözhetetlen szerepe van egy meghibásodás, zárlat lefolyásának kiértékelése során.




*12. ábra - IEC 61850 alapú védelmi és irányítástechnikai rendszer vázlata*

A készülékek kommunikációs felülete, az alkalmazott adatmodellek is szabványosak, ezért a beépített készülékeket egységesen IED[255]-nek nevezzük. Az, hogy az adott rendszerben külön lesznek-e választva a készülékek vagy sem csak attól függ, hogy a készülék specifikációja mit határoz meg, illetve elsősorban az, hogy a rendszer megrendelője / üzemeltetője mit kíván megvalósítani az adott készülékben a rendelkezésre álló szabványos adatmodellekkel valamint, hogy a készülék számítási kapacitása valamint fizikai méretei mit engednek meg. Ez utóbbit a be/kimeneti és a mérőkártyák száma határozza meg, amely szoros összefüggésben van a IED-be integrált funkciók számával. Az előbb leírtakból adódik, hogy nem szerepel külön védelmi és irányítástechnikai készülék az V.12. ábrán sem, csak IED. Középfeszültségen (6 kV-35 kV) jellemző megoldás, hogy egy készülékben valósul meg a védelmi és az irányítástechnikai funkció is, mivel a kezelendő adatpontok (mérés, jelzés, vezérlés) kisebb száma ezt lehetővé teszi. Nagyobb feszültségszinteken a bonyolultabb primer kialakítás és az összetettebb kapcsolókészülékek miatt nem lehet egy készülékbe integrálni minden funkciót, így megmaradt a klasszikus védelem / irányítástechnikai mezőgép megkülönböztetés.

Egy tipikus IEC 61850-es készüléket mutat a 13. ábra.

[255] IED = Intelligent Electronic Device = intelligens elektronikus eszköz


*13. ábra – IEC 61850-es IED eszköz*

Mivel a korábbi rendszerek cseréje, korszerűsítése zajlik, elkerülhetetlen, hogy a mostani adatgyűjtő funkciót megvalósító IED-k a régebbi protokollokon is kommunikáljanak, akár adatgyűjtő (kliens), akár kiszolgáló (szerver) feladatot látnak el. Gyakran szükség van egy IEC 61850/korábbi protokoll konverter ideiglenes beiktatására, ami idővel - ahogyan az adott alállomás/villamos elosztó korszerűsítése zajlik - kikerül a rendszerből (lásd 12. ábra). Ennek az átfutási ideje néhány héttől több évig is terjedhet, mivel számos tényező befolyásolja: a megrendelő/tulajdonos hány lépésben akarja végrehajtani a rekonstrukciót (ez erőteljesen függ attól, hogy mennyi pénze van rá), mikor és milyen időtartamra lehet az adott primer részt kikapcsolni (erőmű esetében igazodni kell a blokkleálláshoz, nemzetközi távvezeték esetében a túloldali féllel leegyeztetett időponthoz és időtartamhoz), mekkora része kapcsolható ki egyszerre az érintett alállomásnak/villamos elosztónak.

Az Ethernet alapú – és főleg az IEC61850 szerinti – adatgyűjtő hálózatoknak igen lényeges rendszerelemei a csatolást biztosító switchek[256] (lásd. 14. ábra).

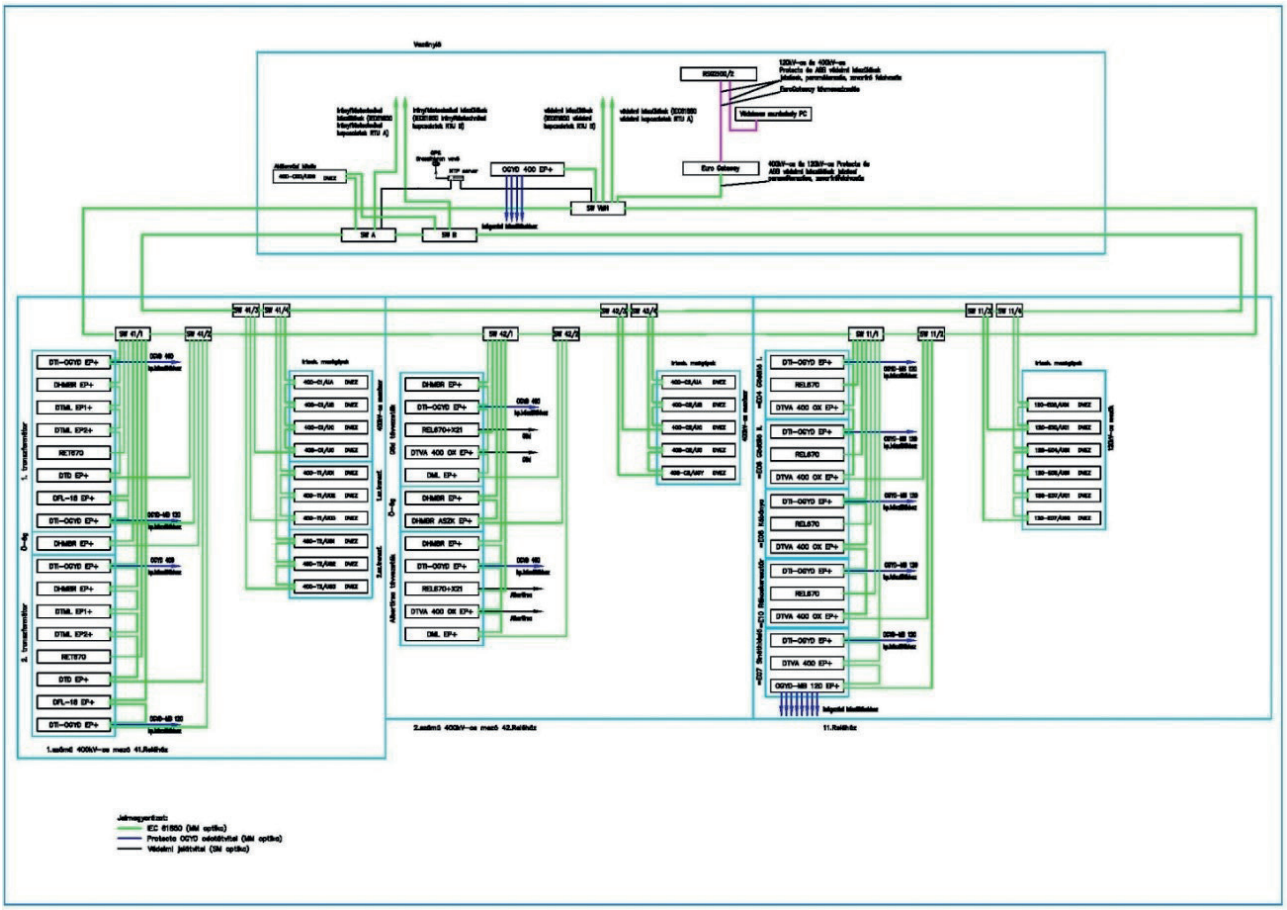
*14. ábra – Alállomási környezetben alkalmazott switch*

[256] switch = Ethernet alapú hálózat csatoló eszköz

Ezek az eszközök alakítják ki a fizikai hálózatot az IED-IED viszonylatban, amennyiben szükséges akkor helységek, épületek, telephelyek közötti optikai átkérők (lásd. 11. ábra) közbeiktatásával. Funkciójukat tekintve hasonlóak az otthoni internet hálózathoz csatlakoztatott switchekhez/routerekhez, de itt meg is áll a hasonlóság. Robosztus, alállomási környezetben érvényes EMC követelményeknek megfelelő, ipari kivitelű eszközök, kettős tápellátással, távmenedzselési funkciókkal, hotswap modulos felépítésűek és maguk is kezelhetők IED-ként. Optikai és (néha) réz patch kábelekkel csatlakoznak hozzájuk az IED-k.

*Nem szabad elfeledkezni arról, hogy az előbb felsorolt követelménynek a fizikai védelmét (EMC, ütés, csepp stb. állóság) szolgálják a hálózati eszköznek. A fizikai védelmen felül egy ilyen hálózati eszköznek kibervédelmi szempontból is védettnek kell lennie, mivel számos IED (és az abban definiált funkciók is!) közvetlen elérhetősége miatt potenciális célpont. A megfelelő eszköz (és gyártó) kiválasztás során figyelembe kell venni az adott eszköz (park) kibervédelmi funkcióit, amelyek közül alapvető a backdoor*[257] *lehetőségének kizárása. Kibervédelmi szempontból nem megfelelően védett eszközökre a legjobb példák a kommersz (igen olcsó) háztartási okosotthon termékek, amelyek csak alap védelmi lehetőségekkel bírnak (némely esetben azzal sem).*

Egy 400/120 kV-os alállomási adatgyűjtő hálózatra mutat példát az 15. ábra.



*15. ábra -400/120 kV-os alállomás adatgyűjtő hálózata*

[257] Backdoor = szoftver vagy rendszer amely lehetővé teszi, hogy a rendszergazda belépjen a rendszerbe hibaelhárítás vagy karbantartás céljából. Ugyanakkor jelenti még társaságok, hírszerző ügynökségek titkos hozzáférését adatokhoz, eszközökhöz tiltott tevékenység céljából. https://www.wired.com/2014/12/hacker-lexicon-backdoor/

Minden doboz egy – egy IED-t jelöl (bele értve az előbb említett switcheket is), a zöld vonalak pedig az IEC 61850-es hálózatot. Ennél az alállomásnál a megrendelő/üzemeltető külön védelmes és külön irányítástechnikai hálózatba szervezte az IED-ket. Mindegyik készülék multimódusú optikai kábellel kapcsolódik az adott épületben lévő adatgyűjtő switchez, amely hurkos kialakítással kommunikál a vezénylő épületben lévő központi egységekkel (RTU, Gateway), amelyek a külső kommunikációs irányokat is biztosítják (MAVIR, ÁSZ). A helyszíneket tekintve a kék vonalakkal határolt részek az egy épületen belüli (reléházak és vezénylő épületek) eszközök, közöttük az 11. ábrán látható optikai átkérőkön megy az összeköttetés. A két hurokban lévő eszközök a switcek, hozzájuk csatlakoznak a védelmi, irányítástechnikai, gateway, RTU és HMI funkciókat ellátó IED-k.

Mivel Ethernet alapú és nem pont-pont összeköttetésű rendszerről beszélünk, így minden küldött adatpontot pontos időbélyeggel kell ellátni, amit az egységes (általában GPS[258] alapú) NTP[259] szerverrel valósítunk meg. Az NTP által biztosított pontosság a jelenlegi rendszerekben megfelelő, de amennyiben az alkalmazott Ethernet kommunikációra időkritikus feladatot is rá kell bízni (pl. gyűjtősín védelmi kioldás), akkor majd a PTP v2 [260] (IEEE 1588-2002[261]) szerinti működő IED, switch, gateway, RTU és HMI eszközökre lesz szükség. Ez a közeljövőben (<5 év) várható az újonnan telepített vagy rekonstruált rendszerek esetén.

A villamosenergia rendszer felügyelete és irányítása során a technológiai fejlődést követve mind az alállomáson és erőművön belüli, mind pedig a távfelügyeletet/kezelést biztosító rendszerek TCP/IP alapú hálózati összeköttetéssel kommunikálnak. Az, hogy ez a fajta adatkapcsolat mennyire van elterjedve az adott szolgáltató/fogyasztó rendszerében attól függ, hogy mennyire új a létesítmény, illetve hol tart a védelmi és irányítástechnikai rekonstrukciója. De előbb vagy utóbb mindenhol a TCP/IP alapú kommunikáció fog megjelenni. Az, hogy ezen felül milyen protokollon (MODBUS TCP[262], IEC 60870-5-104, IEC 61850 és fizikai felületen (csavart érpár, mono/multi üveg optika, műanyag optika) zajlik az adatcsere, az ettől teljesen független. A technológia terjedésére egy jó példa a 16. ábra, ahol egy 400 kV-os alállomás távközlési kommunikációjának egyik központi rack szekrényében lévő csavart érpáras kábeleit láthatjuk. Ez a fénykép akár egy szerverteremben is készülhetett volna bármelyik IT[263] szolgáltatónál.

[258] GPS = Global Positioning System = globális helymeghatározó rendszer www.wikipedia.org

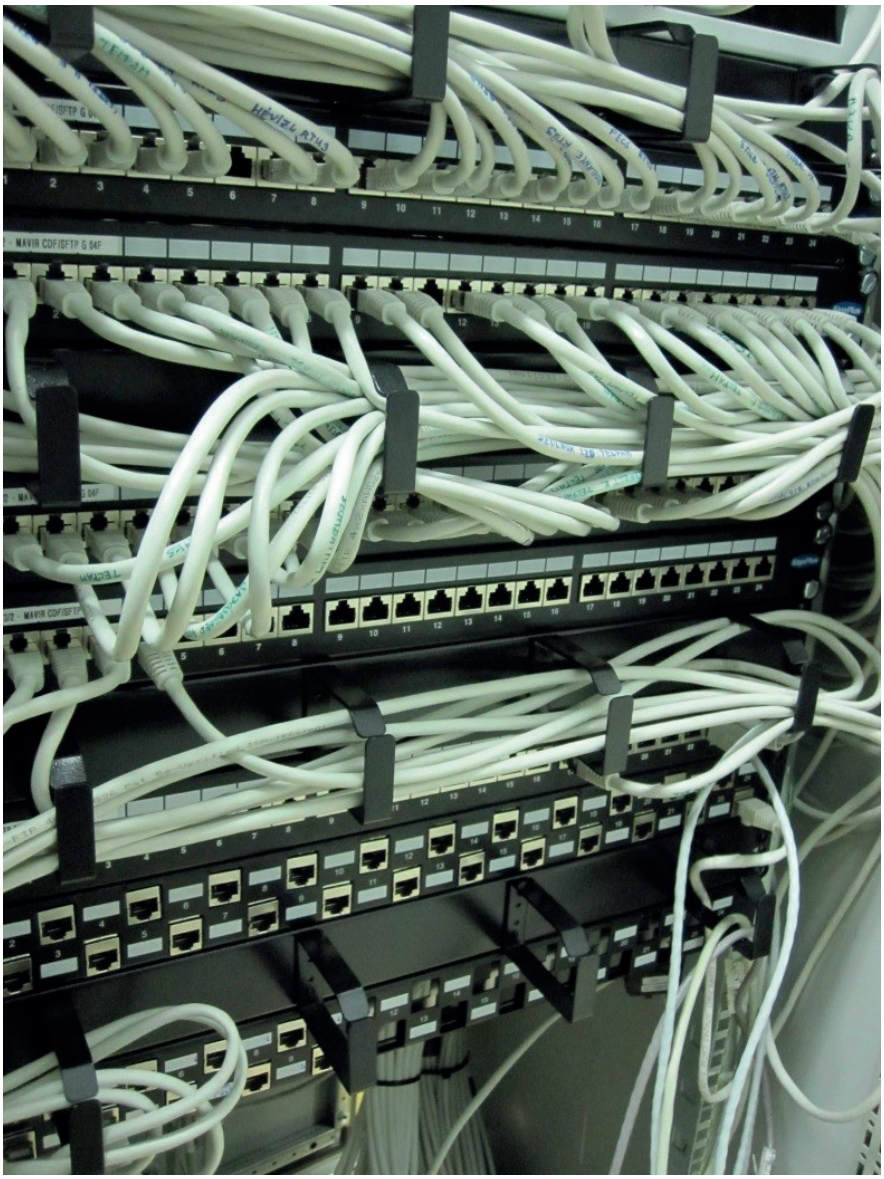
[259] NTP = Network Time Protocol = hálózati időalap protokoll www.wikipedia.org

[260] PTP v2 = Precision Time Protocol Version 2 = precíz idő protokoll, amellyel microszekundum nagyságrendű pontosság tartható a hálózati adatcsomagoknál www.wikipedia.org

[261] IEEE 1588-2002 = a PTP első verziója 2002-ben jelent meg, kisebb pontossággal www.wikipedia.org

[262] MODBUS TCP = TCP alapú MODBUS kommunikáció https://www.ipcomm.de/protocols_en.html

[263] IT = Information Technology



*16. ábra – Tipikus alállomási távközlési kapcsolatok*

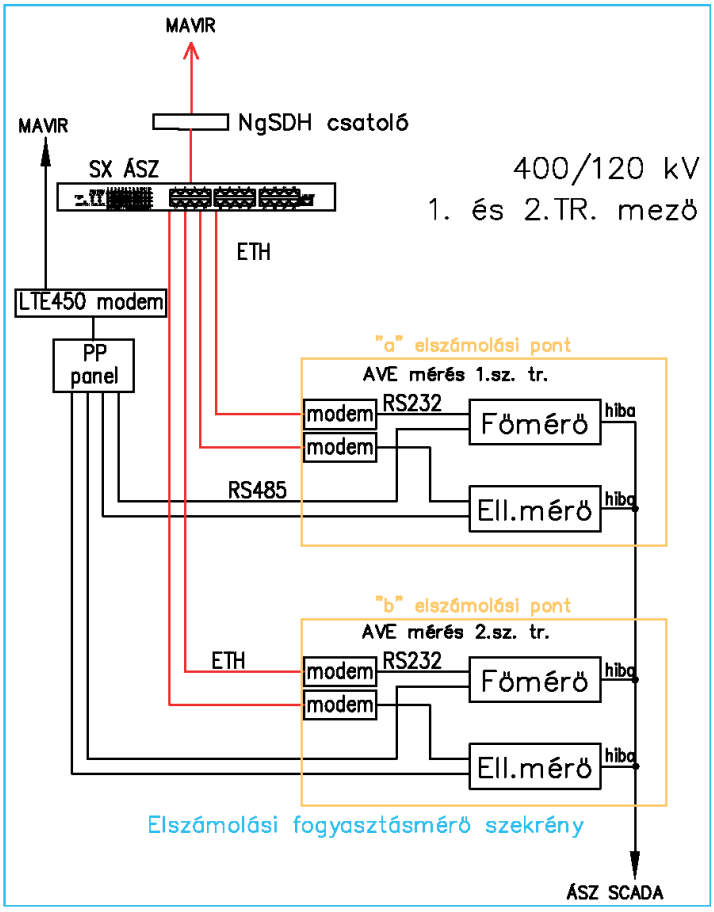
Minden – nagyobb - villamosenergia rendszer szereplőnek van saját adatgyűjtő központja - amely hasonlóan néz ki – így értelmet nyer az a megállapítás, hogy IT infrastruktúra és szolgáltatás nélkül nem létezik villamosenergia rendszer.

Az 5.2. és az 5.3. fejezetekben bemutatott irányítástechnikai és védelmi-automatika rendszeren felül TCP/IP szervezésű Ethernet alapú rendszert használnak az 5.4.3. fejezetben ismertetett – kiszolgáló – rendszerek is.

## *5.4.3. Kiszolgáló rendszerek kommunikációja*

### Elszámolási fogyasztásmérés

Ahogyan az 5.2.2.3.-as fejezet írta, a tényleges villamosenergia elszámolás utólagosan történik (a rögzítése folyamatos), amelyet törvényi előírások alapján a felek (ÁSZ, erőmű, MAVIR, kis- és nagy fogyasztók) üzemviteli szabályzatai rögzítenek. Az üzembiztos és folyamatos adatlekérdezéshez olyan adatgyűjtő struktúrát kell kialakítani, amely ezt biztosítani tudja. Ennek a kiszolgálására a korszerű fogyasztásmérők (nem a lakosságiak, amelyeket lásd. a [264] jegyzet III. fejezetében) több kommunikációs porttal (RS232[265]/RS485[266]) és relés (erősáramú) kontaktussal rendelkeznek. A helyszíni kiszolgáló hálózat tipikus felépítésére mutat példát a 17. ábra MAVIR-ÁSZ elszámolási mérési pont esetére.




*17. ábra – MAVIR – ÁSZ AVE fogyasztásmérés*

A két darab AVE[267] elszámolási mérési pont (sárga keret „a” és „b”, amik jelen esetben az alállomáson lévő 1. számú és 2. számú 400/120 kV-os transzformátorok) saját fő és ellenőrző fogyasztásmérővel rendelkezik. Az 1. lekérdező útvonal felépítése: a kommunikációs portok közül az RS232-k saját

[264] „Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – Kritikus információs infrastruktúrák védelme” című jegyzet
[265] RS232 = pont-pont szabványos soros kommunikáció www.wikipedia.org
[266] RS485 = buszrendszerű soros kommunikáció www.wikipedia.org
[267] AVE = Átviteli hálózati Villamosenergia Elszámolás

RS232/Ethernet modemre majd utána egy közösítő switchre (SX ÁSZ) kapcsolódnak. Az utána lévő Ng SDH[268] csatolóval az MVM NET[269] tulajdonában lévő (vezetékes) távközlési hálózaton keresztül jut el az információ a MAVIR-ban lévő MKP[270]-ba. A 2. lekérdező útvonal felépítése: az RS485 portjai a mérőknek egy PP (patch) panelen közösítődnek, majd az RS485/LTE450[271] távközlési modem felhasználásával (vezeték nélküli) kommunikációval jut el az információ a MAVIR MKP-ba. A relés kontaktusok közül – jelen esetben – csak a fogyasztásmérő belső hibáját jelző van használva, amely az ÁSZ SCADA rendszerébe küldi a jelzéseit.

Ezzel a kettős lekérdező hálózattal biztosított az elszámolás folyamatossága. Mivel a fogyasztásmérők FIFO[272] rendszerben tárolják a pillanatnyi mért értékeket, így amennyiben mindkét kommunikációs rendszerben egyszerre történne meghibásodás utólag is lekérdezhetők a hiányzó adatok. Az ÁSZ az elszámolási adatokat a MAVIR-tól kapja meg külön kommunikációs csatornán keresztül, amelyet a korábban említett üzemviteli megállapodások alapján kell kialakítani. A fogyasztásmérők hibajelzését a MAVIR részére az irányítástechnikai összeköttetésen keresztül adja át az ÁSZ.

Annak függvényében, hogy kik az elszámoló felek valamint, hogy a helyszínen milyen távközlési infrastruktúra érhető el a lekérdező hálózat kialakítása és struktúrája a .17. ábrán látottól eltérő is lehet.

### Telefon és üzemviteli hálózati kapcsolatok

Az Ethernet használata már a beszéd alapú vezetékes hálózatok esetében is szinte teljes körű. IP alapú telefonhálózatok épülnek(tek) ki, amelyek ugyanazt az alap távközlési infrastruktúrát használják, mint a korábban említett védelmi, irányítástechnikai és fogyasztásmérő rendszerek. Jellemzően minden épület minden fontosabb (huzamosabb tartózkodásra alkalmas) helységébe kerül vezetékes telefonkészülék, amely iparági telefonszámmal rendelkezik. A telefonhálózat zárt, külsős szolgáltató nem használhatja. Új, kisebb méretű és rossz távközlési infrastruktúrával rendelkező (leginkább magántulajdonú) létesítmények (pl. kisebb <500 kWp naperőművek) esetén nem kerül telepítésre vezetékes telefonhálózat. A mobiltelefónia egyre jobb lefedettségi mutatója és azt még jobban megnövelő – következő generációs - 5G (6G) hálózatok a vezetékes telefónia jogosultságát egyre jobban csökkentik.

### Vagyonvédelmi-, beléptető- és tűzjelző rendszer

Távkezelt (állandó személyzet nélküli) villamosenergia-ipari létesítményeknél szükséges vagyonvédelmi-, beléptető- és tűzjelző rendszer kiépítése. Annak függvényében, hogy kinek a tulajdonában van (magán, állami) illetve, hogy milyen méretű az energiatermelés vagy az átalakítás a - törvényi előírásokban / rendeletekben leírtakon felül - kiépítettség mértéke jelentősen eltér.

A legegyszerűbb a kis naperőműves rendszereké, amely általában 1 db BHTR[273] épületből és a napelemekből áll vagyonvédelmi kerítéssel körülvéve. Ebben az esetben egy alap kivitelű vagyonvédelmi- és behatolási rendszer kerül telepítésre (1-2 db fix kamerával), illetve egy ettől független tűzjelző rendszer. Mindkettő külön GSM alapú kommunikációval rendelkezik, átjelzéssel a szükséges központokba/felügyeleti rendszerekbe. Nagyobb naperőművek esetén több BHTR kerül telepí-

[268] Ng SDH = Next Generation Synchronous Data Hierarchy = nagy kiterjedésű szinkronjel alapú adathálózat új generációja
https://www.gta.ufrj.br/seminarios/semin2004_1/sonet/files/new_sonet_sdh_whitepaper2_en.pdf

[269] MVM NET = a Magyar Villamos Művek távközlési hálózati (NETwork) leányvállalata

[270] MKP = Mérési Központ, MAVIR, ÁSZ tulajdonú energia-elszámolási központ

[271] LTE 450 = Long Time Evolution (4. generációs vezeték nélküli adatátviteli hálózat) 450 MHz-es vivőfrekvenciával www.wikipedia.org

[272] FIFO = First In First Out www.wikipedia.org

[273] BHTR = BetonHázas TRanszformátor épület

tésre, illetve a lefedendő terület mértéke is nagyobb. Ez több kamerát, beléptetési pontot és tűzjelző érzékelőt jelent, így a helyi központok összetettsége is növekszik. Amennyiben rendelkezik vezetékes távközlési kapcsolattal a naperőmű, akkor a vagyonvédelmi átjelzést azon keresztül szokták megvalósítani a kameraképek jelentős sávszélesség igénye miatt.

Alállomások esetében a tulajdonos határozza meg, hogy milyen kiépítettségű (hány és milyen kamera, beléptető, tűzjelző) rendszer üzemeljen. A vagyonvédelmi- és beléptető rendszer egy közös központot kap, a tűzjelző ettől független. Az irányítástechnika irányába az üzemeltető központok (MAVIR, KDSZ) számára mindegyik központ küld – jelenleg – erősáramú átjelzést. Mivel a vezetékes távközlési rendszer – a legtöbb esetben – adott ezeken a helyszíneken, így a kötelező vezeték nélküli átjelzésen kívül előbbi kerül alkalmazásra, az előző bekezdésben már említett jelentős sávszélesség igény miatt.

### *5.4.4. Távközlési rendszer*

A személyzet nélküli, szinte teljesen autonóm működéssel bíró alállomási rendszerek üzembiztos felügyeletének a távközlési hálózat egy rendkívül kritikus része. Ennek az alapját a teljes országot lefedő optikai gerinchálózat alkotja, amelynek a túlnyomó része monomodusú 48-96 szálas OPGW[274]-ből vagy – urbánus környezetben – behúzókábelből[275] épül fel. A nehezen átjárható területeken (pl. ipari üzemek) kiegészítő kapcsolatra használnak pont-pont összeköttetésű mikrohullámú rendszert is. Ennek a gerinchálózatnak a tulajdonosa az MVM NET Zrt. és nem keverendő össze a kábel/internet/telefonszolgáltatók saját tulajdonú optikai hálózatával. Léteznek olyan OPGW-k amelyek a távvezetéket tulajdonló ÁSZ vagy nagyobb ipari fogyasztó (pl. MÁV) tulajdonában vannak, de a legjellemzőbb az MVM NET Zrt.-és.

Az optikai szálak felhasználásával 10Gbps[276]-os MPLS[277] hálózat, valamint Ng SDH hálózat van kiépítve országos szinten. Az MPLS hálózatot a tulajdonos üzleti célra (nem csak állami) bérbe adja az Ng SDH részt pedig a villamos energetikai cégek használják a 6. fejezetben tárgyalt védelmi jelátviteli, távkezelési, elszámolási mérési, telefon- és üzemviteli, vagyonvédelmi rendszerekhez. Amennyiben a védelmi jelátvitel direkt optikai összeköttetéses akkor egy szálpár (=2 db optikai szál a 48/96-ból, adás/vétel) kerül felhasználásra a két helyszín közötti OPGW-ből vagy behúzókábelből a jelátviteli berendezéseket direktben csatlakoztatva. Ez üzembiztonság szempontjából kiváló megoldás, de sávszélesség szempontjából viszont erősen pazarló, mivel az optikai szál több nagyságrenddel nagyobb sebességet és sávszélességet tud (>10 Gbps), mint amivel a védelmi jelátviteli berendezések (lásd. 5.2. fejezetet) X.21[278] (600[279]kbps-10[280]Mbps) vagy G.703[281]/E1[282] (2Mbps) protokolljai használnak. Ezen utóbbi protokollok illesztését az Ng SDH végberendezések alá befűzött (alacsonyabb sávszélességeket kezelő) UMUX[283] eszközök biztosítják szabványos csatolófelületeken.

---

274 OPGW = OPtical Ground Wire = optikai szálat tartalmazó szabadvezetéki védővezető www.wikipedia.org

275 optikai behúzókábel = földbe fektetett védőcsőbe behúzott optikai kábel

276 Gbps = Gigabits per second

277 MPLS = MultiProtocol Label Switching www.wikipedia.org

278 X.21 = X.21 (sometimes referred to as X21) is an interface specification for differential communications introduced in the mid-1970s by the ITU-T www.wikipedia.org

279 kbps = kilobits per second

280 Mbps = Megabits per second

281 G703 = ITU-T standard for transmitting voice or data over digital carriers such as T1 and E1 www.wikipedia.org

282 E1 = The E-carrier is a member of the series of carrier systems developed for digital transmission of many simultaneous telephone calls by time-division multiplexing. E1 line data is 2.048 Mbps www.wikipedia.org

283 UMUX = Universal Multiplexer

Mindegyik távközlési összeköttetés, amely az Ng SDH vagy az MPLS hálózaton megy keresztül - az alkalmazott protokoll redundanciáján felül - önmagában véve redundáns, mivel a végberendezések legalább két másik helyszínen lévő eszközhöz csatlakoznak, így biztosítva az egyszeres meghibásodás elleni védelmet.

Az állandó kezelőszemélyzettel rendelkező erőművek – és egyes ritka esetekben – az alállomások távközlési rendszerei hasonlóan épülnek fel, mint az előbb bemutatott személyzet nélkülieké azzal a különbséggel, hogy a távfelügyelt részek mértéke kisebb (pl. vagyon- és beléptető rendszer, távkezelt primer/szekunder kapcsolóberendezések, eszközök).

A vezetékes távközlési kapcsolat nélküli megújuló erőművek (elsősorban a <500kWp beépített teljesítményűek) esetében egyszeres kapcsolat van minden távkezelt/felügyelt rendszernél, attól a megoldástól eltekintve, ha két SIM kártyás modemet alkalmaznak, hogy a szolgáltatáskiesést csökkentsék. Minden rendszernek (SCADA, elszámolási fogyasztásmérés, vagyon- és behatolásvédelem, tűzjelzés) saját központja és modemes átjelző rendszere van.

# 6. DR. KRISKÓ EDINA: KRÍZISKOMMUNIKÁCIÓ KIBERTÁMADÁSOK ESETÉN

## 6.1. Bevezető gondolatok

Feltört eszközök, elérhetetlenné vált vagy összeomló weboldalak, megsértett hálózatok, szolgáltatások megtagadása, másolt e-mailek vagy ellopott bankkártya-adatok és más nem kívánatos számítógépes események… mára mindennapjaink részévé váltak. Események, amelyek nyilvánvalóvá tették, hogy egyetlen szervezet sem tud sebezhetetlen lenni, nincs teljes, megingathatatlan kiberbiztonság. A legtöbb szervezet éppen ezért mára már kifejlesztett bizonyos válaszképességeket kiber (IT) és más incidensek esetére, de azok zömmel csak a szűken vett informatikai kérdésekre és a rövidtávú válaszokra terjednek ki. A működésfolytonossági tervek[284] célkeresztjében az áll, hogy a szervezet képes legyen kritikus működési folyamatait *elfogadható szinten* fenntartani[285], így kerülve el, hogy a nem várt (biztonsági) esemény végzetes károkat (katasztrófát) okozzon. Az incidenskezelés[286], ha a hosszú távú hatásokat is szem előtt tartjuk ennél jóval tágabb területet ölel fel: számolni kell az esemény közvélekedésre gyakorolt hatásával, a szervezet reputációjának sérülésével.[287] Ez pedig már a szervezeti kommunikáció kompetenciaterülete. Ez azt jelenti, hogy az információbiztonságért felelős vezető számára elengedhetetlen a válságkommunikáció alapjainak ismerete. Ha nem is ő maga nyilatkozik, mert a közigazgatás hazánkban jelenleg erősen központosított kommunikációs gépezetében erre mondjuk nincs felhatalmazása, a nyilatkozattételért felelős személyeket és a „válság arcát" adó kommunikátort (kommunikátorokat) kell tudnia támogatni. Teheti ezt előzetesen és folyamatosan is megfelelő szakmai információk adásával, a szervezet és különösen a válságstáb (nem kizárólag a kiberincidensek esetére kijelölt válságstáb) rendszeres képzésével, tájékoztatásával, illetve utólagos szakmai kontroll biztosításával.

---

284 vagy üzletmenet-folytonossági terv, BCP – Business Continuity Plan

285 HORVÁTH Gergely Krisztián (2014): Incidens-menedzsment, BCP, DRP integráció A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez, NKE, Budapest.

286 Mivel a szakirodalomban és a jogi normákban is találkozunk a biztonsági esemény-kezelés és incidenskezelés fogalmak szinonimként való használatával, (ahogyan markáns elkülönítésével is) (Fehér, 2018) jelen tananyagban mi is rokon értelműekként alkalmazzuk az említett lexémákat. Annál is inkább, mivel a kríziskommunikáció a válságmenedzsment azon elvéből indul ki, hogy kompetenciája körébe tartozik mindenféle *labilis* szituáció (Fekete-Sándor, 1997), amely az események előrehaladásától, későbbi lefolyásától és az eseménykezeléstől függően válhat később gonddá, problémává, krízissé vagy akár katasztrófahelyzetté (Nyárády-Szeles, 2004).

287 Mossburg, Emily-Gelinne, John-Calzada, Hector (2016): Beneath the surface of a cyberattack A deeper look at business impacts, Cyber Risk, Deloitte, https://www2.deloitte.com/kh/en/pages/risk/articles/beneath-the-surface-of-a-cyberattack.html, (etöltés. 2019. augusztus 12.

## 6.2. A tananyag célja, tartalma

Jelen tananyagfejezet a válságkommunikáció témakörét járja körül. Összegzi azokat a szakmai alapvetéseket, amelyek keretét adják a (közszolgálati) szervezeti kommunikációnak kibertámadások (és más nem kívánt biztonsági események) esetén. Ehhez merít a kommunikációelmélet, a krízismenedzsment és a kríziskommunikáció irodalmából, valamint sorra veszi a különféle hazai és nemzetközi szakmai szervezetek állásfoglalásait. Végezetül pedig esettanulmányokon keresztül mutatja be, mit tehet az információbiztonságért felelős vezető, hogy ne csak az incidenskezelés, de annak külső és belső kommunikációja is professzionális és eredményes, mi több, hatékony legyen.

A képzés során az információbiztonságért felelős személyek megismerhetik a válságkommunikáció fogalmát, célját, eszközrendszerét és munkamódszerét. Áttekintést kapnak a kibertámadások esetén lehetséges és ajánlott retorikai stratégiákról, a szervezeti külső és belső kommunikációval szemben támasztott követelményekről.

Jelen terjedelemben túlzás volna azt állítani, hogy a fejezet átfogó képet ad vagy letisztult szintézise a ma rendelkezésre álló ismereteknek, ugyanis ez idő szerint igen karcsú még a kibertámadások kommunikációjának szakirodalma. Egyelőre kérdésként fogalmazódik meg, hogy kell-e, lehet-e és mit kommunikálni a szervezeteknek önnön sebezhetőségükről. A PR szakma persze azt mondja, lehet és kell, sőt, teljeskörű kommunikációt kell folytatni, az IT szakemberek legtöbbje azonban bizonyára azt mondja, nem szoktuk az ablakba tenni, ha károkat szenvedünk el, és végképp nem hívjuk fel a figyelmet arra, hol vagyunk sebezhetőek. A biztonságpolitikai szakértőket sem igen halljuk amellett érvelni, hogy széleskörű publicitást kellene biztosítani a kritikus infrastruktúrákat és kritikus információs infrastruktúrákat érő támadásoknak. Persze a kommunikációs szakma sem azt mondja, hogy a műhelytitkokat kell nyilvánossá tenni. Annyit mond, hogy a szervezet (külső és belső) nyilvánosságokkal fenntartott kapcsolata életbevágó, nélküle egyetlen szervezet társadalmi elfogadottsága és integrációja nem remélhető. A PR maga is elzárja műhelytitkait a kíváncsi szemek elől, a nyilvánossággal és a nyilvánosságért dolgozik, de szakmai fogásait homályban kívánja hagyni, amíg lehet. Ha még a közösségi média korában egyáltalán lehet...

A hosszú távú bizalomra épülő sajtókapcsolatok alapja azonban mindenképpen az, hogy a szervezet a jó és rossz híreket is menedzseli, azok közlésében és keretezésében vezető szerepet vállal.[288] Hiszen amíg így tesz, ő szabja a közlések hangvételét, ő irányít, ő a hiteles, a tömegből elsőként kihallatszó hang. Válság idején sincs ez másként. Ha a szervezet jól kommunikál, képes befolyásolni azt, ahogyan a közvélemény az adott (kiber)eseményt észleli és amilyennek az események közepette a szervezet helytállását ítéli. Ha a szervezet azt akarja, hogy a válságról kialakuló kép tükrözze saját álláspontját, vállalnia kell a nyilvánosságot. A szervezeti kommunikációmenedzsment azonban ma már nem „csupán" tájékoztatás és imázsépítés, hanem jóformán nyilvános diplomácia, társadalmi felelősségvállalás, nemes ügyek középpontba állítása és sikerre vitele is egyben.[289] Ekként kell tehát elhelyeznünk az információbiztonság és a kibereseményekkezelésének kérdéseit a szervezet stratégiai kommunikációjában. (Remélve, hogy a kommunikációs stratégia az átfogó szervezeti stratégia integráns része.)

[288] Nyárády Gáborné-Szeles Péter (é.n.): *Public Relations I-II.* (II. kötet), Perfekt, Budapest.
[289] Holstein, William D. (2011): Médiaszelidítők, Akadémiai Kiadó, Budapest.

## 6.3. A válságkommunikáció alapjai kiberbiztonsági területen

### *6.3.1. Mivel foglalkozik a válságkommunikáció?*

Sellnow és Seeger (2013) gyakorlati tapasztalataikat és szakirodalmi ismereteiket összegezve úgy fogalmaznak, hogy a válságok közös jellemzője: a nagyfokú bejósolhatatlanság vagy a várakozásokkal való erőteljes ütközés, az események magas prioritású célokat veszélyeztető jellege és – a károk kiküszöbölésének, illetve mérséklésének érdekében – a relatív gyors válaszok adásának követelménye.[290] A válságkommunikáció tehát ilyen események teljeskörű kommunikációmenedzsmentje. Mivel a kibertámadások, de más (információ)biztonsági események kezelése is megköveteli az azonnali figyelmet és a válaszadást, a kárfelmérés és -enyhítés mechanizmusainak haladéktalan beindítását, „helyben vagyunk". A válságkommunikáció szakterülete maga úgy tekinti, hogy kompetenciaterületébe tartozó eseménnyel állunk szemben és szükséges a válságkommunikáció elveinek és eszközeinek alkalmazása kibertámadások esetén.

A kibertámadások – mint válságok – a szakírók tipológiái szerint több kategóriába is sorolhatók. Tekinthetjük őket technológiai válságoknak vagy rosszindulatból eredő válságoknak, de éppen így lehetnek terrorcselekmények, vagy szolgáltatáskrízisek, netán kihívások és vezethetnek technikai összeomláshoz, üzemzavarhoz. Ha azonban nem egyszeri kibertámadásról van szó, hanem háborús összecsapásról (kiberhadviselés), akkor az események besorolása már a konfrontációtól a megakárokig igen széles sávon mozog. Ha a támadók célja a rendszerhamisítás vagy rémhírterjesztés, megint más kríziskategóriaként tekinti a válságkommunikáció. Majd minden szerző külön nevesíti a szervezet saját alkalmazottai által okozott válságait[291] (az olyan belső fenyegetéseket, mint a szabotázs, hiba, mulasztás, munkahelyi erőszak stb.). (lásd. 1. sz. táblázat)

Amennyiben a támadás a kritikus infrastruktúra valamely eleme(i)[292] ellen irányul, már a gazdasági krízisek vagy ipari válságok, netán szállítási katasztrófák rémképe sejlik fel. Még színesebb a „válságpaletta", ha a támadást szélesen értelmezzük, és beleértjük „a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is."[293] Ennek megfelelően a válságkommunikáció is igen széles horizonton mozog, a közvetlen vagy közvetített kétszemélyes kommunikációtól (pl. a személyes vagy telefonos, vagy internetes és online panaszkezeléstől) kezdődően a társadalmi kommunikáción (pl. átfogó lakossági tájékoztatás) át a nemzetközi kommunikációig (pl. kormányzati kommunikáció vagy a szupranacionális szervezetekkel és azokon keresztül folyó kommunikáció).

---

290 SELLNOW, Timothy L.-SEEGER, Matthew W. (2013): Theorizing crisis communication, Wiley-Blackwell, West-Sussex. UK.
Ezzel összecsengően Fekete Ferenc és Sándor Imre 1997-ben megjelent és a hazai szakirodalomban a mai napig meghatározó könyvükben úgy fogalmaznak, hogy minden válságjelenségben megvan 4 összetevő, nevezetesen: van kiváltó ok, fenyegetettséggel kell szembenézni, azonnali figyelem érvényesítése szükségszerű és nem kontrollálható események is zajlanak. (Fekete-Sándor, 1997, 44)

291 Nem csoda, a Kaspersky Lab felmérései szerint 2017-ben a kiberincidensek mintegy 46%-át a (zömmel nem informatikai területen alkalmazott) dolgozók okozták. https://profitline.hu/Az-europai-szervezetek-79-a-szeretne-tudni-hogy-ki-az-oket-ert-kibertamadas-elkovetoje-391128, letöltés: 2019. augusztus 26.

292 Energia előállító, tároló és szállító rendszerek (gáz, olaj, villamos energia); közmű szolgálatok rendszerei (víz, csatorna); távközlési rendszerek; banki- és pénzügyi hálózatok; vészhelyzeti szolgálatok (tűzoltóság, rendőrség, katasztrófavédelem); közlekedés; kormányzati rendszerek (Kovács, 2015, 15), valamint az egészségügy létfontosságú létesítményei és rendszerei (Kovács, 2018, 19)

293 Muha Lajos – Krasznay Csaba (2014): Az elektronikus információs rendszerek biztonságának menedzselése, NKE VTKI, Budapest, 14. o.

| Lerbinger (1997) | Seeger, Sellnow és Ulmer (2003) | Coombs (2010) |
|---|---|---|
| természeti katasztrófák | a közvélemény észlelései | természeti katasztrófák |
| technológiai válságok | természeti katasztrófák | rosszindulat okozta válságok |
| összeütközés, konfrontáció | termék vagy szolgáltatás krízisek | technikai összeomlás, üzemzavar |
| rosszindulatból eredő válságok | terrorcselekmények | emberi hiba |
| szervezeti vétségek | gazdasági krízisek | kihívások |
| munkahelyi erőszak | emberierőforrás krízisek | megakárok |
| rémhírek | ipari válságok | szervezeti vétségek |
| terrorcselekmények | kiömlések, szennyezések | munkahelyi erőszak |
| ember okozta katasztrófák | szállítási katasztrófák | rémhírek |
| | környezeti tényezőkből eredő krízisek | |

*1. sz. táblázat: A válságok típusai*
*Forrás: saját szerkesztésű és fordítású ábra*[294]

*A válságkommunikáció* tulajdonképpen nem más, mint a hatóságok, a szervezetek, a média és az érdekelt személyek, illetve csoportok közötti információcsere, amely a válságesemény előtt, alatt és után történik. Az információáramlás három dolog körül összpontosul: a tényleges válság, a válság kezelésének folyamata, a válság (különféle közvéleménycsoportokban és különböző szintű nyilvánosságokban kialakuló) képe.[295]

Kibertámadásokról lévén szó, jelen tananyag az infokommunikációs létesítmények, eszközök és szolgáltatások elleni kibertérben[296] kiberfegyverekkel[297] elkövetett károkozási célú támadásokra és az azok folytán keletkező *labilis szituációk* (mint potenciális válságesemények) kommunikációjára fókuszál.

A kommunikációs szakemberek és a sajtószóvivők számára, de olykor még a cégvezetők számára sem világos, hogy milyen konkrét eseményekre gondoljunk, amikor kibertámadásról esik szó. Az informatikai és információbiztonságért felelős vezetőnek e téren is támpontot kell nyújtania a közlemények megfogalmazásában és sajtóhoz való eljuttatásában közreműködőknek, vagyis a médiakapcsolati csapatnak. Nem szabad megfeledkezni arról, hogy ők lesznek azok, akik mind a laikus közvélemény, mind a szakmai sajtó tájékoztatásáért felelnek, (hacsak nem maga az információbiztonsági vezető a nyilatkozattevő személy). A sajtókapcsolati csapatot még békeidőben edukálni kell a kiberbiztonság témájában. Számukra tehát a legérthetőbb módon kell megadni milyen eseménynyel állunk szemben, s az incidens bekövetkezésekor nekik már ismerniük kell, mi az egyes események specifikuma, jelentősége. Azért, hogy az információk sajtóképessé/médiaképessé váljanak, a kommunikációs csapat felel majd.

294 Sellnow-Seeger, 2013. i.m. 6. o.
295 *Crisis Communication Handbook*. SEMA's Educational Series 2003:1, Swedish Emergency Management Agency, Stockholm.
296 Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket és beágyazott processzorokat, vezérlőket. (Krasznay-Muha, 2014. i.m. 110.)
297 károkozásra képes hardver és szoftvereszközök

A kommunikációs csapat számára tehát alapvető fogódzót jelentenek az olyan megkülönböztetések, mint hogy:

- kiberterrorizmussal
- hacktivizmussal
- kiberbűnözéssel vagy
- kiberháborúval kell-e szembenézni.[298]

Persze ez nem azt jelenti, hogy ne árnyalhatnánk számukra a képet, ha saját szervezetünk speciális tevékenységet végez vagy valamilyen speciális védelemmel van ellátva és az incidens bekövetkezésekor a fentiektől eltérő megnevezés használata indokolt. Azt azonban fontos tudni, hogy ha az eseményt valamely megjelöléssel ellátjuk, sajtóhírként már végérvényesen hozzátapad az adott *címke* és így „ég bele" a közvélemény tudatába.

Legyen ez az első kommunikációs feladat, nevezzük meg az eseményt! A sajtókapcsolati csapat és nyilatkozók nem élhetnek homályos körülírásokkal, ha el akarják kerülni, hogy találgatások kapjanak szárnyra.

## *6.3.2. A válságkommunikáció célja*

A válságkommunikáció és a reputációmenedzsment alapvetően a szervezet szemszögéből értékel és cselekszik, (ahogyan az információbiztonság is) a kiberbiztonság azonban szervezetközi együttműködést tételez.[299] A kommunikációs feladatokban is megjelenik ez a kettősség kibertámadások esetén. Egyrészt ugyanis ki kell védeni a támadást, vissza kell állítani a normál működést szervezeti szinten, ami hatékony belső és külső szervezeti kommunikáció nélkül nem lehetséges, másrészt a támadást – a kiberbiztonság fogalmából eredően/levezethetően[300] – a kibertér biztonsága/megbízhatósága elleni cselekményként kell tekinteni. Ez azt jelenti, hogy a támadásban érintett szervezet a kibertér más aktorai iránt is felelősséggel tartozik, információit a további károk elkerülése érdekében (haladéktalanul?) meg kell osztania velük. Gyűjteni és kölcsönösen megosztani kell valamennyi szereplőnek a rendelkezésre álló műszaki információkat, proaktívan keresni kell a potenciális fenyegetéseket (threat hunting), be kell kapcsolódni a digitális bűnfelderítésbe és az exploit fejlesztésbe. Támadás észlelése esetén pedig riasztás kiadására van szükség. (Abban az esetben, ha komolyan vesszük a kitételt, mely szerint a nemzeti együttműködés rendszerében értelmezzük a kiberbiztonságot és hosszú távon a nemzeti ellenállóképességet és a szabályozási környezetet akarjuk fejleszteni, megalapozni a kellő kibertudatosságot, erősíteni a (kiber)biztonsági kultúrát.)[301]

A válságkommunikáció feladata, hogy időzített, pontos, releváns, a szervezeti célokkal összhangban álló, azokat támogató információkat juttasson el a különböző közvéleménycsoportokhoz. Coombs ugyanakkor megjegyzi, hogy a válságkommunikációs aktivitásokat két nagy csoportra célszerű bontani, *információk menedzselésére* és *jelentések menedzselésére*. Információk nélkül nem kezelhető a válság, nem hozhatók meg a szükséges döntések, nem lehet végrehajtani az intézkedéseket. A felkészülés és megelőzés szintén körültekintő információkezelést tételez. A jelentések adása azonban más jellegű folyamatokat takar. Ez által befolyásolja a szervezet a stakeholdereit, érdekgazdáit. A jelentések menedzselése határozza meg, hogy válság esetén az érintettek (mind a külső,

[298] Quigley, Kevin-Burns, Calvin-Stallard, Kristen (2015): 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection, Government Information Quarterly 32 (2015) 108–117.

[299] Krasznay Csaba (é.n.): Információbiztonság vs. kiberbiztonság – az okos város szempontjából, NKE Kiberbiztonsági Akadémia, Budapest. https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf, letöltés ideje: 2019. augusztus 3.

[300] lásd. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § (1) 26

[301] Uo. 5.

mind a belső érintettek), hogyan érzékelik a fenyegetéseket, hogyan látják a válságot, az arra adott válaszokat és milyennek ítélik a szervezet helytállását.[302] Avagy a jelentések menedzselésétől függ, hogy milyen az információk (tények) (közvélemény általi) olvasata.

## *6.3.3. A válságkommunikáció (mindenkor érvényes) alapelvei*

### 6.3.3.1. Kiberincidens volt, van és lesz!

A legfrissebb kiberbűnözési és kiberbiztonsági statisztikák adati szerint ma már az adatok elvesztése, ellopása vagy megtámadása a leggyakoribb támadás a cégek, szervezetek ellen, a korábbi évtizedet uraló fizikai támadásokkal szemben. 2018-ban mintegy 137,5 millió új kártevőmintát regisztráltak, 2019-ben csak áprilisig már 24,55 millió mintát. 2018-ban a megfigyelt rosszindulatú programoknak már mintegy 93%-a volt polimorf.[303] Az egyszer már megfertőződött eszközöknek pedig mintegy a fele egy éven belül újra megfertőződik.[304] A rosszindulatú hackerek minden 39. másodpercben indítanak valamilyen támadást számítógépek és/vagy hálózatok ellen.

A számítógépes bűncselekmények az előrejelzések szerint 2021-ig globálisan évente mintegy 6 billió dollár kárt fognak okozni. Mindazon szervezetek számára, akik nem akarnak e károk elszenvedőivé válni, komoly intézkedéseket kell foganatosítaniuk. „Megmenekülésük" záloga a gyors (minden korábbinál gyorsabb) információfelvétel és az azonnali reagálás lesz/lehet.

A válságmenedzsment alapfeltevése, hogy előbb vagy utóbb minden szervezet életében felüti a fejét valamilyen válságesemény. Lehet az egészen csekély, a napi működést alig befolyásoló történés, de lehet akár végzetes katasztrófa is. Éppen ezért a legfontosabb a felkészülés és a megelőzés, amelynél (költség)hatékonyabb kezelési mód nemigen létezik. A válságkommunikáció egyik mantrája is ez: Légy felkészült! Legyen terved! Legyen válságstábod!

### 6.3.3.2. Mindig a lehető legrosszabb eshetőséggel számoljunk!

Sajnos a válságesemények nem arról nevezetesek, hogy végül a jobbik forgatókönyv lép életbe, de ha mégis, micsoda megkönnyebbülés! Ha a legrosszabbra készülünk, azt jelenti, hogy nagy körültekintéssel vesszük számba az összes lehetséges veszélyforrást és kockázatot, és válaszadási képességünk jóval kedvezőbb, mintha arra alapoznánk a felkészülést, hogy nagy baj úgysem történhet. A „túlzott" óvatosságot megbocsátja a közvélemény, a felelőtlenséget, a közönyt vagy az elbizakodottságot nem.

### 6.3.3.3. Legyen válságtervük!

A terv legyen aktuális, időről-időre felülvizsgált és kipróbált! A szervezet vezetése számára ez folyamatos szellemi kihívást és ugyanakkor szakmai naprakészséget jelent. E tervnek legyen kidolgozott szerves része a kommunikációs terv, hiszen a legjobb krízisválaszokat is alááshatja a rossz kommunikáció. Fordítva sajnos nem igaz: jó kommunikáció nem tud semmissé tenni meghozott rossz vezetői döntéseket, hibás válaszlépéseket. A kritikus információs infrastruktúrák védelme kommunikációjakor itt kitüntetett figyelmet kell kapnia azon jogi megfontolásoknak, hogy mikor kivel milyen információt oszthatunk meg. A válság közepén annak mérlegelése, hogy valamely közléssel jogsértést követünk-e el, már nem megengedett időveszteséggel járna.[305]

---

[302] Coombs, Timothy W. (2012): *Ongoing Crisis Communication. Planning, Managing and Responding*, SAGE, Thausend Oaks, California.

[303] kódját folyamatosan megváltoztatni képes, hogy megakadályozza a felismerését

[304] Zaharia, Andra (2019): 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2019 EDITION], https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/, letöltés ideje: 2019. július 11.

[305] INSA, 2018. 11. o.

#### 6.3.3.4. Ne vesztegessük az időt!

A tervek ezért is kellenek. Megadják számunkra, mik az első kötelezően megteendő intézkedések és azok kinek a felelősségi körébe tartoznak. Ilyen kommunikációs intézkedés lesz például az esemény azonnali bejelentése[306]. Bármilyen csekély vagy általános információt adunk is az incidensről, ha megtesszük, azzal jelezzük a közvélemény felé, hogy észleltük az eseményt és kezeljük a helyzetet, vállaljuk a nyilvánosságot. A felelősségvállalás és a transzparencia olyan üzenetek, amelyek minden körülmények között növelik az állampolgárok szervezetbe vetett bizalmát. Jóindulatuk megnyerése segít a későbbiek során a kellemetlen üzeneteket elfogadtatni azáltal, hogy a befogadók érzelmileg és tudatilag is nyitottabbakká válnak, meghallják az érveket, könnyebben azonosulnak az érzelmi üzenetekkel. (A közzététel kihívásait és a közlés ellen szóló érveket lásd a alfejezetben a …. sz. táblázatban). Ez az első közlés lehet sajtótájékoztató vagy átmeneti nyilatkozat. (Mindkettőről lesz még a későbbiekben szó.)

#### 6.3.3.5. Minden esetben az ember legyen az első!

A válságkezelés legfontosabb üzenete, hogy az incidens által érintett emberek (károsultak) érdekei állnak a középpontban. Elsődleges prioritás az ő védelmük, biztonságuk, minden más (szervezeti, politikai, gazdasági stb.) érdek csak azután következik. A szervezet vezetőjének vagy a szakterület felelősének ki kell állnia az emberek (a sajtó nyilvánossága) elé és el kell mondani, hogy érti és átérzi a károsultak aggodalmait, és el kell mondani, hogy milyen konkrét lépéseket tesz a szervezet a védelmükben.

#### 6.3.3.6. Reagáljunk villámgyorsan!

Ez mind a válságkezelésre, mind a válságkommunikációra érvényes követelmény. A szervezeteket ugyanis legalább olyan szigorúan ítélik meg kríziskommunikációjuk alapján, mint a válság (megtörtént incidens) alapján.

### *6.3.4. A legfőbb kérdések*

A kríziskommunikációtól 3 területen várunk el felelős információáramoltatást:

1) Adjon tájékoztatást, informáljon oly módon, hogy az egyes egyén cselekvési kompetenciája az információk birtokában növekedjen (a kapott információ alapján legyen képes felelős döntést hozni jövőbeni cselekvéseit illetően)! Lásd példának okáért a 2018. május 28-ai sajtóközléseket, melyek szerint 54 ország mintegy 500 ezer routerét fertőzték meg orosz hackerek.[307] Az újságírók arra buzdítottak mindenkit, ellenőrizzék, hogy otthoni eszközeik a 14 fenyegetésnek kitett típus valamelyikébe tartoznak-e. Említhető azonban az NKI heti sajtószemléje is.
2) Járuljon hozzá a véleményalkotáshoz (oly módon, hogy kommentál, összefüggésekbe ágyaz, segít megérteni a tényeket, oksági és más kapcsolatokat és fontossági sorrendet állít fel, prioritásokat jelöl ki)! Lásd. pl. a SANS OUCH! Sötét Webről írt lapszámát.[308]

---

306 Szem előtt tartva a jogszabály azon kitételét, mely szerint csak abban az esetben, ha a közlés nem hátráltatja a kármentés

307 https://hvg.hu/tudomany/20180525_orosz_hacker_cisco_router_vpnfilter_virus_kibertamadas, letöltés ideje: 2019. augusztus 11. (Érdekes, hogy a Nemzeti Elektronikus Információbiztonsági Hatóság (korábbi) weboldalán ez csak június 11-ei riasztásként van fent (http://neih.gov.hu/alerts?page=6, letöltés ideje: 2019. augusztus 11.).

308 https://nki.gov.hu/wp-content/uploads/2019/06/201906-OUCH-June-Hungarian-P1.pdf, letöltés ideje: 2019. augusztus 11.

3) Közüggyé tegyen, társadalmasítson, olyan témákat, amelyeket jelentőségüknél fogva társadalmi diskurzusokban kell (célszerű) megvitatni! Lásd. pl. az NKI Biztonságos internet használatról szóló kiadványát.[309]

A kommunikáció hiánya válságok idején elszigetel, s ekkor a közvélemény információéhségétől hajtva alternatív (akár kevésbé megbízható, kevésbé hiteles vagy elfogult) hírforrásokhoz fordul. Egyetlen szervezetnek sem jó, ha fél információk, pletykák, rémhírnek kelnek szárnyra. A kommunikáció ugyanakkor a közösségformálás és társadalmi összefogás eszköze, amelyre a szervezet építhet a helyreállításban.[310]

A legfőbb kérdések megegyeznek a kommunikáció alapkérdéseivel: Ki? Mit? Kinek? Milyen csatornán? Milyen hatással közöl? (Lasswell-paradigma)

A kommunikáció alapkérdéseit egy nem várt kibertámadás újabbakkal tetézi:

- Mit teszünk, ha éppen leggyorsabb és legnagyobb kontaktusszámot biztosító kommunikációs csatornáink, vagyis az online rendszereink nem elérhetőek?
- Hogyan reagálhatunk a bekövetkezett vészhelyzetre, ha digitális csatornáink leállnak?
- Hogyan lehet ilyen körülmények között megfelelni az azonnali reagálás és a kommunikáció irányítása követelményének?

Vészhelyzet esetén a hatékony kommunikáció létfontosságú. Amikor az informatikai rendszerekben hiba lép fel, a szervezetnek akkor is képesnek kell lennie, hogy saját személyi állományával, a veszélyelhárításában résztvevőkkel kommunikáljon, koordinálja a tevékenységeket, a válaszlépéseket. Minél nagyobb késedelmet szenved mindez, annál nagyobb hatása lesz (lehet) a válságnak. Egy sikeres kibertámadás több kommunikációs csatornát is érinthet. Ha a telefon- és hangpostarendszer VoIP-alapú, akkor a szervezet a telefonos kapcsolattartás eszközét is elveszítheti. Amennyiben a dolgozói forródrót is áthalad a hangrendszeren, az is elveszhet. A házon belül üzemeltetett honlap is elérhetetlenné válhat. Ha a törzshálózat sérül, a felhasználók elveszítik a hozzáférésüket a szervezeti adatokhoz, megbénul a munkavégzés, kapcsolattartás.[311] (Hawkins, 2017) Olyan alapvető folyamatok is ellehetetlenülnek, mint a szükséges dokumentumok kinyomtatása, sokszorosítása stb. Veszélyhelyzetben égető szükség van a dolgozók és más érintettek elérhetőségeire, a tervdokumentumokra és a veszélyelhárítás szempontjából nélkülözhetetlen más (a szervezeti elektronikus adatbázisokban tárolt) információkra, a sajtókapcsolati listákra, a médiaadatbankra.

### *6.3.5. A válságkommunikációs terv*

Az egyesült-királyságbeli önkormányzatok szövetsége (Local Government Association) összegyűjtött ajánlásait[312]:

Mindenekelőtt alkossunk válságkommunikációs tervet még „békeidőben". Ne csak elektronikusan tároljuk, őrizzünk belőle nyomtatott példányokat is. Munkaeszközként fognak funkcionálni a válságstáb tagjai számára, ezért legyen elérhető több példány. (Nem kell sok, de sokszorosítással tölteni az időt komoly veszteség, amikor minden perc számít.)

---

309 https://nki.gov.hu/wp-content/uploads/2019/03/20_Biztonsagos-internethasznalat.pdf, letöltés ideje: 2019. augusztus 11.

310 Kriskó Edina (2013): Szervezeti kommunikáció, NKE VTKI, Közigazgatási Vezetői Akadémia, ÁROP-2.2.13., tréning tananyag, Hatékony vezetés modul, Vezetői kommunikáció almodul, NKE, Budapest.

311 Hawkins, Nick (2017): Why communication is vital during a cyber-attack, *Network Security*, March 2017, pp.12-14.

312 https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis, letöltés ideje: 2019. június 20.

Természetesen a válságkommunikációs terv a szervezet átfogó válságkezelési tervébe illeszkedik, annak részeként kerül kidolgozásra. Mindenképpen tartalmaznia célszerű:

- a válságkommunikációs stáb tagjainak adatai (név, beosztás, elérhetőség, elérhetetlenség esetére a helyettes tagok adatai)
- a stábtagok találkozóinak ütemterve a válság első néhány órájára, napjára vagy hetére
- az üzenetek (közlések, közlemények) jóváhagyására jogosult személyek
- a válság esetén elérendő célcsoportok listája, beleértve a kapcsolattartási adatokat
- az érdekgazdák listája, akiket válság esetén el kell érni és/vagy akikkel együtt kell dolgozni, beleértve a kapcsolattartási adatokat
- azoknak a csatornáknak a listája, amelyeken keresztül az üzeneteket a szervezet közvetíteni fogja
- azoknak a jelszavaknak a másolatai, amelyekkel a szervezeti kommunikációs csatornák elérhetők.

Az önkormányzatok szövetsége nem említi, de a válságkommunikációs terv kardinális eleme, hogy ki nyilatkozhat vagy kinek kell nyilatkoznia. A válságot megelőzően kell – szilárd stratégiai elvek mentén – lefektetni a szóvivők, nyilatkozók körét. Ez két okból fontos: egyrészt életveszélyes hazárdjáték olyan szakembert kamerák elé állítani, aki bár a saját szakterületének elismert tekintélye, a nyilatkozatadásban rutintalan. Másrészt az egyébkor szakértői szerepben szívesen tetszelgő vezetőknek – a tapasztalatok szerint – nem feltétlenül akarózik a nyilvánosság elé lépni, ha baj van, ha a felelősségi körükbe tartozó hiba, mulasztás vagy annak csak lehetősége merül is fel. Ha megvan a kijelölt vezetői, szakértői kör, annak tagjait ugyancsak a prekrízis szakaszban rendszeresen felkészíteni, tréningezni kell.

### *6.3.6. Készenlét, válasz és helyreállítás*

A kiberkrízisekhez való megfelelő preventív hozzáállás teszi lehetővé, hogy a válságkezelés, már a számítógépes incidensek megtörténte előtt elkezdődjön, s a felmerülő probléma, ne kizárólag informatikai kihívásként kerüljön definiálásra. A hatékony válságkezelés és -kommunikáció ennél jóval több. A válságkommunikáció (is, hasonlóan más menedzsmentdiszciplínákhoz és gyakorlatokhoz) az előtte, alatta és utána hármasában gondolkodva határozza meg a feladatait.[313] Ezt írja le a *készenlét, a válasz és a helyreállítás* követelménye.

*A készenlét* nem csak egyfajta általános éberséget jelent, mint például 0-24 órás monitoringot, hanem az erőforrások készenléti állapotát is. A válságstábnak, mint multifunkcionális csapatnak, készen kell állnia, hogy bármikor kezelje egy incidens vagy válság minden aspektusát. A készenlét egyúttal azt is jelenti, hogy a stábtagok fel vannak készítve, ki vannak képezve a válságeseményekre: válságtréningeken, krízis-szimulációkban vesznek részt. (Deloitte, 2016) A tréningen gyakorolják a válságkezelési protokollokat, fejlesztik a vezetők döntésképességét, próbára teszik a szervezet és személyzet felkészültségét.

*A válaszadás* azért is érzékeny terület, mert önmagában is válsághelyzet, ha a válasz nem megfelelő, fokozhatja a válságot, további nem kívánatos folyamatokat gerjeszthet. A határozott jól koordinált válaszok azonban mérsékelhetik az idő-, pénz- és ügyfélveszteséget, a reputációvesztést és a helyreállítási költségeket. A szervezetnek a médiumok teljes körét lefedően készen kell állnia arra (beleértve a közösségi médiát is), hogy valamennyi érintett felé kommunikáljon és a helyzetének megfelelő hiteles választ adjon a felmerülő kérdésekre.[314]

---

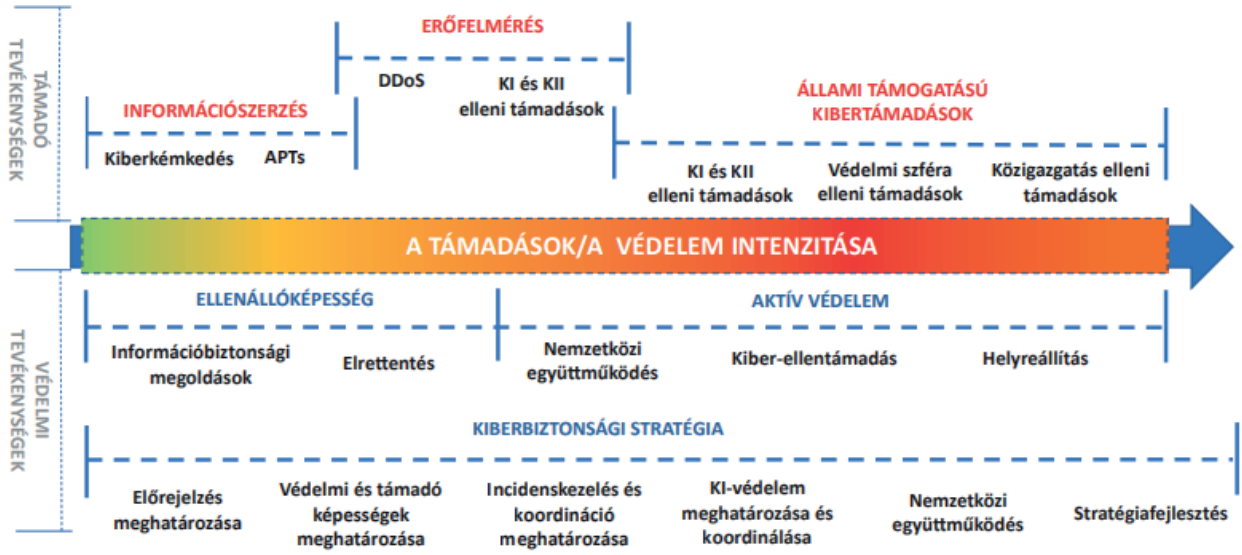
[313] A válságkommunikáció irodalma ismer azonban többlépcsős modelleket is. Aki a saját szervezete számára más válságkommunikációs modellt tart szükségesnek, haszonnal fordulhat Fink négylépcsős és Turner hatlépcsős modelljéhez. Lásd. Sellnow-Seeger, 2013. i.m. 33-40. o.

[314] Uo.

*A helyreállítás* az a folyamat, amellyel a szervezetet és érintettjeit visszavezetjük a normál szervezeti működéshez, a keletkezett kárt helyrehozzuk és lehetőség szerint nem is visszatérünk az eredeti állapothoz, hanem annál jobb állapot elérésére törekszünk. A helyreállítás szakaszában már van idő és mód az okok részletes feltárására, a válságintézkedések értékelésére és tapasztalatok, tanulságok összegzésére. A kibertámadások korában mindez azt jelenti, hogy egy biztonságos, éber és ellenálló szervezetet kell kiépíteni, amely minden időben és szituációban képes (az azonnali és) a rugalmas reagálásra.

### 6.3.6.1. A prekrízisszakasz

A részletes kommunikációs feladatok áttekintéséhez célszerű Kovács (2018) ábráját felhasználni és megnézni, hogy a kiberhadviselés egyes műveletei során milyen tájékoztatási igények merülnek fel. Az ábra alkalmas arra, hogy levezessük a kiberbiztonsággal kapcsolatos általános és rendkívüli helyzetekben szükséges kommunikáció feladatait és céljait.




*1. sz. ábra: A kiberhadviselés lehetséges műveleteinek időbeni lefolyása és azok lehetséges elemei*
*Forrás: Kovács, 2018, 30. o.*

Az ún. prekrízis szakaszban természetesen az előrejelzésen és megelőzésen van a hangsúly, ám ez nem jelent némaságot. Üzeneteket ekkor is megfogalmazhat és gyakorta meg is kell, hogy fogalmazzon a szervezet. Az ún. előremenekülési retorikai stratégiák lényege éppen az, hogy már békeidőben is lehet felkészültségeket és veszélylehetőségeket kommunikálni. Amikor és ahogyan a szervezet megszervezi információbiztonságát, kialakítja annak technológiai, műszaki megoldásait és humánerőforrás támogatását, már üzenetet fogalmaz meg ellenállóképességéről. Nyilvánvalóan a szervezet belső közvéleménye számára az információ direktebb és közvetlenebbül hozzáférhető lesz (a szervezeti dokumentumok és napi rutinok által), de a külső nyilvánossághoz is elérnek üzenetek. Gondoljunk csak az információbiztonságért felelős vezető kinevezésére, s annak sajtóbeli megjelenésére vagy külső cég megbízásakor az együttműködési szerződés nyilvánosságára. Közbeszerzéseknél már önmagában a kiberbiztonsági megoldások szállítására szánt összeg is sokatmondó.

A veszélyek kommunikálása éppen így nem elhanyagolható. Ha a lehetséges fenyegetések tudata „benne van a levegőben", az érintettek számolnak vele, bekövetkezésük esetén, már nem kell azt magyarázni, hogyan is fordulhatott elő az adott káresemény. Mentegetőzés és hosszas okfejtés helyett lehet a kárenyhítésre koncentrálni. A „benne volt a pakliban" tudat, „tudtuk, hogy megtörténhet" üzenetek persze csak akkor működnek, ha melléjük tudjuk tenni, hogy milyen előzetes intézkedéseket tettünk, milyen terveink, eszközeink, módszereink voltak talonban erre az eshetőségre. Vagyis voltak-e, vannak-e és kommunikáltuk-e a védelmi képességeinket valami módon? Szóltunk-e korábban az információbiztonsági megoldásokról, amelyeket bevezettünk? Folytattunk-e elrettentő kommunikációt?[315]

Mikor alkalmazható stratégia az előremenekülés? Minden olyan alkalommal, amikor valami újat próbálunk, amikor elhagyjuk a járt utat: amikor technológiaváltás van, amikor eszközcserék zajlanak, amikor új termékek, szoftverek jelennek meg, próbaüzem vagy átfogó rendszerfrissítés van, amikor innovatív megoldásokkal kísérletezünk, amikor tanuló üzemmódban vagyunk. Ez utóbbi mindig jól alkalmazható kommunikációs fogás, de meg kell neveznünk, milyen tudással lettünk gazdagabbak az incidens bekövetkezésével, mennyivel visz ez minket előre az úton. (Tanulópénzként sok minden „eladható" a közvéleménynek, de nem minden. Általunk előidézett katasztrófa (besorolású) esemény nem.)

A válságkommunikációs tervek elkészítésekor szerencsére nagymértékben támaszkodhatunk (és támaszkodnunk is kell) az informatikai kockázatfelmérés és elemzés eredményeire. Bármely módszertannal is történjen ez, választ kapunk olyan kérdésekre, minthogy:

- Milyen típusú kockázatokkal, fenyegetésekkel kell számolnia a szervezetnek?
- Mi az egyes kockázatok bekövetkezésének valószínűsége?
- Az egyes események bekövetkezésekor milyen mértékű (és értékű) kárral kell számolnunk?
- A releváns bekövetkezési valószínűségű események milyen előrelátható becsült kárt okoznak?
- Mi az adott kockázat kezelésének módja, mi az adekvát védelmi intézkedés (kerülés, csökkentés, megosztás vagy áthárítás, kockázatvállalás)?[316]

Ez egyúttal azt is jelenti, hogy van egy sor olyan információnk, aminek a nyilvánosság próbáját kiálló üzenetté formálásáról még „békeidőben" határozhatunk. Ugyanígy a felkészülési időszak fontos kiinduló dokumentuma az incidenskezelési terv (IRP).

Minden szervezet számára biztonsággal kommunikálható üzenettartalom, hogy a szervezet milyen szervezeti és/vagy regionális és/vagy hazai és/vagy nemzetközi tanúsítási vagy egyéb szabvány(ok)nak felel meg.[317] Ez tényként, akár mindenfajta kommentár nélkül is alkalmas arra, hogy növelje a szervezet iránti bizalmat. Hordozza annak üzenetét, hogy a szervezet gondot fordít az elektronikus információbiztonságra. Ennél óvatosabb üzenet, ha különféle szakmai ajánlások figyelembevételére hivatkozunk.

A közvélemény emellett nyilván elvárja – jól tudván, hogy egy gyorsan változó és minden nap akár új kihívást hozó környezetben kell helytállnunk -, hogy elmondjuk, folyamatosan monitorozzuk a működésünket és folyamatosan fejlesztjük a védelmi képességeinket. Ugyancsak a felkészültség hatását erősítő üzenetek, amelyek a szakmai párbeszédben való részvételünket demonstrálják (szakmai szervezeti tagságok, K+F tevékenységek, szakmai érdekképviselet stb.), folyamatos tanulási hajlandóságunkat mutatják (elvégzett tanfolyamok, megszerzett képesítések, tanúsítványok, szakértői címek). Nem beszélve az elnyert díjakról, elismerésekről, szóljanak azok akár a szervezeti megoldásoknak, akár az azokért felelős személyek szakmai munkájának.

---

315 Itt nem kizárólag arra gondolunk, hogy egyrészről olyan kibervédelmi megoldások kialakítása történik meg, amelyek áttörése nem, vagy csak komoly erőforrások segítségével lehetséges, illetve, hogy ellenséges kibertámadásra válaszul támadó képességeket építünk ki (Kovács, 2018, 29), hanem, hogy ezen lépéseknek milyen mértékben szervezünk publicitást. A publicitásszervezés elkövetett vagy elhárított támadás esetében is elrettentő erővel bír(hat). Minden esetben stratégiai kommunikációs kérdés az esemény és hatásainak bemutatása.

316 László Gábor (2014): Kockázatértékelés, kockázatkezelés, NKE, Budapest.11-21. o.

317 Szádeczky Tamás (2014): Információbiztonsági szabványok, NKE, Budapest, 7-8. o.

### 6.3.6.2. Az aktív kríziszakasz

A legintenzívebb kommunikációs időszak az *aktív krízisszakasz*, amikor a nem kívánt számítógépes esemény/információbiztonsági esemény/ kiberesemény, -cselekmény megtörténik (vagy még zajlik, vagy éppen bekövetkezett a kár). A közvélemény azonnali reagálást, válaszokat, de legfőképpen cselekvést vár. A szervezet tehát érintettjeivel szavakkal és tettekkel kommunikál. S a tettek mindig erősebbek a szónál. Hallani és ma már mindinkább saját szemével látni akarja a közvélemény, hogy mit teszünk. A valósidejű kommunikáció korában a hír/médiafogyasztó részese akar lenni a történéseknek, szavak helyett bizonyítékot és élményt vár. Nem elég az informatikai probléma kezelése, kell a komplex válságkezelés/incidenskezelés, a (tudomány és) menedzsmentterületek összefogásával. (A konkrét kommunikációs üzenetekről és a lehetséges retorikai stratégiákról a következő fejezetben lesz szó.)

Válság idején első és legfontosabb a kríziskezeléshez szükséges belső szervezeti információknak a hatékony áramoltatása, a krízis felszámolásában résztvevők (válságstáb) értesítése és folyamatos kapcsolattartásának biztosítása. Ezt követi az érintettekkel való kommunikáció fontosságuk sorrendjében (elsőként a meghatározó, utánuk a veszélyes, a függő és a domináns stakeholderek, majd a követelőző, a diszkrecionális és alvó stakeholderek[318]). A világ számos táján lefolytatott krízisgyakorlatok aláhúzzák annak fontosságát, hogy a szervezet megértse érintettjei információigényét. Ezért is fontos a kétoldalú kommunikáció kialakítása, hogy az érintettek információs igényeiket jelezni tudják. (Ha a kormányzat például elhallgat információkat a támadások forrását, motivációját illetően megnehezít(het)i, hogy az ipar és kiberszakma képviselői hatékonyan lépjenek fel a további károk elkerülése érdekében vagy a potenciálisan érintett rendszereket és hatásokat – netán az elkövetői kört - beazonosítsák[319].) Mivel számolni kell a kommunikációs csatornák sárülésével, kiesésével, alapvető cél a redundáns kommunikáció biztosítása. Sokféle csatornán, ismétlődően biztosított információk, hogy azok biztosan eljussanak az érintettekhez.

*A kommunikáció legfőbb célja, hogy megértés alakuljon ki a társadalmi környezetben.* Ehhez pedig tisztességes, egyenes és következetes információkra és azok közzétételének helyes időzítésére van szükség. A szervezet, amely ezt elfogadja, lerántja a titokzatosság fátylát, feltárja a helytelen információk rétegeit, kiszorítja a pletykát és a spekulációt, hogy teret adjon a tényeknek.[320]

A közbizalom fenntartása érdekében valamennyi szereplőnek gyakran és átláthatóan, illetve megbízhatóan kell kommunikálnia, így elkerülhetővé válnak az információs túlterhelések is. A megfelelő széleskörű tájékoztatás lehetővé teszi, hogy a specialisták a legfontosabbakra az emberi élet és egészség védelmére, a biztonság (illetve kritikus infrastruktúra elemek) helyreállítására koncentrálhassanak. A felelős kommunikáció segít, hogy a közvéleményben reális elvárások fogalmazódjanak meg a szolgáltatások helyreállításával kapcsolatban és elősegítheti annak megvitatását, hogy miben, mivel segíthetnek az állampolgárok.[321]

Szükséges továbbá a kommunikáció központosítása, hogy a közvetített üzenetek következetesek, korrektek legyenek és kiszűrhetővé váljanak a helytelen, megtévesztő információk, melyek szárnyra kapnak. Adott szervezet nevében történő nyilatkozatadásra szóvivőt kell kijelölni. Kibertámadások esetén jó, ha ez a személy szakértőszóvivőként állhat a nyilvánosság elé (tehát kiberbiztonsági szakértő, illetve információbiztonsági felelős médiajártassággal).

---

318 Mitchell, Ronald K.- Agle, Bradley R.- Wood, Donna J. (1997): Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts, The Academy of Management Review, Vol. 22, No. 4 (Oct., 1997), pp. 853-886.

319 INSA, 2018, 13. o.

320 Fekete-Sándor, 1997. i.m. 127. o.

321 INSA, 2018. 15. o.

#### 6.3.6.3. A posztkrízis szakasz

Az ún. posztkrízis szakaszban a hosszú távú helyreállítás folyamatain van a hangsúly. A helyreállítás szakasza időben igen tág keretek között mozoghat, súlyos válságeseményeknél hónapokat is felölelhet (természetkárosító ipari katasztrófák azonban évekig, évtizedekig elhúzódó helyreállítási folyamatokat tehetnek szükségessé). A PR törekvése igen ambiciózus: nem is az eredeti állapotot, hanem annál kedvezőbbet érjünk el! Azt kell üzennie a szervezetnek, hogy egy következő lehetséges támadás már jóval felkészültebben érné. El kell érni, hogy a stakeholderekben pozitív nyomot hagyjanak a szervezet válságkezelési erőfeszítései, biztosítani kell őket arról, hogy a válság valóban véget ért.[322]

A szervezeti kommunikáció nem ér véget ott, ahol az IT biztonsági tevékenységek visszaterelik a szervezetet a normál működésbe. A szervezeti kommunikációnak azt is követnie kell, hogyan halad az okok, hatások, elkövetők kilétének felderítése, van-e gyanúsított, a hatóság kezdeményezett-e eljárást, történt-e letartóztatás, az igazságszolgáltatás gépezete hol tart, születik-e elmarasztaló ítélet stb. (Még akkor is, ha kibertámadások esetében igen ritkán olvasunk erről szóló médiabeszámolókat.)

A háromlépcsős modell kríziskommunikációs mantrája az *odafigyelés, kárenyhítés és megnyugtatás.* (Anthonissen, 2009) Az események egyes szakaszában ezt várja a közvélemény.

Összességében és egy mondatban úgy fogalmazhatunk: Nem elég, ha a rendszereink biztonságosak, úgy is kell tűnniük, hogy azok.[323]

## 6.4. Válságkommunikációs lehetőségek Magyarországon

### *6.4.1. A közszektor megközelítései*

A kritikus infrastruktúrák kijelöléséért és védeleméért felelős nemzeti ügynökségek (NCIPA) és a kritikus (információs) infrastruktúra üzemeltetők között szoros, mindkét fél erőfeszítéseit figyelembe vevő és elismerő együttműködés szükséges a sikeres és hatékony kritikus (információs) infrastruktúra védelem (CIP/CIIP) megvalósítása érdekében. Ahhoz például, hogy az NCIPA-k elláthassák hatósági felügyeleti feladataikat, információkat kell kapniuk a kritikus infrastruktúrák üzemeltetőitől. Az NCIPA-k visszajelzései (beleértve a fenyegetés-tudatosságot és a szakmai ajánlásokat) pedig az üzemeltetők számára jelentenek fontos információt vagyonuk védelmében.[324] Elmondható, hogy a kétirányú rendszeres kommunikáció már az incidenseket megelőző időszakban kiemelt jelentőséggel és a prevencióban közvetlenül érvényesülő hasznokkal bír. Mégis, az üzemeltetők (szolgáltatók) gyakorta vonakodnak együttműködni, és csak a jogszabályokban előírt minimum követelményeknek tesznek eleget. Ahogyan az egyes országok egyre több tapasztalattal rendelkeznek a CIIP terén, egyre inkább rá kell jönniük, hogy a közszféra nem képes minden időben biztosítani az összes szükséges kritikus infrastruktúra eszközt, ezért tevékenységében az üzemeltetők támogatására és a szakmai tanácsadásra célszerű inkább összpontosítania. Miközben bővíti saját kapacitásait a monitorozásban és biztosítja a korai figyelmeztetések nemzeti szintű rendszerét, a közszektor fontos szerepet játszik az információk valamennyi infrastruktúra-üzemel-

322 Coombs, 2012. i.m. 12. o.

323 Quigleya, Kevin-Burnsb, Calvin-Stallarda, Kristen (2015): 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection, Government Information Quarterly, Volume 32, Issue 2, April 2015, p.108-117.

324 Zaballos, Antonio García -Jeun, Inkyung (2016): Best Practices for Critical Information Infrastructure Protection (CIIP) Experiences from Latin America and the Caribbean and Selected Countries, Inter-American Development Bank and Korea Internet & Security Agency, Washington, 51-52.o.

tetővel való megosztásában. Információkkal, tanácsadással növelheti más aktorok rezilienciáját[325] a (kiber)támadások elleni fellépésben.

A magánszektorral fenntartott kapcsolatok sarokköve a bizalom, amelynek kiépítésére mintegy 10-15 éve volt már az egyes országoknak, de az együttműködések további elmélyítése folyamatosan napirenden van. A közszféra erős partner lehet a magánszektor számára, ha figyelembe vesszük, hogy a nemzeti és regionális szinten ösztönözheti a tudományos életet, célzott kutatásokat és fejlesztéseket támogathat, ezzel saját döntéshozatali kapacitásait is erősíti.

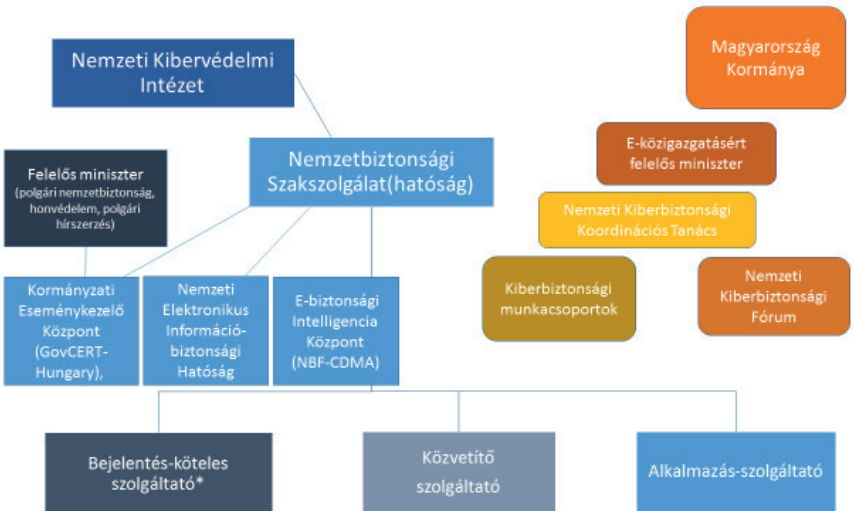
A partneri struktúrák hatékonyságát nagyban elősegítheti, ha vannak felkészült kapcsolattartók a két szektor (magán és közszektor) között.[326] Az ágazati megközelítés a partnerségi struktúrákban ugyancsak növelheti a hatékonyságot. A mérések, a monitorozás és a szakmai megbeszélések során a magánszektor is társvezetővé, koordinátorrá léphet elő. Az ágazati munkacsoportok hozzájárulhatnak a nemzeti és ágazati CIP tervek előkészítéséhez és végrehajtásához és a folyamatos információmegosztás révén a közösségépítéshez.

A kritikus infrastruktúravédelem nemzeti szintű rendszeres rendezvényei, valamint az aktuális kérdések megvitatására szolgáló rendszeres ágazati összejövetelek elősegítik a CIIP napirend megállapítását és rámutathatnak, hol kell erőfeszítéseket tenni. Ezen struktúrák révén megvalósulhat a nemzetközi együttműködés és a szakmai tapasztalatcsere a CIIP területén.

Be kell vonni az akadémia és a kutatóközösséget: A sebezhetőség és a kockázatok felmérése, valamint minden egyéb nagyobb analitikus munka jelentős kutatási kapacitást igényel, amely általában nem áll rendelkezésre az állami intézményekben. A minőségi CIIP-terveket márpedig nem lehet ilyen tudományos alap nélkül megépíteni. E helyen nem soroljuk fel az egyes aktorok jogszabályokban lefektetett feladatait, csak utalunk rá, hogy a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján megjelölt stratégiai célok mindegyike aláhúzza a felek szoros együttműködésének szükségességét, melyet a stratégia az 1.1 pontjában maga is külön nevesít.

[325] A kiber reziliencáról részletesen lásd pl. Understanding Local Cyber Resilience. A guide for local government on cyber threats and how to mitigate them, March 2015 Department for Communities and Local Government, London.

[326] Zaballos-Jeun, 2016. i.m. 58.o.




** az Országgyűlés Hivatala, az Alkotmánybíróság Hivatala, az Országos Bírósági Hivatal és a bíróságok, az ügyészségek, az Alapvető Jogok Biztosának Hivatala, az Állami Számvevőszék, a Magyar Nemzeti Bank, a fővárosi és megyei kormányhivatalok, a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalai, a hatósági igazgatási társulások, a Magyar Honvédség*
*** az ábrán nem jelöltük külön, de a stratégiai irányítás keretrendszerének része a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság, amely az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt elektronikus információs rendszerek vonatkozásában lát el hatósági feladatokat, illetve az MTA SZTAKI, amely Az Információbiztonsági törvény hatálya alá nem tartozó elektronikus információs rendszerek, hírközlési szolgáltatók tekintetében működtet eseménykezelő szervezetet (előbbieken kívül a Kormányzati Informatikai Fejlesztési Ügynökség működtet számítógépes biztonsági eseménykezelő szervezetet)*

*2. sz ábra: A kiberbiztonságért felelős aktorok*
*Forrás: saját szerkesztésű ábra*

A zártcélú elektronikus információs rendszerekkel kapcsolatos rendelkezésekről lásd a187/2015. (VII. 13.) Korm. rendeletet.[327] Rendészeti területen a zárt rendszert működtető szerv vezetője, honvédelmi területen a Katonai Nemzetbiztonsági Szolgálat főigazgatója, külpolitikai területen a felelős miniszter, a polgári hírszerzést felügyelő miniszter irányítása alatt a rendszert működtető szerv vezetője az eljáró hatóság.

A kritikus információs infrastruktúrák globális összekapcsoltsága azt jelenti, hogy a kibervédelem nem állhat meg a nemzeti határoknál, hiszen egyetlen gyenge láncszem veszélyt jelent a világ más nemzeteinek kritikus információs infrastruktúrájára.[328] Ezért – ahogyan azt az NBSZ és NKI weboldalán is olvashatjuk – ugyancsak magas prioritást élveznek a nemzetközi szakmai kapcsolatok más országok CERT-jeivel, és az olyan nemzetközi kibervédelmi szervezetekkel, mint: az ENISA[329], a FIRST[330], a TI[331], az IWWN[332] vagy a Közép-Európai Kiberbiztonsági Platform[333].

327 http://njt.hu/cgi_bin/njt_doc.cgi?docid=176705.363342, letöltés ideje: 2019. augusztus 12.
328 Luiijf, Eric-Schie, Tom van-Ruijven, Teo van-Huistra, Auke (2016): *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers*, TNO, Rijswijk, Netherlands, https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf, letöltés: 2019. augusztus 21.
329 European Network and Information Security Agency
330 Forum of Incident Response and Security Teams
331 Trusted Introducer
332 International Watch and Warning Network
333 Central European Cyber Security Platform (Visegrádi Négyek és Ausztria kiberbiztonsági szervezeteit tömörítő platform)

## *6.4.2. A jogi normákba foglalt kommunikációs feladatok (kötelezettségek)*

Az Alaptörvény VI. cikkének (3) bekezdése[334] kimondja, hogy Magyarországon mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez. Az információs önrendelkezési jogról és az információszabadságról szóló törvény 3.§-a definiálja az adatvédelmi incidens fogalmát, 25/I és J §-a pedig rögzíti, hogy az adatkezelőt milyen kötelezettségek terhelik az adatbiztonsági intézkedések megtétele és az adatvédelmi incidensek kezelése során.[335]

2001. évi CVIII. törvény[336] az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről kimondja, hogy „6/A. § * (1) A bejelentés-köteles szolgáltatások nyújtói megteszik a megfelelő intézkedéseket arra, hogy az általuk használt hálózati és információs rendszerekkel összefüggésben a biztonsági események bekövetkezését megelőzzék, hatásukat csökkentsék, illetve bekövetkezés esetén azokat kezeljék." 6/B. § * (1) * A bejelentés-köteles szolgáltatást nyújtók haladéktalanul bejelentik a Kormány által rendeletben kijelölt eseménykezelő központ (a továbbiakban: eseménykezelő központ) részére a külön Korm. rendeletben meghatározott biztonsági eseményeket. A szolgáltató jogkövető magatartását a Kormány által megjelölt hatóság végzi, amely bírságot is kiszabhat pl. a hálózati és információs rendszereit érintő biztonsági események bejelentésének elmulasztásakor (6/C.§ (b)).

15/B. § * (1) A szolgáltató az elektronikus információs rendszereket érintő biztonsági események megelőzésével, kezelésével összefüggő tevékenység vonatkozásában köteles együttműködni az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 19. § (1) bekezdés szerinti eseménykezelő központtal. Köteles az biztonsági esemény kezelése és kivizsgálása szempontjából szükséges általa kezelt és rendelkezésre álló adatokat az eseménykezelő központnak átadni.

Jelen képzésben résztvevő számára talán nem kell magyarázni, hogy egy olyan szigorúan szabályozott terület esetén, mint az információbiztonság és a kiberbiztonság, minden szervezet életében elsődleges a jelentéstételi kötelezettség, a hatóság szerveivel folytatott hivatalos kommunikáció. Itt a válságkommunikációs stábnak nincs különösebb mozgástere, feladata az, hogy az incidenst megelőzően („békeidőben") dolgozza ki az idevágó protokollokat és a felkészülési szakaszban (válságkezelési tréningek során) begyakoroltassa az eljárásokat, hogy a bejelentéssel kapcsolatos intézkedések váljanak rutinná. Amikor beüt a krach, mindenkinek tisztában kell lennie azzal, hogy mi a dolga, ki tesz jelentést, milyen csatornán, milyen információtartalommal.

A bejelentés tartalmát a jogszabály ugyancsak világosan rögzíti. Az eseménykezelő központ felé jelenteni kell:

a) a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
b) a biztonsági esemény időtartamát,
c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
d) a szolgáltatás működésében támadt zavar mértékét,
e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét. (Feltéve, hogy a hatásokat a szervezet ki tudja értékelni a vonatkozó (EU) 2018/151 bizottsági végrehajtási rendelet értelmében.)

---

334 Magyarország Alaptörvénye (2011. április 25.) https://net.jogtar.hu/jogszabaly?docid=A1100425.ATV, letöltés: 2019.08.31.

335 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, https://net.jogtar.hu/jogszabaly?docid=A1100112.TV, letöltés: 2019.08.31.

336 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről, https://net.jogtar.hu/jogszabaly?docid=A0100108.TV, letöltés ideje: 2019. augusztus 23.

A bejelentés-köteles szolgáltatók számára eljáró hatóságként a Kormány a Nemzetbiztonsági Szakszolgálatot jelölte ki. A Nemzetbiztonsági szakszolgálat (továbbiakban: hatóság) kapcsolatot tart

a) a bejelentés-köteles szolgáltatást nyújtókkal és a közvetítő szolgáltatókkal,
b) a rendvédelmi szervekkel,
c) az Európai Unió más tagállamainak illetékes ágazati hatóságaival,
d) a Nemzeti Adatvédelmi és Információszabadság Hatósággal,
e) az Európai Unióban nem letelepedett, Magyarországon belül szolgáltatásait kínáló bejelentés-köteles szolgáltatást nyújtók által kinevezett képviselőkkel;

Emellett feladati körében

– a nyilvánosságot szükség szerint tájékoztatja az egyes biztonsági eseményekről;
– szükség szerint kötelezi a bejelentés-köteles szolgáltatást nyújtót a nyilvánosság tájékoztatására;

Bejelentés-köteles szolgáltató az eseménykezelő központ felé megteszi bejelentését (ha az esemény hatásait ki tudja értékelni, majd az eseménykezelő központ összefoglaló értékelése alapján indul (vagy nem indul) hatósági eljárás. Ekkor a hatóság az eseménykezelő központtal egyeztetve tájékoztatja a nyilvánosságot vagy kötelezi erre a bejelentés-köteles szolgáltatót.

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról[337] rögzíti, hogy az adott szerv vezetője „felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért" (11. § (1) m)). A 13. § kimondja, hogy a szervezet elektronikus információs rendszereinek biztonságáért felelős személy az, aki kapcsolatot tart a hatósággal és az eseménykezelő központtal. (11. § (2) f)) A biztonsági eseményekről pedig a jogszabályban meghatározott szerve(ke)t tájékoztatni köteles.

270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről[338]

A jelentős biztonsági eseményekkel és azok bejelentésével összefüggő szabályok
6. § (1) A bejelentés-köteles szolgáltatást nyújtó haladéktalanul bejelenti az eseménykezelő központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására.
(2) A biztonsági események hatása jelentőségének megállapításakor figyelembe kell venni az (EU) 2018/151 bizottsági végrehajtási rendeletben meghatározott paramétereket.
(3) A biztonsági esemény hatása jelentőségének meghatározása érdekében a bejelentés-köteles szolgáltatást nyújtó szolgáltató tájékoztatásának az alábbi adatokat is tartalmaznia kell:
a) a biztonsági esemény által érintett felhasználók számát, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását,
b) a biztonsági esemény időtartamát,
c) a biztonsági esemény által érintett terület földrajzi kiterjedését,
d) a szolgáltatás működésében támadt zavar mértékét,
e) a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértékét.
(4) A biztonsági esemény bejelentésére vonatkozó kötelezettség csak abban az esetben áll fenn, ha a bejelentés-köteles szolgáltató számára elérhetők azok az információk, amelyek alapján a (2) bekezdésben említett paraméterek figyelembevételével ki tudja értékelni a biztonsági esemény hatását.

[337] https://net.jogtar.hu/jogszabaly?docid=a1300050.tv, letöltés ideje: 2019. július 25.
[338] https://net.jogtar.hu/jogszabaly?docid=A1800270.KOR, letöltés ideje: 2019. július 25.

(5) Az eseménykezelő központ a biztonsági esemény műszaki vizsgálatát követően hatósági eljárás megindítása és lefolytatása céljából a rendelkezésre álló információkat összefoglaló jelentéssel átadja a hatáskörrel és illetékességgel rendelkező hatóság részére.
(6) A hatóság az eseménykezelő központ összefoglaló jelentése alapján hivatalból indítható hatósági eljárása keretében
a) vizsgálja a bejelentés-köteles szolgáltatást nyújtó által megtett megelőző és eseményt kezelő tevékenységet;
b) vizsgálja a 4. §-ban és az 5. §-ban meghatározott követelmények teljesülését;
c) vizsgálja a bejelentés-köteles szolgáltatást nyújtó biztonsági intézkedéseinek megfelelőségét;
d) a vizsgálat során jogosult a 3. § szerinti cselekményeket elvégezni;
e) a vizsgálat eredményeként hatósági döntést hoz, amelynek tartalma legalább:
ea) a biztonsági esemény bekövetkezése tényének megállapítása,
eb) az elhárításra javasolt intézkedések,
ec) a további károkozások megelőzése érdekében javasolt intézkedések;
f) az eseménykezelő központtal történt előzetes egyeztetést követően tájékoztathatja a nyilvánosságot vagy kötelezheti a bejelentés-köteles szolgáltatást nyújtót a nyilvánosság tájékoztatására, ha erre egy adott biztonsági esemény megelőzéséhez vagy egy már folyamatban lévő biztonsági esemény kezeléséhez szükség van, vagy ha egy biztonsági esemény nyilvánosságra hozatala egyéb módon a közérdeket szolgálja.

Az elektronikus hírközlési szolgáltató a kormányzati eseménykezelő központ tájékoztatása alapján köteles értesíteni azon előfizetőjét vagy felhasználóját, amelynek elektronikus hírközlő végberendezése vagy információs rendszere a biztonsági esemény bekövetkezésében érintett vagy azt okozta, vagy az által tudomása szerint fenyegetett. (92/B (3))[339]

Emellett a „Hatóság előírhatja az elektronikus hírközlési szolgáltatók számára, hogy az előfizetőik, és felhasználóik tájékoztatása céljából a Hatóság által meghatározott módon közérdekű tájékoztatást állítsanak össze. A közérdekű tájékoztatás kiterjedhet - többek között - az alábbiakra: […] c) az elektronikus hírközlési szolgáltatások használata során a személyes biztonságot, a magánéletet és a személyes adatokat fenyegető kockázatokkal szembeni védelem céljából rendelkezésére álló eszközökre.” (144. § (2) c))[340]

További –a témánkból fontos – rendelkezéseket tartalmaz az elektronikus hírközlési törvény 156. §-a is:

(3) A személyes adatok megsértésének az észlelése esetén az elektronikus hírközlési szolgáltató haladéktalanul köteles azt a Hatóságnak bejelenteni.
(5) Ha a személyes adatok megsértése várhatóan hátrányosan érinti az előfizető vagy más magánszemély személyes adatait vagy magánéletét, akkor az elektronikus hírközlési szolgáltató erről az előfizetőt vagy magánszemélyt is indokolatlan késedelem nélkül köteles értesíteni. Nem kell az érintett előfizetőt vagy magánszemélyt értesíteni a személyes adataival való visszaélésről, ha az elektronikus hírközlési szolgáltató a Hatóságnak kielégítően igazolni tudja, hogy végrehajtotta a megfelelő technikai védelmi intézkedéseket, vagy, hogy ezen intézkedéseket alkalmazták a biztonság sérelmével érintett adatok tekintetében. Az ilyen technológiai védelmi intézkedéseknek értelmezhetetlenné kell tenniük az adatokat az azokhoz való hozzáféréshez engedéllyel nem rendelkező személyek számára.
Azért itt álljunk meg egy szóra! A pr szakma alapvetése ugyanis az, hogy ha volt esemény, annak híre megy: vagy a konkurencia, vagy valamely nemes érzülettől hajtott dolgozó meg fogja szellőztetni, hogy bizony *vannak rések a pajzson*. Éppígy a média tudomására hozhatja a támadás tényét azonban az elkövető is. Ekkor pedig már késő azt magyarázni, hogy azért nem szóltunk róla, mert nincs jelentősége. Ekkor bizonyosan defenzívába szorul a szervezeti retorika, azonnali a *bizalomvesztés*.

[339] 2003. évi C. törvény az elektronikus hírközlésről, https://net.jogtar.hu/jogszabaly?docid=A0300100.TV, letöltés ideje: 2019. augusztus 9.
[340] Uo.

(6) Az érintett előfizetők vagy magánszemélyek értesítésére irányuló szolgáltatói kötelezettség sérelme nélkül - amennyiben a szolgáltató még nem értesítette az előfizetőt vagy magánszemélyt a személyes adatok megsértéséről - a Hatóság, a Nemzeti Adatvédelmi és Információszabadság Hatóság véleményének kikérését követően, kötelezheti erre, miután megfontolta a biztonság megsértésének várható hátrányos hatásait.
(7) Az előfizetőnek vagy magánszemélynek szóló értesítés tartalmazza legalább a személyes adatok megsértésének jellegét és azokat az információs pontokat, ahol az előfizető további felvilágosítást kaphat, továbbá intézkedéseket javasol a személyes adatok megsértése lehetséges hátrányos hatásainak enyhítésére. A Hatósághoz intézett értesítés ezen túlmenően leírja a személyes adatok megsértésének következményeit, és az annak orvoslására az elektronikus hírközlési szolgáltató által javasolt, vagy megtett intézkedéseket.
(10) A szolgáltató tájékoztatja az előfizetőt a hálózat egységességével és a szolgáltatás biztonságát veszélyeztető, a szolgáltató által megtett műszaki és szervezési intézkedések ellenére fennmaradó, ismert kockázatokról és a védelem érdekében az előfizető által tehető intézkedésekről.
(11) Ha a hálózat egységességével és a szolgáltatás biztonságát érintő vagy veszélyeztető esemény következtében korábban nem ismert, új biztonsági kockázat jelentkezik, a szolgáltató legalább ügyfélszolgálatán és internetes honlapján haladéktalanul tájékoztatja az előfizetőt a korábban nem ismert, új biztonsági kockázatról, a védelem érdekében az előfizető által tehető intézkedésekről, és azok várható költségeiről. A szolgáltató által nyújtott tájékoztatásért külön díj nem kérhető az előfizetőtől. A szolgáltató által nyújtott tájékoztatás nem mentesíti a szolgáltatót a védelem érdekében teendő, a hálózat egységességével és a szolgáltatás megszokott biztonsági szintjének visszaállítása érdekében szükséges intézkedések megtétele alól.

A jogszabályok egyértelművé teszik, hogy a kommunikáció egyik kiemelt címzettje, bejelentés-köteles szolgáltatást nyújtó szervezet esetében a Nemzetbiztonsági Szakszolgálat – mint eljáró hatóság – elsődleges a bejelentési kötelezettség alá eső biztonsági eseményekről történő jelentéstétel. Erre protokoll kidolgozása szükséges a szervezeti folyamatmenedzsment és stratégiai tervezés részeként. Az alapvető szolgáltatást nyújtó szervezetek esetében pedig a MB Országos Katasztrófavédelmi Főigazgatóság a kijelölt eljáró hatóság.

A szervezet részéről folytatott tudatos kommunikáció azért is életbevágó, mert a 270/2018. (XII. 20.) Korm. rendelet értelmében a hatóság maga is megteszi nyilatkozatát a nyilvánosság felé a biztonsági eseményről, ha úgy ítéli, hogy az szükséges, illetve erre kötelezi a szolgáltatót. (2. § (2) e) és f))

A szervezeten kívüli kommunikáció lehetséges címzettjei még a jogszabályban meghatározott olyan koordinációs és egyéb (tanácsadó) szakmai testületek, mint a Nemzeti Kiberbiztonsági Koordinációs Tanács és a Nemzeti Kiberbiztonsági Fórum, illetőleg a más ágazati és funkcionális munkacsoportok.[341] Itt fontos megjegyezni, hogy a „Tanáccsal kapcsolatos kommunikációs feladatokat a Tanács elnökének irányításával a kiberkoordinátor látja el és felügyeli.” (11. §)

Ahogyan az EU végrehajtási rendeletnek[342] való megfelelést, úgy a szervezeti kommunikációs aktivitásokat is dokumentálni kell. Válság esetén kiemelten fontos, hogy az információadás nyomon követhető és visszakereshető legyen. (Anthonissen – pl. sajtókapcsolati űrlap).

A kommunikáció hivatalos jellegét minden esetben erősíti a hazai (Ibtv.) és nemzetközi jogi normákra (GDPR) és irányelvekre (NIS) való hivatkozás, azok beidézése. Bánjunk azonban csínján a jogi és kibernetikai szakterminusokkal, mert túlzott alkalmazásuk könnyen az üzenet érthetőségének rovására mehet.

[341] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről, https://net.jogtar.hu/jogszabaly?docid=a1300484.kor, letöltés ideje: 2019. augusztus 9.

[342] https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R0151&from=BG, letöltés ideje: 2019. július 25.

## 6.5. Kibertámadások és a média

### *6.5.1. A kibertámadás mint hír*

Nehéz tudományos alapossággal megmondani, hogy a mi a hír. Az újságíró iskolák rendszerint azt hangsúlyozzák, hogy alapja a változás. Valami történik, megváltozik, elmozdul.[343] Ha mint médiaműfajt tekintjük, azért a tapasztalatból levonhatók bizonyos következtetése esszenciális jegyeit illetően: „…hírnek az olyan objektivitás látszatával rendelkező aktuális, újdonságot tartalmazó információt nevezzük, ami sokakat érdekelhet és/vagy sokak életében változást okozhat."[344] Erre mondja a sajtszakma, hogy a hír attól lesz hír, hogy hírértéke van.

A kibertámadások minden esetben komoly hírértékkel bíró események, amelyek maguktól értetődően számot tartanak a média érdeklődésére. Ha a biztonsági esemény ráadásul több hírértéket befolyásoló dimenziót felölel, nagy esélyünk van rá, hogy vezető hírként találkozunk a minket ért „csapással" a hírmédiában. A végrehajtási rendelet értelmében jelentős hatást gyakorló eseménynek minősülő incidens ugyanis minden bizonnyal agresszió, negatív esemény, illetve hatása, kimeríti a konfliktus, a kár vagy a normasértés fogalmát, széles az érintettek köre, ha nem meglepő[345], akkor nagy valószínűséggel más események sorába (bevett tematikai keretbe) illeszkedik/illeszthető.[346] Az esemény ezen jegyei önmagukban is arra predesztinálják a „sztorit", hogy a sajtóba kerüljön. Ha földrajzi vagy kulturális közelség, az elit nemzetek érintettsége felmerül, még szorongatóbb az újságírók információéhsége és beszámolási kényszere.

A hírértéket az újságírói működés egyik szakmai kódjának is tekintjük, amely segíti a hírek szelektálását, közöttük fontossági sorrend felállítását. A hírtől objektivitást, tényszerűséget és igaz közlést várunk, a hírérték azonban relatív és a válságkommunikációban e tulajdonságát kihasználhatjuk. Megfelelő retorikai stratégiával növelhetjük vagy csökkenthetjük egy esemény hírértékét.

#### 6.5.1.1. A sajtókapcsolatok általános szabályai

Mivel a válságkommunikáció sem a válság bekövetkezésével, hanem jóval előbb, a prevencióval, a biztonságtudatosság kiépítésével és kommunikálásával kezdődik, e helyen célszerű az általános sajtókapcsolati szabályokat röviden áttekinteni.

A legfontosabb, hogy tartsuk nyitva a kommunikációs csatornákat (kölcsönös elérhetőség), legyünk elérhetőek. Jelöljük meg azt a személyt és módot, akitől és ahogyan információt kérhetne kiberbiztonsági témákban (békeidőben és rendhagyó helyzetekben is).

Folyamatosan bővítsük az újságírók ismereteit azokban a témákban, amelyek számunkra fontosak. Képezzük tehát őket a kiberbiztonság témában részletes szakmai háttérinformációk adásával, háttérbeszélgetésekkel, kiegészítő információk adásával, az információk összefüggésekbe ágyazásával, ha ezt igénylik. Könnyítsük meg az újságíró, szerkesztő munkáját, adjunk jól strukturált, világos könnyen kezelhető, lehetőség szerint illusztrációval ellátott anyagokat. Jelöljünk meg további forrásokat, ahol tájékozódhatnak adott szakmai kérdésekben.

---

343 Bernáth László (szerk.) (é.n.): Műfajismeret, Sajtóház Kiadó, Budapest. 46. o.

344 Zsolt Péter (2003): Médiaháromszög, EU-Synergon, Vác. 34. o.

345 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;

346 Részletes lásd Luzt Erbring és Winfried Schulz felsorolását a hírértéket befolyásoló tényezőkről, In: Herendy Csilla-Kriskó Edina (2012): A közkapcsolat-tartás gyakorlata, NKE KTK, Budapest.

Ne kivételezzünk!

Ne használjuk ki, és ne zsaroljuk a médiát!

Menedzseljük a rossz híreket is!

Tanúsítsunk mértékletességet a helyreigazításokat illetően!

Küzdjünk a publicitásért![347]

Nem feledkezhetünk meg arról, hogy a média sztorikban gondolkodik, kerek egész történeteket igyekszik fogyasztói elé tárni. A tájékoztatási szükséglet kielégítésén (objektív tényközlés) túl szórakoztatni is akar. A hírműfajban is fontos, hogy ki, mit mikor, hol miért csinál (tényhír), de az események bemutatásának teljességhez hozzátartozik a hogyan (teljes hír)[348] és a híranyag élményszerűvé tétele. Fel kell tehát készülni rá, hogy az újságírót a legapróbb részletek is érdekelni fogják. Ablakot akar nyitni közönsége számára, amelyen keresztül egy korábban nem ismert világ titkaiba nyújt bepillantást.[349]

A sajtónak szánt közlemény hírértékét növeli formai szempontból, ha közérthető, tárgyszerű, tömör és pontos. Az újságíró szereti, ha a kapott információ félreérthetetlen és félreértelmezhetetlen, világosan megállapítható mik a tények, s hol kezdődik a kommentár, minősítés. Végül, de nem utolsósorban fontos, hogy ne legyen az anyag spekulatív és manipulatív.[350]

### 6.5.1.2. A nyilatkozatadás szabályai

A nyilvános szereplések és médiakommunikáció mára talán már elcsépeltnek is tűnő hármasa, a kell, lehet és tilos információk megkülönböztetése alapozza meg a válságnyilatkozatokat. Egyes számú szabály, hogy első közléskor csak annyit mondjunk, amennyit feltétlenül szükséges és/vagy amennyit a közvélemény már amúgy is tud (észlelése vagy az információk kiszivárgása alapján). Kettes számú szabály, jelöljük meg az időpontot, amikor bővebb tájékoztatást adunk. Vigyázat! Innentől ketyeg az óra, annyi időnk van felkészülni az átfogó tájékoztatásra, amennyit az első közlésben szabtunk.[351] (Anthonissen, 2009) Hármas számú szabály, hogy alaposan készüljünk fel a *kell*, *lehet* és *tilos* típusú információkból. Vagyis gondoljuk végig, mi az, amit mindenképpen el akarunk mondani, bele kell férnie a nyilatkozatba, mi az, amiről célszerű volna még beszélni, ha alkalom kínálkozik rá, és mi az, aminek a sajtóban történő elhangzását el kell kerülni.[352]

A nyilatkozattétel alapvető szabályai (Juhász, 2009, 14)

- A nyilatkozó mutatkozzon be és adja meg, milyen minőségben nyilatkozik (ezzel autoritását fejezi ki).
- Jelölje meg a nyilatkozat célját (megnyugtatás, tájékoztatás, tévhitek eloszlatása).
- Juttassa kifejezésre, hogy figyelemmel kíséri az ügyet (képben van), hiteles információi vannak, azokat érti, belelát a dolgokba, átlátja a helyzetet.
- Konkretizálja a szükséges lépéseket, szólítson fel azokban való részvételre, vagy távolmaradásra, a szabályok betartására.
- Jelölje meg az igénybe vehető segítségeket, ki hova fordulhat, ezzel támaszt nyújt és bizalmat ébreszt.
- Rajzoljon pozitív jövőképet (Ha így tesznek….).
- Mindig azzal zárja nyilatkozatát, hogy megköszöni az együttműködést. (Juhász, 2009, 15)

[347] Nyárády-Szeles, é.n. i.m. 112-113. o.
[348] Domokos Lajos (1995): A nyomtatott és az elektronikus újságírás elmélete, Teleschola, OMIKK.
[349] Bernáth, é.n. i.m.
[350] Zsolt, 2003. i.m.
[351] Anthonissen, 2009. i.m.
[352] Németh Erzsébet (2006): Közszereplés, Osiris, Budapest.

## 6.6. A lehetséges retorikai stratégiák és a közzététel

Mielőtt sorra vesszük a lehetséges közlési stratégiákat tekintsük át, milyen kihívásokat rejt az incidenskommunikáció![353] Kulikova és szerzőtársai (2012) megerősítve a pr szemléletét azt mondja, hogy még „békeidőben", az incidenseket és válságokat megelőzően célszerű kidolgozni egy döntéstámogató keretrendszert, amely segít meghatározni az események nyilvános közléseinek stratégiáját. A kommunikáció korábban is említett alapkérdéseit ők (mint azt az alábbi táblázat mutatja) négy aspektusból tartják szükségesnek megválaszolni: a megelőzés és kárenyhítés, az jogszabályoknak való megfelelés, a költséghatékonyság és a hírnév dimenzióinak figyelembevételével.

| | **Kinek?** | **Mikor?** | **Mit?** | **Hogyan?** |
|---|---|---|---|---|
| **Kárenyhítés és megelőzés** | Kik azok az érintettek, akiket tájékoztatni kell a kárenyhítés megelőzés lépéseiről? | Mikor kell értesítéseket kiadni az eseményekre való reagálás megkönnyítése érdekében? | Mit tartalmazzon az értesítés az érintettek számára, hogy a kockázatokat felmérhessék és a megfelelő lépéseket megtehessék? | Az értesítés mely módja biztosítja a szükséges információk gyors és pontos közzétételét? |
| **Előírásoknak/ jogszabályoknak való megfelelés** | Kit kell értesíteni a jogi kötelezettségekkel kapcsolatosan? | A törvény által előírt érdekelt felek tájékoztatását hogyan célszerű ütemezni? | A közzétételekben milyen jogi szempontból kötelező információknak kell szerepelniük? | A jogi kötelezettségekkel kapcsolatos értesítéseknek mi legyen a módja? |
| **Költséghatékonyság** | Hogyan biztosítható, hogy az értesíteni kijelölt érintettek köre tükrözi az esemény súlyosságát? | Mely időpontban tegyük közzé az információkat, hogy az ne rontsa tovább a szervezet helyzetét? | Hogyan szűrjük vagy csomagoljuk úgy az információkat, hogy azok ne okozzanak további anyagi károkat a szervezetnek? | Melyek a legköltséghatékonyabb értesítési módszerek? |
| **Hírnév** | Kik azok az érintettek, akik hozzájárulhatnak a hírnév helyreállításához és kik azok, akik tovább ronthatják azt? | Hogyan időzítsük úgy a közléseket, hogy azok segítsenek a szervezeti hírnév helyreállításában? | Melyek azok a tartalmak (üzenetek), amelyek erősíthetik és nem ronthatják a szervezet hírnevét? | Mely értesítési módszerek hatnak jótékonyan a szervezet hírnevére? |

*2. sz. táblázat: Az incidensinformációk közzétételének kihívásai*
*Forrás: saját készítésű és fordítású táblázat*[354]

A keret kidolgozásának alapja az események életciklusa volt: az események hatásának értékelés, a válság vagy incidenskezelő csapat felállítása és a károk mérséklésének, elhárításának megkezdése (1). Ezt követi a további információgyűjtés és értékelés az eseményről, majd a szervezeti prioritások meghatározása a reagálásban (2). Harmadik lépcső az események nyilvánosságpolitikájának kialakítása és az értékelés eredménye alapján az intézkedések foganatosítása (3). Negyedik és egyben záró lépés a közzététel és a tanulás (4). (A folyamatábrát lásd a 2. sz. mellékletben).

[353] Kulikova, Olga-Heil-Ronald-Berg Jan van den-Peters, Wolter (2012): Cyber Crisis Management: A decision-support framework for disclosing security incident information, 2012 International Conference on Cyber Security, Washington, DC, USA, 14-16 Dec. 2012. (IEEE), DOI: 10.1109/CyberSecurity.2012.20

[354] Kulikova et al., 2012, i.m. 106. o.

A kibereseményekkel kapcsolatban felmerülő kérdések között elsőként kell megválaszolni az alábbiakat:

- Hogyan derült fény az eseményekre? (Ki vette észre? Belső érintettek valamelyike, hatósági szerv, a média vagy netán hackerek, esetleg ügyfelek vagy más külső személy?)
- Mekkora az incidens kiterjedése?
- Mi a támadás eredménye? (jogosulatlan hozzáférés, adatokkal való visszaélés, szolgáltatáskiesés stb.)
- Jelentős anyagi kockázatot jelent-e az esemény?
- Szükség van-e külső segítségre a kárelhárításhoz és enyhítéshez?
- Az önkéntes megosztás előnyt jelent-e a szervezet számára?[355]

Javasolt emellett az eseménykezelésben a prioritások átláthatóságának biztosítása érdekében valamilyen szemléltető, áttekintő eszközt alkalmazni. Kulikova és társai az ún. eseménykezelés-prioritási csúszkát javasolják. (lásd. 3. sz. melléklet). Álláspontjuk szerint ugyanis nem lehet minden prioritást egyforma súllyal és kapacitással szolgálni a folyamatban, ezért meg kell határozni, mely területeken ad fel céljaiból a szervezet és hova összpontosítja erőforrásait. Ez adhatja alapját az optimális esemény-nyilvánosságra hozatali (esemény-közzétételi) stratégia kidolgozásának.

Ha ezzel megvagyunk, következhet az üzenetek kidolgozása**.** Elsőként a tagadási stratégiák csáberejéről kell szólnunk. Elvégre, ha nincs válság, nincs probléma, nincs kommunikáció. Működik a no comment. Ez a tagadás legegyszerűbb és legdurvább módja. Jegyezzük meg, kizárólag az autoriter szervezeteknél, a hatalmi pozícióban lévő aktorok számára járható út. Az erő pozíciójából el lehet hallgattatni a kíváncsiskodókat. Természetesen, ha van cáfolat, amely nyilvánosságra kerül, a szervezet hitelessége végleg oda. Aki hazudik válságidőszakban, azt békeidőszakban is megvetés és alapvető kétkedés övezi.

A retorikai ellentámadás célpontja kibertámadás esetén a hatóság, az eseménykezelő központ vagy más szakmai és vagy nemzetközi szervezet lehet, amelynek esetleges mulasztására hivatkozik a támadás elszenvedője. (Az eseménykezelő központ például nem adott ki időben figyelmeztetést vagy nem tett elérhetővé fontos a megelőzést lehetővé tevő információkat.)

Kérdés persze, hogy mely szervezet vállalja azt fel, hogy a sajtó nyilvánosságában szembe megy, támadólag lép fel az eseménykezelő vagy a felügyeletet gyakorló szervvel.

Amikor a közvélemény felelőst (kvázi bűnbakot) akar, a törvényből s a működési folyamatokból és védelmi felelősség alapján is elsődleges célponttá válhat a fejlesztést végző, az üzemeltetés végző, az üzemeltetésért felelős és az információbiztonságért felelős személy. A szervezet reputációját azonban csak a bűnbakként megnevezett szervezeten kívüli személy vagy csoport nem sérti. Nem sérti nagyon. A közvélemény ugyanis nem szereti azokat, akik másra mutogatnak. (Mindig van egy olyan konnotációja, hogy ki akar bújni a szervezet a felelősség alól.)

Az *események jelentőségét* nyilatkozatainkban úgy is *csökkenthetjük*, ha a kibertámadások tömegességéhez mérjük saját áldozattá válásunkat, azt kommunikáljuk, hogy minden percben kibertámadások százai indulnak a világ számítógép-hálózatának különböző pontjain lévő felhasználók ellen. Igen szemléletesen mutatják ezt az olyan valós idejű térképalkalmazások, mint a Threatcloud *Live Cyber Attack Threat Map* alkalmazása[356]. A Kapersky globális biztonsági vállalat kiberfenyegetettségi statisztikája szerint Magyarország a 47. leginkább támadott ország, míg Szlovákia a 87.[357] Július hónapban Európában a leginkább fertőzött 5 ország sorrendben a következő volt: Fehéroroszország, Oroszország, Ukrajna, Moldova és Albánia.[358]

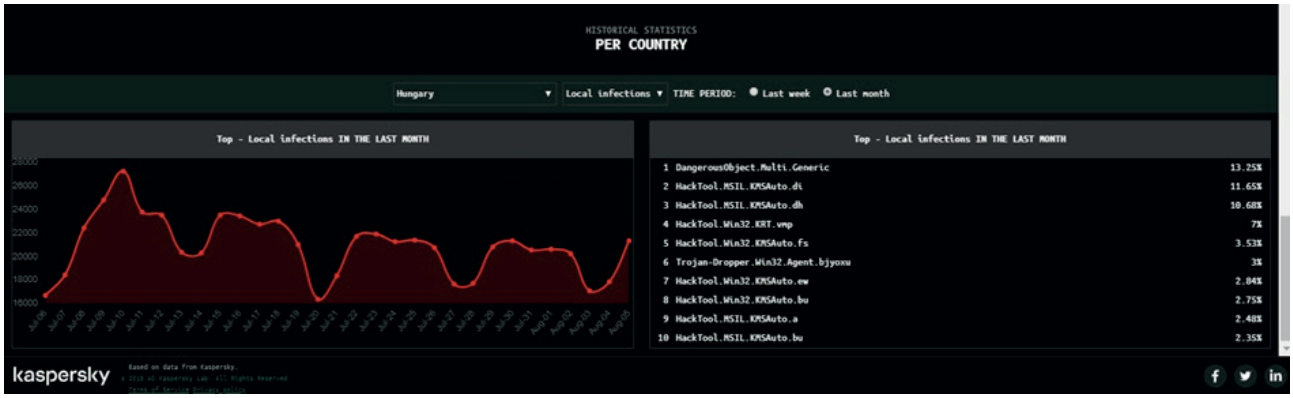
[355] Kulikova et al. 2012. i.m. 108. o.

[356] https://threatmap.checkpoint.com/ThreatPortal/livemap.html, letöltés ideje: 2019. augusztus 7.

[357] https://cybermap.kaspersky.com/, letöltés ideje: 2019. augusztus 7.

[358] https://cybermap.kaspersky.com/stats/#country=122&type=oas&period=m, letöltés ideje: 2019. augusztus 7.


Az interneten tehát bárki nyomon követheti, mennyire nem egyedi eset az, ha egy szervezet vagy hálózat kibertámadás áldozatává válik. Ilyen üzeneteknél szokás átvitt értelmű kifejezéseket és hasonlatokat használni.




A *mentegetőzés* retorikája arra fókuszál, hogy az események folyásában a szervezet minél kisebb felelősségét ismerje el vagy olyan okot találjon, amely felmenti a szervezetet, ha hibázott. Az „aki dolgozik, hibázik” üzenetei ezek. Például a szervezet arra helyezi a hangsúlyt, hogy a jó szándék vezette, jó célból tett lépései sodorták veszélybe. A szándékosságot ilyenkor kizárja a szervezet.

A *megokolás* stratégiája rokona az előbbinek. Ekkor az üzenet arról szól, hogy milyen lépések, oksági összefüggések vezethettek az incidenshez. A józan belátásra alapoz ekkor a kommunikátor. (Pl. Bármennyire igyekszünk is, a hackerek és bűnözői vagy terrorista csoportok előttünk járnak. Több forrás, kapacitás stb. áll rendelkezésükre a támadó fejlesztések lekövetése a védelmi vonalon időt igényel.)

| | |
|---|---|
| **Tagadási stratégiák** | |
| Ellentámadás | A vád és vádló visszatámadása, fenyegetés (erővel, perrel) |
| Tagadás | A krízis tagadása és okszerű alátámasztása. |
| Bűnbakkeresés | A szervezeten kívüli személy vagy csoport okolása |
| **Az események jelentőségének csökkentése** | |
| Mentegetőzés | A felelősség minimalizálására tett kísérlet, a szándékosság tagadásával |
| Megokolás, indoklás | Magyarázat adása, az okozó megérdemelt sorsa |
| Újjáépítési stratégiák | |
| Kártérítés | Pénz vagy egyéb juttatás felajánlása az áldozatoknak |
| Bocsánatkérés | Nyilvánosság előtti felelősségvállalás és bocsánatkérés |
| **Támogatást kereső stratégiák** | |
| Emlékeztetés | Korábbi érdemek, eredmények hangsúlyozása |
| Hízelgés | Az érintettek dicsérete, hízelgés |
| **Áldozat szerep** | Annak hangsúlyozása, hogy a hatások elszenvedője a cég, maga is áldozat |

*3. sz. táblázat: A válságkommunikáció lehetséges retorikai stratégiái*
*Forrás: saját szerkesztésű és fordítású táblázat*[359]

Ha egy szervezet az imázsa védelmét helyezi előtérbe és a jövő stratégiai partnerségeire gondol, és persze költségkeretébe belefér a kártérítési összegek megfizetése, választhatja a *kártérítés* és vagy *bocsánatkérés* stratégiáját is. Vagy arra koncentrál, hogy a károsultak számára mit nyújt, hogy megingott bizalmuk helyreálljon, az okozott kárt ellensúlyozza vagy arra, hogy bocsánatkérésével az érintettek és a szélesebb közvélemény jóindulatát is megnyerje.

A közvélemény támogatását el lehet nyerni azonban a korábbi érdemek megidézésével, hízelgéssel és a mártíromsággal is.

A szervezeti kommunikáció nem ér véget ott, ahol az IT biztonsági tevékenységek visszaterelik a szervezetet a normál működésbe. A szervezeti kommunikációnak azt is követnie kell, hogyan halad az okok, hatások, elkövetők kilétének felderítése, van-e gyanúsított, a hatóság kezdeményezett-e eljárást, történt-e letartóztatás, az igazságszolgáltatás gépezete hol tart, születik-e elmarasztaló ítélet stb.

## *6.6.1. Megoldást jelentő kommunikációs csatornák*

Válság (kibertámadás) esetén a veszélyhelyzeti riasztórendszerek lépnek először működésbe és küldenek szöveges figyelmeztető üzeneteket. A válságkezelés azonban, mint az előzőekben már rámutattunk, árnyalt és alapos tájékoztatást követel meg. Elsősorban a felhő-alapú kommunikációs platformok jelenthetik a kiutat a szervezet számára, segíthetik a veszélyhelyzeti kommunikáció javítását. Segítségükkel hamarabb talpra állhatnak a támadás hatásaiból.[360]

Az elmúlt időszak – nem kizárólag kiberbiztonsági területen bekövetkezett – válságeseményei ugyanakkor arra is rámutattak, hogy a közösségi média platformjai elsődleges kommunikációs csatornákká léphetnek elő a külső közvéleménycsoportok tájékoztatásában. (Lásd a Norsk Hydro esettanulmányt a IV.

[359] Coombs, 2012. im. 155. o.
[360] Hawkins, 2017 i.m.

fejezetben) Előnyük, hogy olyan kétirányú információáramlást tesznek lehetővé, amely révén a szervezet is hozzájuthat a számára szükséges információkhoz a felhasználóktól. Emellett a közösségi média széles körben teheti hozzáférhetővé az elvárt magatartásokkal kapcsolatos tájékoztatást. Terjedelmi korlátok okán nem térhetünk ki a felhasználók számára adandó iránymutatások követelményeire részleteiben, csak utalunk rá, hogy vannak már kutatások, amelyek célja feltárni, hogy a fenyegetéskommunikáció miként-je hogyan befolyásolja felhasználók maladaptív viselkedését. (Zsaroló fenyegetések esetében vizsgálták, hogy a fenyegetés kommunikációban a narratív félelemkeltés, az élénk üzenetküldés vagy a megfigyelő tanulás stratégiáinak alkalmazása hogyan befolyásolja a felhasználók kiberbiztonság percepcióit és az események megértését, védelmi motivációjukat.) A kutatások jelen állása szerint kedvezőbb hatás érhető el, ha a felhasználókban felébresztjük a félelmet (de ennek szintjét nagyon körültekintően határozzuk meg), de nagyobb hangsúlyt helyezünk saját védelmük biztosításának gyakorlati módjaira.[361]

## 6.7. Esettanulmányok

### *6.7.1. Postai úton bejelentett adatvédelmi incidens – avagy címlapon a BRFK pendrive-ügye*

„Ötmillió forintra bírságolta a Nemzeti Adatvédelmi és Információszabadság Hatóság a Budapesti Rendőr-főkapitányságot, mert elveszítettek egy 4 GB-os pendrive-ot, amin fent volt a BRFK teljes nevesített személyzeti állománytáblája – szúrta ki az erről szóló határozatot[362] az Index.

Az adatok között ott volt a rendőrök születési neve, születési ideje, anyja neve, TAJ száma, beosztása és munkaköre.

A főkapitányság munkatársa még januárba vitte magával a pendrive-ot egy értekezletre. Az adathordozót a kulcskarikájára fűzte, a kulcsot pedig magával vitte a szállodai szobájába. Másnap kijelentkezett a szállodából, majd egy rövid gyorsétteremi kitérő után visszatért a budapesti szolgálati helyére, ekkor vette észre: nincs meg pendrive.

Még aznap jelentette az elöljárójának, hogy nyoma veszett az adathordozónak. Rögtön megindult a telefonálgatás, felhívták a szállodát és a gyorséttermet is, azonban mindhiába.

A pórul járt rendőr a személyes adatokat tartalmazó dokumentumokat nem a szolgálati, hanem magáncélra használt adathordozóra másolta át, és nem alkalmazott semmilyen biztonsági intézkedést a tárolt adatokkal kapcsolatban, ezért vele szemben fegyelmi eljárás indult.

A pendrive azóta sem került elő."[363]

Fenti esetben nyilvánvalóan az a kommunikációs kihívás, hogy reagálni kell ama lapértesülésre, mely szerint „Az adathordozó, valamint az azon található állományok semmilyen hozzáférésvédelemmel (pl. jelszó, titkosítás) nem voltak ellátva. Az adathordozón nem szerepelt egyébként olyan anyag, amely más forrásból ne lenne helyreállítható."

Ha egyszemélyben az alkalmazottat tesszük felelőssé, azonnal bűnbakot szolgáltatunk a sajtónak és céltáblává tesszük az állomány számára. A szervezet pedig azonnal szembesül a váddal, hogy inkompetens embereket alkalmaz, így többes számban. („Ezek hülyék!") Azután érkeznek az olyan szofisztikáltabb elmarasztalások, mint hogy nincs semmilyen biztonságtudatosság. (Felmerül, hogy

[361] Maretta, Kent-Vedadib, Ali-Durcikovac, Alexandra (2019): A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses, Computers & Security Volume 80, January 2019, Pages 25-35., https://doi.org/10.1016/j.cose.2018.09.004

[362] http://naih.hu/files/NAIH-2019-2471-hatarozat.pdf, letöltés: 2019. július 12.

[363] https://hvg.hu/itthon/20190712_Elhagytak_egy_pendriveot_rajta_a_BRFK_osszes_rendorenek_adataival, letöltés: 2019. július 12.

vajon milyen információkkal bánik még ilyen könnyelműen a BRFK? És ekkor már az egész szervezet jelenik meg mint hanyag, felelőtlen, hozzá nem értő adatkezelő.)

Négy nappal később a BRFK a hivatalos weboldalán adott tájékoztatást arról, hogy a pendrive megkerült, és az adatok nem kerültek illetéktelen kezekbe, hiszen mindvégig a szolgálati autóban voltak, amelyet kizárólag az adathordozót „elvesztő" munkatárs vezetett.[364]

Minden jó, ha jó a vége, de vajon vége van-e? Motoszkál a kétely az ember és különösen az internetes híreket fogyasztó magyar állampolgár fejében. Mégiscsak 6 hónapig volt kontroll nélkül az eszköz. Hisszük vagy nem a történetet a soha ki nem takarított és kizárólagosan használt szolgálati gépjárműről. Ilyen a médiafogyasztó, különösen, ha egy szervezet bizalmi indexe nem túl magas. Merthogy látunk rosszabbul végződő történeteket is…

A BRFK közleménye a pendrive megkerüléséről ugyancsak elgondolkodtató. Nem reflektál arra a körülményre, hogy a közvélemény a sajtóból értesült az incidensről, az esetet a BRFK maga nem kommunikálta a NAIH határozat megjelenését taglaló cikkek megjelenéséig. Nem tért ki a sajtóközlemény arra sem, hogy a sajtóhírek információtartalma mennyiben felelt meg a valóságnak. Nincs arra vonatkozó információ, hogy a BRFK tett-e lépéseket annak érdkében, hogy a jövőben hasonló eset ne ismétlődhessen meg, hiszen, ha az adatok nem is kerültek illetéktelen kezekbe, az információbiztonság elemi szabályait szegte meg a vétkes munkatárs. A vétkes mukatárs ellen indított fegyelmi eljárás eredményét sem közli a hatóság, csak jelzi, hogy lezárult. (Klasszikus hatalmi pozícióból történő kommunikáció tanúi vagyunk. A hatóság bűnbakot szolgáltat, nem kér elnézést, nem magyarázkodik, nem bocsátkozik részletekbe, elmond annyit, amennyit feltétlenül szükségesnek tart, amennyit a közvélemény más forrásokból már amúgyis tud. Nem látjuk annak nyomát, hogy a BRFK felelősnek érezné magát – pl. az alacsony szintű biztonságtudatosság miatt – hogy hosszú távon akarna megnyugtató választ adni, információkezelési gyakorlata iránt bizalmat építeni.)

### *6.7.2. Az ellopott laptop és a hamis felhasználói fiókok*

Egy 23,5 millió tagot számláló és mintegy 50.000 főt foglalkoztató egészségügyi szolgáltató közel 2,8 millió ügyfél adatát tartalmazó laptopját ellopták a társaság egészségügyi elemző szoftverének gyártójától. Az esetre öt nappal később derült fény, amikor egy vállalati ügyfél jelezte az egészségügyi szolgáltató felé, hogy néhány alkalmazottjának adatai szerepeltek egy a sötét neten (dark net) értékesített listán. Ezzel egyidőben az egészségügyi/betegellátó alkalmazás adminisztrátorai pedig jelezték, hogy jelentősen megugrott az új és aktív felhasználói fiókok száma. Észlelték továbbá azt is, hogy mintegy egymillió betegrekordot töltöttek le az egészségügyi alkalmazásból, nem tudni, hogy engedélyezett felhasználásra-e vagy sem. Ekkor a társaság (az egészségügyi szolgáltató) lekapcsolta az orvosok hozzáférését a rendszerhez és riasztotta a számítógépes eseményekre reagáló munkacsoportját.[365]

Az alkalmazást két héten keresztül, míg az esemény kivizsgálása zajlott, offline állapotban tartották. Ez idő alatt az orvosok és szolgáltatók végig manuálisan végezték a követelések érvényesítését és a fedezetellenőrzést és a vállalat call centere nyújtott támogatást. Bebizonyosodott, hogy az ellopott laptop hitelesítő adatait használva számos új felhasználói fiókot hoztak létre az alkalmazásban. Következésképpen minden felhasználó számára új fiókot és azonosítókat kellett kiadni, új alkalmazás és rendszerellenőrzés lépett életbe.

Rövidtávon alapvető üzleti folyamatok szakadtak meg azáltal, hogy megszűnt az orvosok hozzáférése a beteggondozási alkalmazáshoz. Mivel a betegriasztásokat más alkalmazásokon keresztül

[364] http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/kozrendvedelem/nem-kerultek-illetektelen-kezekbe-az-adatok, letöltés: 2019. július 18.

[365] Mossburg, Emily-Gelinne, John-Calzada, Hector (2016): Beneath the surface of a cyberattack A deeper look at business impacts, Cyber Risk, Deloitte

kellett kezelni, növekedett a betegek egészségügyi kockázata. Az egészségbiztosítás pénzügyi információinak hiányában pedig a szolgáltatók kockázata növekedett. Egyértelműen azonnali károkat szenvedett el a cég hírneve is. Az információbiztonsági aggályok azonnali ügyfélvesztést okoztak, amely azonban a következő 3 évben is éreztette hatását az ügyfélakvizíción. A magasabb hitelfelvételi költségek a stratégiai beszerzések késleltetését eredményezték, miközben ügyféloldalon öt éves időtávon kellett a tervezett díjemelést mérsékelni.

| **Hatásfok** | **Időtáv** | **Költség (millió USD)** | **Költség (teljes költség %-ában)** |
|---|---|---|---|
| Sérülés utáni ügyfélvédelem | 3 év | 21.00 | 1,25 |
| Kiberbiztonsági fejlesztések | 1 év | 14.00 | 0,83 |
| Ügyfélértesítés | 6 hónap | 10.00 | 0,6 |
| Ügyvédi díjak és peres ügyek | 5 év | 10.00 | 0,6 |
| Szabályozásnak való megfelelés | 1 év | 2.00 | 0,12 |
| Public Relations | 1 év | 1.00 | 0,06 |
| Műszaki vizsgálat | 6 hét | 1.00 | 0,06 |
| Ügyfélveszteség (meg nem kötött szerződések) | 5 év | 830.00 | 49,43 |
| Ügyfélveszteség (tagok) | 3 év | 430.00 | 25,61 |
| Kereskedelmi név leértékelődése | 5 év | 230.00 | 13,70 |
| Megnövekedett hitelfelvételi költségek | 5 év | 60.00 | 3,57 |
| Biztosítási díjak emelkedése | 3 év | 40.00 | 2,38 |
| Működési zavar | azonnal | 30.00 | 1,78 |
| Szellemi tulajdon elvesztése | nem értelmezhető | 0.00 | 0,00 |
| Összesen | | USD 1,679.00 | |

*4. sz. táblázat: Az incidens hatásai időben és pénzben kifejezve*
*Forrás: Mossburg et al.. 2017. 8. o.*

## *6.7.3. Tervrajzok és dolgozói adatok hacker kézen*

*2018 novemberében olvashattuk, hogy „Hackerek törték fel egy francia cég adatbázisát: nukleáris létesítményekről és börtönökről szereztek meg adatokat - tárta fel a német és a francia sajtó. Az adatok egy része németországi szervereken kötött ki."*[366]

A válságkommunikáció üzeneteinek megfogalmazásához és a nyilatkozattevő személy felkészítéséhez az egyik legalapvetőbb eszköz a kérdés-felelet lista (Q/A) összeállítása. Ekkor az összes elképzelhető felmerülő kérdést feljegyezzük és megpróbáljuk megválaszolni. Nem szelektálunk asze-

[366] https://888.hu/amerika-london-parizs/sulyos-kibertamadas-tortent-franciaorszagban-4160485/, letöltés ideje: 2019. augusztus 2.

rint, hogy a kérdés helyénvaló-e, jogos-e, szakmailag korrekt-e vagy sem. A laikusok és a szakértők részéről várható felvetések mindegyikét számba kell vennünk. Minden kérdést megválaszolunk és a választ addig csiszoljuk, amíg úgy ítéljük, kiállná a nyilvánosság próbáját. Mit értünk ez alatt?

Azt, hogy mérlegeljük az egyes kifejezések korrektségét nyelvi és tartalmi értelemben, a kifejezések érzelmi töltetét, a közvéleményre és szervezetünk hírnevére gyakorolt várható hatását. Példának okáért a *fatális tévedés* kifejezés figyelemfelhívó és fokozza egy esemény drámaiságát, végzetesnek tünteti fel a hibát. Értelemszerűen nagyhatású retorikai alakzat, épp ezért kizárjuk a lehetőségek közül, ha mi idéztük elő a válságot. Ha valaki más fatális tévedésének áldozatai vagyunk, akkor azonban nagy valószínűséggel fog visszaköszönni nyilatkozatainkban.

*„Az Ingerop szóvivője az ügyről nyilatkozva elmondta: több mint 11 000 fájlhoz fértek hozzá a támadók, amely mintegy tucatnyi projekthez kapcsolódik. Sajtóértesülések szerint a projektek között volt egy franciaországi börtön bekamerázásának tervrajza is, amelyen láthatóak a kamerák pontos helyei. Emellett egy nukleáris hulladéklerakó tervrajza is a kiberbűnözők kezébe került. A projektek mellett az Ingerop cég alkalmazottainak, ezer embernek a személyes adatai is a hackerek tulajdonába jutottak – írja az ügyet összefoglaló Deutsche Welle."*

Az események kontextusba ágyazásának ékes példája, ahogyan a médiabeszámolók azzal zárulnak, hogy *„A meglopott francia céget rendszeresen kemény kritikával illetik francia és német származású atomenergia-ellenes aktivisták. A cég főként egy tervezett nukleáris hulladéklerakó miatt került a bírálatok középpontjába."*

A média tehát előveszi, miről is nevezetes a szervezetünk, mivel került már média vagy a társadalmi érdeklődés homlokterébe. Visszautal korábbi velünk kapcsolatos eseményekre, mert így jobban eladható a hír (hiszen alanya kvázi ismerős, az esemény valamely korábbi történet folytatása).

Kibertámadás esetén biztosak lehetünk benne, hogy az újságírók „leporolják" velünk kapcsolatos korábbi tudósításaikat, előveszik – ha voltak – a korábbi (információ)biztonsági incidenseinket, esetleg a vezetőkkel kapcsolatos adatokat (életrajzi és szakmai adatok, előmenetel, kinevezés ideje, körülményei, korábbi munkahelyeken elszenvedett kiberkárok stb.).[367]

Most visszakeresve sem az Ingèrop weboldalán, sem Facebook oldalán nem találunk az incidensről szóló bejegyzést. (A szervezeti weboldalon sem a nyilatkozatok, sajtóanyagok, sem a hírlevelek, nemzetközi hírlevelek, dokumentumok, közzétételek rovatokban nincs nyoma az eseménynek. Leginkább a német sajtóban és a Twitteren vannak elérhető beszámolók az incidensről.) Az Ingèrop a nemzetközi válságkommunikáció elrettentő példája. A sajtóban megjelent cikkek alapján, a sajtó jobban értesült és jobban követi a kiberincidens részleteit, mint maga a cég, miközben annak 52 irodája működik világszerte és tevékenysége 70 országban van jelen.[368] Értékei pedig az elkötelezettség, függetlenség, *felelősségvállalás*, kiválóság, innováció és teljesítmény.

[367] Nem írtuk, de minden esetben az újságírást magas szinten űző szakemberek tevékenységét, a szakmai és etikai standardokat és/vagy a médialogikát vesszük alapul. Avagy a plurális média, az oknyomozó újságírás, a média őrködő szerepének érvényre jutása, mint ideálállapot, jelenti a kommunikációs gondolkodás alapját. Ha ezen elvek valamelyike sérül, akkor az erő pozíciójából való kommunikáció, azaz a hallgatás, a különböző mértékű elzárkózás és a tagadás, ellentámadás retorikai fogásai nyernek létjogosultságot.

[368] https://www.ingerop.fr/en/who-we-are letöltés ideje: 2019. augusztus 16.

### *6.7.4. Ha veszélyben az ellátási lánc – a Norsk Hydrot ért támadás professzionális kommunikációja*

„A Hydro[369] legtöbb informatikai részlege érintett a március 18-án (hétfő) este kezdődő széleskörű kibertámadásban, így a hiba kijavításáig manuális termelésre álltak át.

A kibertámadás miatt teljesen leálltak az alumínium gyártó és megújuló energiaforrásokkal foglalkozó Hydro IT rendszerei, így érintettek a magyar, ezen belül a fehérvári termelőüzemek is. Kedd délután még a cég honlapját sem lehetett elérni. A Hydro a Fehérvár Televízió telefonos megkeresésére nem kívánt nyilatkozni." [370]

A *no comment* már régen nem tartható retorikai stratégia. Amíg a 90-es évek végén még találkoztunk vele a szakirodalomban, az internet megjelenésével, de különösen a közösségi média és a különféle mobil és okos eszközök széleskörű elterjedése óta kiveszni látszik a teoretikusok és válságstratégák felsorolásaiból. Az ok egyszerű, ha nem mi, majd valaki más hírét viszi a bajnak. Ekkor azonban már elvesztettük a lehetőséget, hogy mi szabjuk a híradások hangvételét, a sztori kontextusát. Nincsenek titkok, a szervezet dolgozóit nem némíthatjuk el, ha nem szándékos kiszivárogtatás, akkor vétlen és véletlen elszólás okozza majd a vesztünket és utána persze rögtön lesz, aki exkluzív dokumentum, hang, fotó, vagy multimédia illusztrációval szolgál a sajtónak. Ha nem a károkozás szándéka vezeti majd a fecsegőt, akkor állampolgári kötelességtudata, erkölcsi érzéke indítja arra, hogy szót emeljen a veszély/fenyegetettség vagy elszenvedett kár kapcsán.

De nézzük, mit is tett a globális alumíniumgyártó, hogy mindennek elejét vegye!

A Hydro anyavállalata (Norsk Hydro) délelőtt 9 óra 42 perckor tette közzé az első jelentést a kibertámadásról a Facebookon. A bejegyzés mindösszesen annyit tartalmazott, hogy a cég éppen kibertámadás alatt áll, a helyzettel kapcsolatos frissítéseket pedig a Facebook oldalán fogja közzétenni a vállalat. Ezzel a cég egyes számú tájékoztatási kötelezettségének eleget tett, megerősítette azt, amit nyilván többen már tudtak, sejtettek, érzékeltek, hogy baj van az IT rendszerekkel és egyúttal megadta azt is, milyen csatornán fog kommunikálni (közösségi média). Ezt hívja a kommunikációs szakma átmeneti nyilatkozatnak (bármennyire rövid és hiányos is a híradás).

Az átmeneti nyilatkozatban olyan tények megerősítését végzi el a szervezet, amely a közvéleményhez, tudomása szerint, már eljutott, és arra vonatkozóan ad még információt, hogy mikor kaphatnak részletes tájékoztatást az érintettek, érdeklődők. (A Hydro közléséből ez az időpont hiányzott.)

A további részleteket illetően a11 óra 24 perckor közzétett bejegyzésben adtak felvilágosítást. Abból derült ki, hogy már előző nap késő este megkezdődött a támadás. E bejegyzésnek az elején, már a második mondatban leszögezte a vállalat, hogy a támadás emberek biztonságát nem veszélyezteti. (Fontos üzenete annak, hogy az emberélet az első minden körülmények között.) Elmondták, hogy a károk mérséklésére koncentrálnak és arra, hogy továbbra is biztosítsák az emberek biztonságát. Elismerték, hogy olyan kiterjedt támadásról van szó, amely több üzleti folyamatot érint, ezért ahol csak lehetséges volt, kézi műveletekre tértek át. A Hydro úgy nyilatkozott, korai volna még a támadás hatásait, kiterjedését vagy ügyfelekre gyakorolt hatását megítélni. Megerősítették, hogy minden érintett hatósággal kapcsolatba léptek és a Facebookot fogják elsődleges csatornaként használni a tájékoztatásra. Időpontot nem írtak, hogy mikor nyújtanak legközelebb információkat, csak, hogy a lehető leghamarabb.

13 órakor jelentette be a Hydro, hogy 15 órakor sajtótájékoztatót tartanak az őket ért támadásról, megerősítve az előző posztban foglaltakat. Egyúttal közzétették a linket, amelyen keresztül a sajtótájékoztatót élőben követni lehetett, s a melyen keresztül a felvétel most is visszanézhető.[371] A sajtótá-

---

369 A Norsk Hydro, a világ egyik legnagyobb könnyűfém-gyártójának magyarországi gyára.

370 https://fmc.hu/2019/03/19/kibertamadas-erte-a-hydrot-a-fehervari-gyar-is-erintett/, letöltés: 2019. augusztus 2.

371 https://webtv.hegnar.no/presentation.php?webcastId=97819442&fbclid=IwAR0Ze8fLhdFw0z1_7WQS-b9wl88M1GZFgZ_H-w7bSFy9Y026pqbByqwCmZqE, letöltés: 2019. augusztus 2.

jékoztatón a moderátoron kívül a válságstáb feje (a pénzügyi igazgató), valamint a nemzetbiztonsági hatóság kiberbiztonsági igazgatója és a kommunikációs igazgató vett részt.

Március 19, 20-án, 21-én, 22-én, 25-én, 26-án, 27-én, 28-án, április 1-jén, 5-én frissítették a kibertámadással kapcsolatos információkat a cég hivatalos Facebook oldalán.[372]

Április végén már arról számolt be a szaksajtó[373], hogy a Hydronak csaknem 52 millió dollárjába került a kibertámadás az első negyedévben. A kiberbiztonságért felelős hatóság szerint a támadás a LockerGoga nevű vírust használta, ami a Ransomeware viszonylag új törzse. Fájlok titkosításával okoz kárt oly módon, hogy váltságdíj megfizetéséhez köti a titkosítás feloldását. A Hydro leszögezte, hogy nem enged a zsarolásnak, nem fizet a szerverekhez és számítógépekhez való hozzáférés visszaszerzéséért, inkább a biztonsági mentések alapján próbálja helyreállítani a rendszereit és az üzleti-termelési folyamatokat.

A támadás elsősorban a vállalat Extruded Solutions (extrudált megoldások) egységét érintette hátrányosan, amelyek termelése az első negyedévben az előző évi 362.000 tonnáról 333.000 tonnára esett vissza. Ebben az egységben továbbra is a korábbinál nagyobb fokú kézi működtetésre volt szükség.

A kibertámadásokban rejlő ipari válság-lehetőségek iskola példája ez, hiszen a Norsk Hydro üzemzavara megnövelte a globális ellátási lánc megszakadásának kockázatát. (Annál is inkább, mert az alumíniumgyártásban egy maroknyi vállalat uralja a világpiacot.) A Hydro pénzügyi vezetője úgy nyilatkozott, (üzleti szempontból) az az elsődleges, hogy visszanyerjék a konkrét vevői megrendelések adatait és megtalálják a módját a megrendelések teljesítésének. Az ellátási lánc szempontjából a Daimler AG és a Ford Motor Co., illetve a hasonlóan magas műszaki követelményeket támasztó alumíniumipari fogyasztók voltak a leginkább kritikus helyzetben.[374]

Április 9-én a Hydro már arról közölt részletes összeállítást, hogy munkatársai milyen kreatív megoldásokkal éltek a válság kezelése során. A Hydro ezzel új mítosz megteremtésbe kezdett, az incidens bénító valósága után a heroikus küzdelem képei következnek, a vállalat a hőstettekből kovácsol bizalmi tőkét. Az új üzenet immár: Okos alkalmazottak és együttműködés.[375] A hőstettek pedig csak úgy özönlenek a nemzetközi vállalati színtérről: Belgium, Németország, Franciaország, az Egyesült Királyság, Dánia. Mindezt nem csak szóban, de videóösszeállításban[376] is elénk tárja az alumíniumipar kiválósága. Jegyezzük meg, hogy a saját weboldalán megjelenő cikknek már az első két bekezdésében megidézi a vállalat saját érdemeit, hogy érintett üzletága a világ 40 országába mintegy 30.000 ügyfélnek szállít extrudált megoldásokat minden ipar számára az autóipartól a tengeri szállításig.

### *6.7.5. Kitérő: Kibertámadások a vezetői diskurzusban és a politikai retorikában*

Liisa Past készített 2015-ben retorikai elemzést[377] arról, hogy Vlagyimir Putyin orosz elnök és Petro Poroshenko ukrán elnök milyen – egyébként igen hasonlatos a „mi" és „ők" dichotómiájára építő – retorikai stratégiát alkalmazott Oroszország és Ukrajna konfliktusát illetően. A felek egyike sem

372 https://www.facebook.com/norskhydroasa/, letöltés ideje: 2019. augusztus 2.

373 Norsk Hydro Cyber Attack Cost It Nearly $52M in First Quarter, Insurance Journal, April 30, 2019, https://www.insurancejournal.com/news/international/2019/04/30/525093.htm, letöltés: 2019. augusztus 4.

374 Mark Burton and Jonas Cho Walsgard: Norsk Hydro Cyber Attack Exposes Risks of Global Supply Chain Disruptions, Insurance, Journal, March 20, 2019, https://www.insurancejournal.com/news/international/2019/03/20/521150.htm, letöltés: 2019. augusztus 4.

375 https://www.hydro.com/en-NO/about-hydro/stories-by-hydro/employees-find-creative-solutions-in-response-to-cyber-attack/?fbclid=IwAR3jZDjePu62yhzf-j7acRX2Zwt1DpINcbRBNtdSe61yJBMrnAaMn8OS2Ok, letöltés ideje: 2019. augusztus 11.

376 https://www.youtube.com/watch?time_continue=3&v=S-ZlVuM0we0, letöltés ideje: 2019. augusztus 11.

377 Past, Liisa (2015): Missing in Action: Rhetoric on Cyber Warfare, In: Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn, p. 95-102., https://ccdcoe.eu/uploads/2018/10/Ch11_CyberWarinPerspective_Past.pdf, letöltés ideje: 2019. augusztus 10.

tagadja, hogy a kibertér is a hadviselés tartománya, de nem is hangsúlyozza annak fontosságát. Az orosz politikai közbeszéd általában átlép a kiberkérdéseken, míg Ukrajna egy tágabb fogalomba építve, a hibrid háború terminust használva utal azokra. Past legfőbb kérdése az volt, hogy az államfők, mint legfőbb döntéshozók, a geopolitikában mit mondhatnak el a kibertér konfliktusairól (nemzetbiztonsági válság idején).

A legtöbb kiberművelet a nyilvánosságtól elzárt (már csak a hibrid hadviselés terminus használata okán is), de történnek hírszerzési kiszivárgások, illetve képet kaphat róluk a figyelmes elemző az nyílt forráskódú elemzések révén. A Szerző orosz és ukrán vezetői nyilatkozatokat elemzett – elsősorban angol nyelvűeket, melyeket a nemzetközi közvéleménynek szántak – azzal a céllal, hogy motivációkat, hiedelmeket és ideológiákat tárjon fel. (Olyasmibe próbál tehát betekintés nyújtani az effajta retorikai elemzés, ami nyílt fórumokon a kiberműveleteket illetően nem megvitatható.)[378]

Past elemzése rámutatott többek között arra is, hogy Vlagyimir Putiyn a 2014-ben kirobbant válság során egyszer sem használta a cyber/kiber szót. Óva int azonban mindenkit attól, hogy ezt úgy fogja fel, hogy Oroszország nem vett részt számítógépes/kiber műveletekben. Ez sokkal inkább annak bizonyítéka, hogy ezen kérdéseket Oroszország nem kívánja nyilvános fórumokon megvitatni. (Olyan olvasat is felmerült, mely szerint a kiberműveleteket az orosz államfő nem tekinti a támadás olyan külön formájának, amely jelentős szerepet játszik a két ország konfliktusában.) Persze a konkrét kibertámadásokról szóló híreket[379] a Kreml szóvivője rendre azzal utasítja el, hogy mindez csak a nyugati propaganda része, amely már sportot űz abból, hogy az országot vádolja (mindenért).[380]

Ukrajna nyilatkozatai jóval világosabbak voltak a kiberműveleteket illetően. Az elnöki nyilatkozatokban rendre megjelentek olyan terminusok, mint kiberbiztonság, Ukrajna informatikai kiberbiztonsági rendszere vagy kiber és információbiztonság. 2014-ben előbb az egyik távközlési cég jelentette, hogy ismeretlenek megsértettek egy optikai gerinchálózati kábelt, ami a Krím és az ország többi rész közti kommunikációs kapcsolat elvesztését okozta, majd az ukrán biztonsági főnök számolt be arról, hogy támadás zajlik a parlament tagjainak mobiltelefonjain. A legszofisztikáltabb támadás azonban csak ezután következett az ukrán Központi Választási Bizottság ellen az elnökválasztáskor. Hivatalosan egyik támadást sem erősítette meg Kijev.

A nemzetközi közvéleménynek szánt nyilatkozataiban Prosenko a hibrid háború szélesebb témájára reflektált többízben, a nyugat narratíváihoz igazítva mondanivalóját. A régiót érő hibrid fenyegetésekre hívta fel a figyelmet beszédében. (Mivel a hibrid hadviselésnek nincs közös definíciója, itt beleértendő az internetes propaganda, az információs műveletek és a számítógépes hackelés. Elkeseredett csatát vívnak a nem állami kibervezetők is Ukrajnában az orosz hekkerek és trollok ellen Az ő retorikájuk egyértelműen elmarasztalja a kormányt, amely nem áldoz a kiberharcra, annak ellenére, hogy egyértelmű, hogy információs hadviselés is zajlik a két ország között.

A két vezető retorikájában tehát a mi és ők, jó és rossz csatájaként jelenik meg a két ország konfliktusa, amelynek színtere a kibertér is. Egyik ország sem fordít sok figyelmet közleményeiben direkt módon a kiberhadviselésre, Oroszország csak magasszintű diplomáciai értelemben utal a kérdésre, Ukrajna pedig a hibrid hadviselés kérdésébe „csomagolja" vonatkozó mondanivalóját. Oroszország nemzeti érdekeket hirdető, Ukrajna pedig NATO- és nyugatbarát nyelvi fordulatokat alkalmaz.

Miért fontos ez nekünk? Mert a vezető és különösen az egyes számú geopolitikai vezető kiberműveletekkel kapcsolatos közlései alapján formálódik minden hazai kiberincidens társadalmi léptékű kontextusa. Rányomja bélyegét a szakmai és közbeszédre, hogy mi a politikailag korrekt, az elvárt. Felülről lefelé haladva fogja átszőni minden a kibertéma minden nyilvános megvitatását, hogy mi például a kormányzati álláspont, stílus, hangvétel, retorikai gyakorlat kibertámadások esetén.

---

[378] Feltevése, hogy ezzel feltárhatók a kiberműveletek nem kifejezett céljai, megérthetővé válik a számítógépes támadások rejtett természete. Megtudunk, tehát, általa valamit az érintet nemzetek kiberháborúval kapcsolatos nem kifejezett céljairól is.

[379] amelyekről például a FireEye számolt be

[380] Past, 2015. i.m. 97-98. o.

Különösen, mivel a hazai kiberbiztonsági intézményrendszer erősen centralizált, hatóságilag felügyelt.

Nem árt felidézni, hogy már a kétezres évek elején megjelent a trend, mely szerint a kormányok világszerte hajlanak arra, hogy eltitkolják a világ elől a hálózataikat ért csapásokat.[381] (S ekkor még volt biztonsági vezető, aki tagadta a cyberterrorizmus létezését, s úgy nyilatkozott, sem a közeli, sem a távoli jövőben nem látja realitását.)

### *6.7.6. A kormányok és a kibertámadások*

2018. szeptember 17-én számolt be róla a 168óra.hu (az MTI híranyagára hivatkozva), hogy előző nap az esti órákban egymást átfedve, három hullámban túlterheléses támadás érte a magyar kormány honlapját. A külföldi IP-címekről indított és a kormany.hu frontoldali infrastruktúráit célzó támadást a belügyminisztérium DDoS védelmi rendszere sikerrel visszaverte. A közleményben (lásd. 6. sz. melléklet) hangsúlyozták, hogy a támadás szolgáltatáskieséssel nem járt.[382]

Ez az eset jóval kisebb médiavisszhangot kapott, mint a 2016-os, a Közigazgatási és Igazságügyi Hivatal honlapját (kih.gov.hu), a kormany.hu-t és a Külgazdasági és Külügyminisztérium publikus szolgáltatásait célzó túlterheléses támadás, amelynek kommunikációjában „maszatolással" vádolták Bakondi György miniszterelnöki főtanácsadó, majd a BM-et.[383] Az újságírók érdeklődésének homlokterében olyan kérdések álltak, mint, hogy miért tartott napokig a védekezés felépítése, sikerült-e azonosítani a támadókat és a támadás célját és hogyan fordulhat egyáltalán ilyen bénító eset a magyar kibervédelemben.

2018 márciusában azonban a német kormány sem találta magát könnyű helyzetben, mikor a Berlin-Bonn gerinchálózatot érte támadás. Az eset visszásságai között a sajtó munkatársai arra a kérdésre is keresték a választ, hogy hogyan fordulhatott elő, hogy a parlamenti ellenőrző testület csak a sajtóból értesült a támadásról.[384] Bővebb felvilágosítást – tekintettel arra, hogy a támadás még folyamatban volt – nem adtak. Ennél komolyabb aggályokat ébresztettek azonban azok a lapértesülések, melyek szerint: a támadást már az előző év decemberében észleleték (és nem kommunikálták csak a legszűkebb kormányzati körökben), de az akár az év elejétől is tarthatott.

Az eset magyar vonatkozását adja, hogy a feltételezett támadó az az APT 28 és Fancy Bear álneveken ismert csoport volt, amely 2017-ben – hivatalosan meg nem erősített információk szerint - a Honvédelmi Minisztérium ellen is intézett támadást.[385] Sokatmondó a cikk záró mondat a lehetséges hazai kommunikációs stratégiákról:

„A HM nem erősítette meg a támadás tényét, de azt elmondták a 444-nek, hogy összetett védelmi mechanizmus érzékeli és értékeli a lehetséges támadásokat."

[381] Egyre kevesebb a cybertámadás, VOMIT, Index.hu, 2002.11.15. 13:19, https://index.hu/tech/jog/hack1115/, letöltés ideje: 2019. augusztus 10.

[382] Külföldi kibertámadás érte az Orbán-kormány honlapját, 168óra, 2018. szeptember 17. 15:52, https://168ora.hu/itthon/kulfoldi-kibertamadas-erte-az-orban-kormany-honlapjat-156140, letöltés ideje: 2019. augusztus 10.

[383] https://hvg.hu/itthon/20160407_kibertamadas_hackerek_kormany_hu_belugyminiszterium_bakondi, letöltés: 2019. augusztus 30.

[384] https://infoter.eu/cikk/nem-ert-veget-a-nemet-kormany-elleni-kibertamadas, letöltés ideje: 2018. augusztus 30.

[385] https://index.hu/tech/2017/03/16/a_magyar_hadugyet_is_tamadtak_az_orosz_hekkerek/, letöltés ideje: 2019. augusztus 30.

## *6.7.7. Stratégiai kommunikáció és közösségi média avagy a társadalmi kibertámadások*

A NATO Stratégiai Kommunikációs Kiválóság Központjainak munkatársai, Elina Lange-Ionatamishvili és Sanda Svetoka tanulmányukban[386] leszögezik, hogy az új kommunikációs környezet megváltoztatta a hadviselés jellegét. A valódi hadszíntér gyakorta már nem földön, vízen vagy levegőben keresendő, hanem a kibertérben, illetve kommunikációs területen. Egy nagyobb stratégia részeként ma már a közösségi média is felhasználható hírszerzésre, de emberek vagy szervezetek megtámadására is. A szerzőpáros a számítógépes környezetben végrehajtott és a kritikus infrastruktúra elemeket célzó támadások mellett felhívja a figyelmet az ún. lágy kibertámadások veszélyeire. Értik ez alatt az olyan információs támadást, amely manipulált információk révén kívánja befolyásolni a helyzetértékelést, a döntéshozatalt és az ezek nyomán meginduló cselekvést. Mivel a döntéshozatalt befolyásolják, hatásaik éppoly súlyosak lehetnek, mint a kritikus infrastruktúrák elleni támadásoknak. Érvelésük úgy szól, hogy ha ilyen információs manipulációk révén sikerül a támadónak mozgósítania támogatóit, démonizálnia ellenségét, demoralizálnia ellenségének kormányát és fegyveres erőit, egyúttal legitimizálnia saját tetteit, feleslegessé is válnak a konvencionális harcok (hagyományos fegyveres összecsapások).

A stratégiai kommunikáció (StratCom) egy olyan gondolkodásmód, amely azt jelenti, hogy a szervezet a kommunikációt a szervezeti stratégia középpontjába helyezi. Ekkor a szervezet vallja és vállalja, hogy tevékenysége narratíván alapul, és üzeneteit szavai, tettei és fizikai megnyilvánulásai koordinálásával közvetíti a különféle közönségei felé. számára. A kibertér egyre fontosabb szerepet játszik a StratCom-ban, mivel nap mint nap növekszik a modern technológiáktól, a számítógépes hálózatoktól és az internettől való függőségünk. A kiberterületet gyakran használják konfliktusokban az ellenfél kommunikációs rendszereinek kiiktatására. Az ukrán konfliktus azonban megmutatta, hogy a kibertér szerepet játszhat egy narratíva-vezérelt művelet végrehajtásában is, ahol a legfőbb célpontok nem a gépek vagy hálózatok, hanem az emberi elmék. Az internetet és a közösségi médiát, azon tulajdonságuknál fogva, hogy képesek gyorsan alacsony költségek mellett megsokszorozni az információkat, egyre inkább használják propaganda, információs hadviselés és befolyásolás céljából. Ezek mindegyike megváltoztathatja a célközönség észlelését és viselkedését.

A közösségi média egy olyan felhasználó-vezérelt gyorsan változó környezet, ahol könnyű vírusként terjedő üzenetet küldeni és nehéz az eredeti forrást visszakeresni, ellenőrizni a tények hitelességét, elkülöníteni a tényeket a fikciótól (az eredetit a manipulálttól). Nem véletlen, hogy egyre vonzóbbnak tűnik (a szerzők és más teoretikusok számára is) a *társadalmi kibertámadás* fogalmának bevezetése. Az ukrán válság során megfigyelt társadalmi kibertámadások arra a feltevésre vezettek, hogy a támadások legalább egy részét szervezett módon hajtják végre egy nagyobb befolyásolási stratégia részeként.

Az észlelés, attitűd és viselkedés befolyásolása tekinthető katonai tevékenységnek, amelynek eszköze gyakorta a pletyka: a gyűlölet, félelem és remény tárgyú szóbeszéd. A közösségi média pedig a kapcsolataik által összekötött emberek megcélzását teszi lehetővé. Mivel az információ egy ismeretségen és ebből fakadóan bizalmon alapuló hálózaton keresztül érkezik, hitelessége a felhasználó számára nagyobb, mint a hivatalos tömegtájékoztatásé.

A társadalmi kibertámadás, hamis állítások szerint vagy anonim módon jár el, vagyis manipulált jelet bocsát ki a közösségi médiába, vagy meglévő jelet manipulál a kívánt hatások elérése érdekében, hogy káoszt, pánikot keltsen, zavargásokhoz vezessen. Az ilyen típusú számítógépes támadás másképp néz ki, mint a számítógépes környezet hagyományos (pl. információbiztonsági képzésekben tanított) támadásai, mivel ezeknek a támadásoknak pusztán pszichológiai következményei vannak. Ám ezt ne becsüljük alá, a pánik vezethet tömegtüntetésekhez, zavargásokhoz, tömeges pénzfelvételhez a bankokból vagy olyan csoportok vagy egyének elleni szervezett támadásokhoz, akiket a kommu-

[386] Lange, Elina-Sveotka, Ionatamishvili Sanda (2015): Strategic Communications and Social Media in the Russia Ukraine Conflict, In: In: Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn, 103-111. o.

nikációban ellenségként ábrázoltak. A közösségi média hirdetőfelületeinek, üzenőfalainak feltörése nem volt más az orosz-ukrán konfliktusban, mint kibertámadás lefolytatása narratívák és pletykák terjesztésével, amelyek mind manipulált információkon alapultak.

Az oroszpárti erők leckét adtak a világnak. A Twitter és a YouTube segítségével ismeretlen támadók elhallgatott telefonbeszélgetést tártak a nyilvánosság elé, amely Victoria Nuland amerikai külügyi államtitkár és Geoffrey Pyatt kijevi amerikai nagykövet között folyt. Ez példája volt az információs rendszer technikai kihasználásának, az ügy sajtókommunikációja pedig a nyugat elleni, közösségi médián keresztül elkövetett pszichológiai támadásnak.[387] Az oroszországi hangok szisztematikusan gerjesztették a félelmet, a szorongást és a gyűlöletet Ukrajna orosz (és más nem ukrán) lakosságának körében. A manipulált tartalmak az ukrán hadsereg túlkapásairól, kínzásokról, tömegsírokról és szervkereskedelemre használt civilekről szóltak, de megjelentek álhírek gyermekek katonai toborzásáról, nehézfegyverek polgári lakosság elleni bevetéséről, sőt, még kannibalizmusról is. Egy orvosi álprofil által az orosz VKontakte közösségi oldalon közzétett személyes bejegyzés áldozatok élve elégetéséről 24 óra alatt 5000 megosztást ért el, mígnem hoaxnak minősítették.

A stratégiai kommunikáció szempontjából mindezek alapvetőek. Meg kell érteni a közösségi médiában végrehajtott információs műveleteket (beleértve a dezinformációt és lélektani hadviselést), belátni jelentőségüket, hiszen alapvetően befolyásolják a politikai (vagy más) narratívát. Fontos fellépni a közösségi médiában megjelenő manipulált, nem valós, hitelt rontó tartalmak ellen és a tényeket elkülöníteni a fikciótól. Ehhez jó támpontot ad az információt terjesztő felhasználói fiókok létrehozásának dátuma, tartalmaik hitelessége, kapcsolati hálójuk valódisága. Ezt az elemzést azonban precízen és időben kell elvégezni, amelyre kevés szervezetnek, de általában még a bűnüldöző hatóságoknak sincs kapacitása. A várakozások szerint a jövőben az infrastruktúrára és az emberi pszichológiára irányuló tevékenységek kombinációját a jövőben még kifinomultabb és kiszámíthatatlanabb módon fogják használni a helyszíni a katonai műveletek támogatására világszerte.

A szerzők következtetése, hogy a kormányoknak és a védelmi szervezeteknek is javítaniuk kell képességeiket a közösségi média kártékony felhasználásának felismerése terén. Figyelemmel kell kísérniük és elemezniük a megjelenő tartalmakat, hogy idejében felvehessék a harcot az információs támadások e puha válfajával. A kampányok szervezettségének feltárása és hatásainak elemzése azonban komoly kapacitásokat igényel.

A polgári újságírók tevékenysége bebizonyította, hogy a tényfeltárás hatékony eszköz lehet a dezinformáció hatásainak enyhítésére, de az ellenpropagandába való bekapcsolódásuk csak olaj a tűzre, amely kiterjeszti az információs háborút. A humor valószínűleg hatékonyabb fegyver lehet az agresszív propaganda ellen, legalábbis ezt mutatja az orosz-ukrán konfliktus. (Példának a @DarthPutinKGB or @Sputnik_Intl kezdeményezést hozzák.)

Legvégül Lange-Ionatamishvili és Svetoka arra hívják fel a figyelmet, hogy egy (nemzetet) egységbe fogó stratégiai narratíva, az állampolgárok kritikus gondolkodásra és médiatudatosságra nevelése, a médiakultúrájuk fejlesztése nyújthat védelmet leginkább az ellenséges propagandával szemben. Azonosítás, kihívás, tanulás és felkészülés, így összegzik tehát minden ország kormánya és védelmi intézményrendszere előtt álló feladatokat.

[387] Azóta az orosz dezinformációs gépezetről és a közösségi média szerepéről számos tanulmány született már. Alexander Lawrence például nyílt forráskódú információk alapján mutatott rá a Kreml-barát webkampányok működési elveire és gyakorlatára. (Open-Source Information Reveals Pro-Kremlin Web Campaign,13 July 2015, https://globalvoices.org/2015/07/13/open-source-information-reveals-pro-kremlin-web-campaign/, letöltés ideje: 2019. augusztus 17.)

## *6.7.8. Választási kiberincidensek kommunikációjának tervezése*

A választásokkal kapcsolatos kiberincidensek a számítógépes tevékenységek széles spektrumát ölelik fel, és mivel általuk megingatható a demokratikus intézményekbe vetett (köz)bizalom, szólnunk kell erről is. A választások tisztaságának, sértetlenségének (integritásának) megőrzése közérdek, kommunikációjuk sem lehet esetleges. A politikai szereplőktől ma már e téren is profizmust és felelősségvállalást vár a közvélemény.

A bizalom fenntartásának központi eleme a megfelelő időben történő pontos tájékoztatás, a fals információk kiszűrése és korrigálása, különösen a közösségi média színterein. Mindez akkor igazán hatékony, ha a párt(ok) tisztviselői és a joghatóság nyilatkozattevői összehangolják üzeneteiket, közöttük a koordináció szoros, folyamatos.

A Német Szövetségi Parlament rendszerébe való 2015-ös behatolás, majd azt követően a hollandok[388] és norvégok[389] arról szóló döntése 2017-ben, hogy a szavazatokat kézzel összesítik a választások alkalmával (tartva az esetleges hackertámadásoktól), megerősítették, hogy a politikai választások megzavarásától való félelem erősödik. Nyilvánvalóvá vált, hogy a politikai pártok biztonsági stratégiáiban külön fejezetet kell szentelni a számítógépes támadásoknak, kivédésüknek és azok válságkommunikációjának. A nyilatkozatoknak ez esetben is azt kell tükrözni, hogy a párt tisztségviselői kompetens személyként felelős módon kezelik a helyzetet. Épp ezért alapszabály például, hogy csak olyan tényt közöljenek, amely nem fog változni. Mivel a politikusok szavahihetőségét amúgy is kételyek övezik, a kezdeti információk későbbi módosítása alááshatja a megbízhatóságukat a közvélemény szemében. (Bizonytalan információ e tekintetben például a támadás kiterjedtsége, a hatásai, az okozott kár, a folyamatok időbelisége.)

A szakértők nagyfokú körültekintést javasolnak már csak annak okán is, hogy a számítógépes válságok nagyban különböznek más típusú válságoktól, így például abban:

- Az első közléskor minden bizonnyal a megszokottnál is kevesebb információval fog rendelkezni, ennek ellenére kell tudnia meggyőzni a közvéleményt arról, hogy kézben tartja az irányítást és magabiztosan és hozzáértően kezeli a válságot.
- Minden bizonnyal lesznek olyan (szak)újságírók – akiknek megfelelő kapcsolataik vannak, ismerik a technikai és politikai részleteket (hiszen egyébként is kibertémákban publikálnak) és megbízható forrásokból akár olyan részleteket is ismernek, amelyeket a nyilatkozattevő még nem.
- Az események koordinált együttműködést igényelhetnek olyan kormányzati és nem kormányzati szervek között, amelyek egyébként nem működnek együtt a mindennapokban.
- A politikai kampányok infrastruktúráinak támadásai lépcsőzetesen haladva átjuthatnak hagyományos joghatóság határain.
- A kibertámadások/incidensek alááshatják a jelöltek és más politikusok, illetve a különböző politikai erők iránti bizalmat, megingathatják a demokratikus választási rendszerbe vetett bizalmat.
- A pánikot és felesleges riadalmat kerülő őszinte kommunikáció válik szükségessé.

<u>Minden aktor számára megtehető lépések:</u>

- a kommunikációs tervet igazítsa a műszaki (technikai) válságkezelési tervhez, mindkettőt frissítse rendszeresen

[388] https://index.hu/kulfold/2017/02/01/hollandiaban_annyira_felnek_az_orosz_hackerektol_hogy_megint_kezzel_szamoljak_a_szavazatokat/, letöltés ideje: 2019. augusztus 14.

[389] https://korkep.sk/cikkek/kulugyek/2017/09/01/norvegiaban-tartanak-a-hackerektol-a-szavazatokat-kezzel-szamoljak-majd/, letöltés ideje: 2019. augusztus 14.

- tesztelje a terveket különféle szimulációs során a párt különböző szintjein
- rendszeresen végezze el a fenyegetések elleni frissítéseket, különös tekintettel a választásokra
- ápolja a kapcsolatokat azokkal a szakértőkkel és tisztviselőkkel, akik relevánsak lesznek egy esetleges kiberincidens kivizsgálásában és kezelésében
- tájékoztassa a nyilvánosságot az elvégzett munkáról (a felkészülés lépéseiről)
- alakítsa a közvélemény előzetes várakozásait a várható fenyegetések vonatkozásában, magyarázza el a választás folyamatára gyakorolt várható/lehetséges hatásukat

A kiberbiztonság a politikai kampányokban ma már mindenki felelőssége. A napvilágra került támadások kiváltó oka számos esetben az emberi hiba vagy mulasztás, éppen ezért a jelölteknek és a kampányfőnököknek az egyik legfőbb feladata, hogy a biztonságtudatosságot beépítsék a stáb működésébe. A szoftverek mellett az emberi döntések fontosságát is nyilvánvalóvá kell tenni. A legjobb kampányok már egyértelművé tették, hogy a recept a következőkből áll: kemény munka, konzisztens üzenet, a csoport iránti hűség, a (jó) biztonsági protokoll követése.[390]

3 dolgot kell elsőként mérlegre tennünk, hogy a kiberválságok kommunikációját tervezni tudjuk:
- a kampány környezete (széles értelemben vett kontextusa)
- azok a veszélyek és fenyegetések, amelyekkel a kampány szembesül
- a kiberkockázatok kezelésének fontossága

A kampányok sérülékenyek, mert:
- természetüknél fogva átmeneti jellegűek (adott választási ciklusra szólnak)
- nincs idejük és pénzük átfogó, hosszútávra szóló és kiforrott biztonsági stratégiák kimunkálására
- sok embert foglalkoztatnak, a személyzeti felvételi folyamat gyors, szinte nins betanítási/betanulási idő
- sokan saját hardver eszközükön dolgoznak (elve fertőzött eszközzel lépnek a csapatba)
- a kampányok nagy földrajzi távolságokat is áthidalhatnak, a személyzet nem feltétlenül találkozik személyesen, sokan távmunkásként vesznek részt
- a dolgok gyorsan zajlanak, olykor hirtelen lépéseket kell tenni, melyeknek nagy a tétje, s olyankor sok mindenre nem jut idő, a (kiber)biztonságra sem
- nagy a hibázás lehetősége, nagy a terhelés
- emellett sok szenzitív információval dolgoznak: választói adatok, közvéleménykutatások és ellenzéki kutatások, azok adatbázisai és kutatási jelemtései, sebezhetőségi tanulmányok és támogatói névjegyzékek, címlisták, a személyzeti adatbázis, politikai tervdokumentumok és levelezések stb.

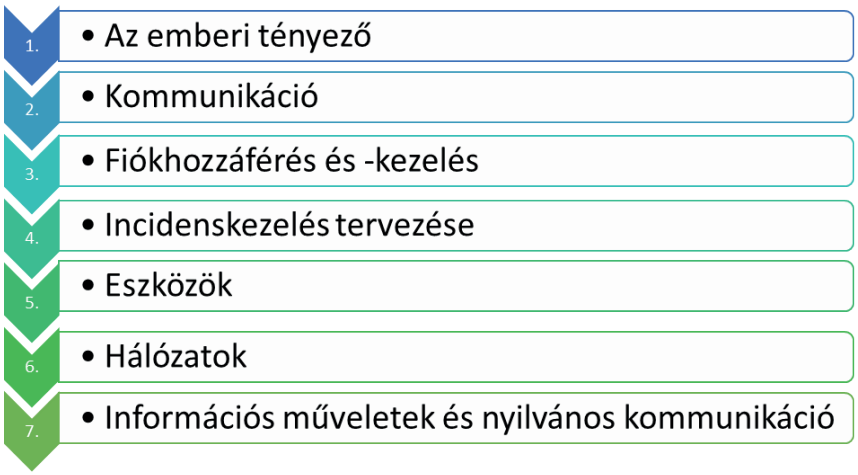
Egy politikai kampányban önmagában valamely kibertámadás híre súlyos következményekkel jár. Gondoljunk csak arra, hogy elvonja a média és rajta keresztül a közvélemény figyelmét a politikai kampányüzenetről. Akadozhat a támogatókkal folyó kommunikáció, létfontosságú pénzeszközöktől eshet el a jelölt. Ha kiszivárognak támogatói adatok, súlyos jogi következményekkel kell adott esetben szembe nézni. Az adatszivárgás eltántoríthat más adományozókat. A személyi számítógépek és szerverek elleni támadás akár hetekre is lelassíthatja vagy ellehetetlenítheti a munkát. Önmagában a rend felborulása kedvez a politikai riválisoknak. A lejáró kampányok kezébe ászokat ad az ellenfél sebezhetősége (felkészületlen, inkompetens, gyenge, felelőtlen stb.).

[390] The Cybersecurity Campaign Playbook, European Edition, Defending Digital Democracy Project, May 2018, Belfer Center for Science and International Afairs Harvard Kennedy School, Cambridge. https://www.belfercenter.org/sites/default/files/files/publication/EuropeanCampaignPlaybook.pdf, letöltés ideje: 2019. 7. o.

Mivel bármifajta dezinformáció, manipulált és kiszivárogtatott információ valódi hatással van (lehet) a választások kimenetelére, azok a mechanizmusok, amelyek biztosítják az adatok védelmét és a kommunikációs csatornák fenntartását minden korábbinál fontosabbakká váltak.

Az információbiztonsági szakértőknek a kampányfőnökökkel kell igen szorosan együttműködniük. Kampányszakértőként ugyanis ők határozzák meg, mekkora fontosságot tulajdonítanak a kiberbiztonságnak, ennek tükrében mennyit áldoznak rá a kapacitásokból. Ők határozzák meg a legfontosabb adatok és rendszerek körét, döntenek olyan alapvető kérdésekben, mint hogy milyen adatokhoz milyen felhasználói kör férjen hozzá, mely adatokat kell megőrizni vagy eldobni. A kampány fejeként kezükben a döntés, hogy mennyi időt szánnak képzésre, a biztonságtudatos viselkedést mennyire jelenítik meg példamutatóan a stábtagok számára. Tehát technikai és emberi felelősei is a kockázatmenedzsmentnek. Tőlük holisztikus szemléletet várunk. A Harvard szakértői a felkészülés (prepare), a védelem (protect) és a fenntartás (persist) hármasában látják a sikeres incidensmenedzsment zálogát.[391]

Az ajánlások kétféle védelmi szintet különböztetnek meg, a jó szintet, amely a legszükségesebb minimumelvárásokat fogalmazza meg és a továbbfejlesztett szintet, amelyre törekedni kellene minden kampányban (ha idő, pénz, kompetencia stb. rendelkezésre áll). (Az ellenőrző listát lásd a 7. sz. mellékletben)




*A politikai kampányok biztosításának 7 lépcsős modellje*
*Forrás: saját készítésű ábra D3P, 2018, 14 nyomán*

A Harvard Belfer Centre hétlépcsős modelljéből számunkra az első és utolsó lépés kifejtése tűnik indokoltnak, mert ez tartalmaz konkrét kommunikációs feladatokat. (Nyilván a többi lépés sem mellőzheti a hatékony kommunikációt, de a képzésbe résztvevők ezt más tantárgyak során vagy korábbi képzésükben már elsajátították.)

Első helyen azért szerepel a humán tényező, mert a legjobb műszaki megoldások esetén is ezen bukhat a biztonság, ha a személyzet nem tartja be a(z alapvető) szabályokat (sem). A kiberbiztonsági gyakorlatok és szimulációk sikere is a dolgozókon és biztonsági kultúra megalapozásán múlik. Ehhez legjobb eszköz az onboarding, azaz az új belépők kiberbiztonsági alapképzése a számukra egyébként is indított más képzésekkel egyetemben, vagy azok részeként. De éppen így célszerű más (senior és szinten tartó vagy rendszeres továbbképzési) képzési programokba is beépíteni a kiberbiztonság témát. A kiberbiztonság szempontjából érzékeny területen dolgozók és kulcspozícióban lévők (sajtókapcsolati munkatársak, rendszergazdai jogosultságokkal rendelkezők stb.) számára pedig speciális, kibővített képzések indítása lehet indokolt. Harmadik tényezőként pedig a vezetők és senior munkatársak példamutató magatartása lehet a biztonságtudatos szervezeti kultúra záloga. (Rossz hír, hogy az informatikai vezető e kérdésben nem mindig a leghatékonyabb üzenethordozó. Őt „technikai" személyként azonosítják.) A kommunikációs feladatok között szerepel még a kiberbiztonsági fejlesztő cégekkel és biztonsági szakértőkkel való kapcsolatok kiépítése.

[391] Playbook, 2018. i.m. 11. o.

## 6.8. Zárszó helyett

Jelen tananyag az ideálállapotot mutatja be. A vonatkozó ajánlások felhívják a figyelmet arra, hogy a hosszú távú eredmények, a bizalom helyreállítása érdekében milyen szempontokat kell szem előtt tartani, Ez nem jelenti ugyanakkor azt, hogy ne volnánk tisztában azzal, hogy az itt leírt elvek számos esetben sérül(het)nek, a szervezet hatalmi és kommunikációs kultúrája okán, valamilyen hatósági korlátozás miatt vagy a tulajdonosi, illetve egyéb üzleti érdekek védelmében.

## 6.9. Mellékletek

### *1. sz. melléklet: Ellenőrzőkérdések a szervezet számára*[392]

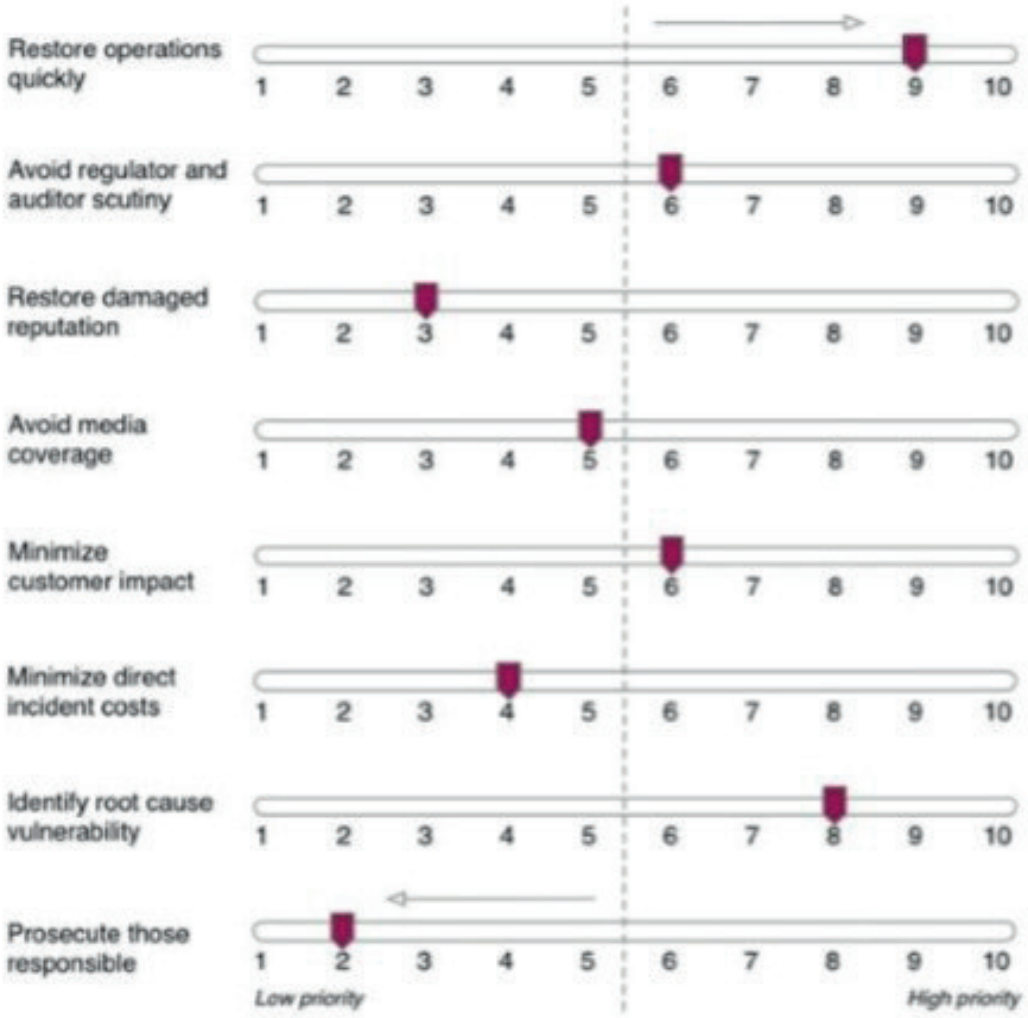
Rendelkezésre áll a megfelelő válságkezelő csapat?
Mit kell jelenteni, mikor és kinek?
Van időről-időre felülvizsgált és begyakorolt válságterv, amelynek végrehajtását a személyzetnek volt módja begyakorolni?
Hogyan építi be a szervezet a válságtréningek (és később az éles helyzetek) tanulságait a működésébe?
Mikor kell értesíteni a csúcsvezetőket és a válságstábot?
A stratégia felöleli a külső és belső koordinációt is?
Hogyan segíti a szervezet (hogyan segítik a folyamatok) az érintetteket?
Melyek a legjobb (leghatékonyabb) kommunikációs csatornák?
Milyen esemény és válságkezelési technikákat alkalmaz a szervezet?
Milyen technikai képességekkel vagyunk felvértezve és melyek hiányoznak?
Milyen bűnügyi, kriminalisztikai források állnak rendelkezésre, milyen eszközökhöz és adatbázisokhoz van hozzáférése a szervezetnek?
Hogyan gyűjti és használja fel a szervezet a fenyegetésekkel kapcsolatos információkat?
Mely üzleti folyamatok és alkalmazások kritikusak a szervezet működése szempontjából?
Milyen infrastruktúra szükséges az elérhető legmagasabb szintű védelem biztosításához?
Hogyan lehet visszatérni a teljeskörű működéshez?
Hogyan tudják támogatni a helyreállítást az alkalmazottak, a beszállítók és az érintettek?
Mik az esemény-bejelentési kötelezettségek és követelmények?
Melyek a szabályozási és a harmadik felet érintő kötelezettségek?
Mikor és hogyan tájékoztassa a szervezet a rendészeti szerveket, (a bűnügyi) hatóságokat?
Hogyan befolyásolja egy egyszeri partikuláris esemény vagy események bizonyos mintázata a szervezet megfelelőségi politikáját és magatartását?
Sikerült azonosítani az IT és üzleti folyamatok gyökereit, okait?
Készült a fenyegetettség, illetve sebezhetőség megszüntetésére terv?
Sikerült felszámolni vagy minimalizálni a kiváltó okokat?
Mi a tanulság, hogyan tudjuk alkalmazni?

[392] Deloitte, 2016, i.m.

*2. sz. melléklet: Incidens-közzétételi stratégia folyamatábrája*


*Forrás: Kulikova et al. i.m. 2012. 107. o.*

*3. sz. melléklet: Az ún. incidenskezelés-prioritási csúszka*




*Forrás: Kulikova et al. 2012. i.m. 108. o.*

*4. sz. melléklet: A Norsk Hydro első hivatalos közleménye a kibertámadásról*


*Forrás: https://www.facebook.com/pg/norskhydroasa/posts/?ref=page_internal*

## *5. Sz. melléklet: A Norsk Hydro második hivatalos közleménye a kibertámadásról*

„Update on cyber-attack against Hydro:
Hydro became subject to an extensive cyber-attack late Monday evening CET
The attacks have not affected people safety. Hydro's main priority now is to limit the effects of the attack and to ensure continued people safety.

The attack has impacted operations in several of the company's business areas globally. IT systems in most business areas are impacted and Hydro is switching to manual operations where possible. Hydro's power plants are running normally on isolated IT systems.
*It is too early to assess the full impact of the situation.
*It is too early to assess the impact on customers.
We have established dialogue with all relevant authorities.
Hydro has established Facebook as our main external communication channel. We will give updates as soon as possible."
*Forrás: https://www.facebook.com/pg/norskhydroasa/posts/?ref=page_internal*

## *6. sz. melléklet A Belügyminisztérium sajtóközleménye*

2018. szeptember 17., hétfő 15:17

A Belügyminisztérium közleménye

Budapest, 2018. szeptember 17., hétfő (OS) - Eredményes védekezés

Egymást átfedve, három hullámban, nem magyarországi IP címekről elosztott túlterheléses (DDoS) támadás érte 2018. szeptember 16-án 21 óra 8 perc és 22 óra 32 perc között a kormany.hu-t. A támadás legjelentősebb időszaka 21 óra 30 perc és 21 óra 50 perc között történt és az UDP protokollon a kormany.hu frontoldali infrastruktúra felé irányult.
A Belügyminisztérium 2017-ben megvásárolt, letelepített és üzemeltetett DDoS védelmi eszközrendszere a külföldről érkező támadásokat sikeresen elhárította, az azokban aktívan résztvevő IP címek letiltása megtörtént. A támadások ideje alatt szolgáltatáskiesés nem történt.

Kiadó: Belügyminisztérium

*Forrás: Országos Sajtószolgálat, MTI.hu, http://os.mti.hu/hirek/138427/a_belugyminiszterium_kozlemenye, letöltés ideje: 2019. augusztus 10.*

*7. sz. melléklet: Top 5 ellenőrzőlista politikai kampányokhoz*

1. Építsd ki az információbiztonság-tudatosság kultúráját!
Vedd komolyan a kiberbiztonságot, vállalj felelősséget érte, képezd a személyi állományt, beleértve az önkénteseket is és mutass jó példát! (A sérülések elsődleges oka valamilyen emberi hiba.)

2. Használd a felhőt!
A felhőalapú szolgáltatások biztonságosabbak lesznek, mint, amit a szűkre szabott költségvetésből magad elő tudnál teremteni.

3. Használj kétfaktoros hitelesítést és erős jelszavakat!
Minden fontos fiókhoz, e-mail vagy tárolási szolgáltatáshoz, közösségi médiához használj második védelmi réteget (mobilalkalmazást vagy fizikai kulcsot). Tartsd be a jelszavak létrehozásának és használatának alapvető szabályait (soha ne ismételd a korábban már használt jelszót).

4. Használj titkosított üzeneteket érzékeny beszélgetésekhez és anyagokhoz!
A rejtjelezés csökkenti annak valószínűségét, hogy üzeneteidet, ha illetéktelenek meg is szerezték, a tartalmához is hozzáférjenek.

5. Tervezz és készülj fel!
Készíts tervet a biztonsági esemény bekövetkezésének esetére, tudd, kit kell hívnod, mik a kötelezettségeid, áll készen a gyors és hatékony belső és külső kommunikációs válaszadásra.[393]

## 6.10. Irodalomjegyzék


- Anthonissen, Peter Frans (2009): *Kríziskommunikáció. A válságkezelés és reputációmenedzsment pr-stratégiái*, HVG, Budapest.
- Bernáth László (szerk.) (é.n.): *Műfajismeret*, Sajtóház Kiadó, Budapest. 46. o.
- Coombs, Timothy W. (2012): *Ongoing Crisis Communication. Planning, Managing and Responding*, SAGE, Thausend Oaks, California.
- *Crisis Communication Handbook*. SEMA's Educational Series 2003:1, Swedish Emergency Management Agency, Stockholm.
- Fehér Judit (2018): Információbiztonsági események kezelése egy belügyi szervnél, *Rendvédelem*, 2018. különszám, 5-28. o.
- Fekete Ferenc-Sándor Imre (1997): *Válságkezelés és kríziskommunikáció*, BKE, Budapest.
- Hawkins, Nick (2017): Why communication is vital during a cyber-attack, *Network Security*, March 2017, pp.12-14.
- Horváth Gergely Krisztián (2014): *Incidens-menedzsment, BCP, DRP integráció A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez*, NKE, Budapest.
- Herendy Csilla-Kriskó Edina (2012): *Közkapcsolat-tartás gyakorlata*, NKE KTK, Budapest.
- Holstein, William D. (2011): *Médiaszelidítők*, Akadémiai Kiadó, Budapest.


[393] https://www.belfercenter.org/sites/default/files/files/publication/EuropeanCampaignPlaybook.pdf, letöltés ideje: 2019. augusztus 12.

- Kovács László (2015): *Kiberhadviselés Magyarországon* (előadás), NKE, Budapest. https://docplayer.hu/840415-Kiberhadviseles-magyarorszagon-keszitette-kovacs-laszlo-budapest-2015-marcius-24.html, letöltés ideje: 2019. július 21.
- Kovács László (2018): *Kiberbiztonság és -stratégia*, Dialóg Campus, Budapest. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_Kiberbiztonsag_es_strategia.pdf, letöltés ideje: 2019. július 21.
- Krasznay Csaba (é.n.): *Információbiztonság vs. kiberbiztonság – az okos város szempontjából*, NKE Kiberbiztonsági Akadémia, Budapest. https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf, 2019. augusztus 3.
- Kriskó Edina (2013): *Szervezeti kommunikáció*, NKE VTKI, Közigazgatási Vezetői Akadémia, ÁROP-2.2.13., tréning tananyag, Hatékony vezetés modul, Vezetői kommunikáció almodul, NKE, Budapest.
- Kulikova, Olga-Heil-Ronald-Berg Jan van den-Peters, Wolter (2012): Cyber Crisis Management: A decision-support framework for disclosing security incident information, *2012 International Conference on Cyber Security*, Washington, DC, USA, 14-16 Dec. 2012. (IEEE), DOI: 10.1109/CyberSecurity.2012.20
- Lange, Elina-Sveotka, Ionatamishvili Sanda (2015): Strategic Communications and Social Media in the Russia Ukraine Conflict, In: In: Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn, 103-111. o.
- László Gábor (2014): *Kockázatértékelés, kockázatkezelés*, NKE, Budapest.
- Luiijf, Eric-Schie, Tom van-Ruijven, Teo van-Huistra, Auke (2016): *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers*, TNO, Rijswijk, Netherlands, https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf, letöltés: 2019. augusztus 21.
- *Managing a Cyber Attack on Critical Infrastructure: Challenges of Federal, State, Local, and Private Sector Collaboration, Intelligenece and National Security Alliance*, INSA Tabletop Exercise After-Action Report, INSA, August 2018, https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf, letöltés ideje: 2019. augusztus 21.
- Maretta, Kent-Vedadib, Ali-Durcikovac, Alexandra (2019): A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses, *Computers & Security,* Volume 80, January 2019, Pages 25-35., https://doi.org/10.1016/j.cose.2018.09.004
- Mitchell, Ronald K.- Agle, Bradley R.- Wood, Donna J. (1997): Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts, *The Academy of Management Review*, Vol. 22, No. 4 (Oct., 1997), pp. 853-886.
- Mossburg, Emily-Gelinne, John-Calzada, Hector (2016): *Beneath the surface of a cyberattack. A deeper look at business impacts*, Cyber Risk, Deloitte.
- Muha Lajos (2007, 2015): A kritikus információs infrastruktúrák védelme, RelNet Technológia Kft., http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf, letöltés ideje: 2019. augusztus 23.
- Németh Erzsébet (2006): *Közszereplés*, Osiris, Budapest.
- Nyárády Gáborné-Szeles Péter (é.n.): *Public Relations I-II.* (II. kötet), Perfekt, Budapest.
- Quigley, Kevin-Burns, Calvin-Stallard, Kristen (2015): 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection, *Government Information Quarterly* 32 (2015) 108–117.

- SELLNOW, Timothy L.-SEEGER, Matthew W. (2013): Theorizing crisis communication, Wiley-Blackwell, West-Sussex. UK.
- Szádeczky Tamás (2014): *Információbiztonsági szabványok*, NKE, Budapest.
- *The Cybersecurity Campaign Playbook*, European Edition, Defending Digital Democracy Project, May 2018, Belfer Center for Science and International Afairs Harvard Kennedy School, Cambridge.
- https://www.belfercenter.org/sites/default/files/files/publication/EuropeanCampaignPlaybook.pdf,
  letöltés ideje: 2019. augusztus 12.
- *Understanding Local Cyber Resilience. A guide for local government on cyber threats and how to mitigate them*, March 2015 Department for Communities and Local Government, London.
- Zaballos, Antonio García -Jeun, Inkyung (2016): Best Practices for Critical Information Infrastructure Protection (CIIP) Experiences from Latin America and the Caribbean and Selected Countries, Inter-American Development Bank and Korea, Internet & Security Agency, IDB, Washington.
- Zaharia, Andra (2019): 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2019 EDITION],
  https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/,
  letöltés ideje: 2019. július 11.
- Zsolt Péter (2003): Médiaháromszög, EU-Synergon, Vác.
- Az európai szervezetek 79%-a szeretné tudni, hogy ki az őket ért kibertámadás elkövetője, ProfitLine, 2019. 03. 29.,
  https://profitline.hu/Az-europai-szervezetek-79-a-szeretne-tudni-hogy-ki-az-oket-ert-kibertamadas-elkovetoje-391128,
  letöltés: 2019. augusztus 26.
- https://hvg.hu/tudomany/20180525_orosz_hacker_cisco_router_vpnfilter_virus_kibertamadas,
  letöltés ideje: 2019. augusztus 11.
- http://neih.gov.hu/alerts?page=6,
  letöltés ideje: 2019. augusztus 11.
- https://nki.gov.hu/wp-content/uploads/2019/06/201906-OUCH-June-Hungarian-P1.pdf,
  letöltés ideje: 2019. augusztus 11.
- https://nki.gov.hu/wp-content/uploads/2019/03/20_Biztonsagos-internethasznalat.pdf,
  letöltés ideje: 2019. augusztus 11.
- https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf,
  letöltés ideje: 2019. július 21.
- https://threatmap.checkpoint.com/ThreatPortal/livemap.html,
  letöltés ideje: 2019. augusztus 7.
- https://cybermap.kaspersky.com/,
  letöltés ideje: 2019. augusztus 7.
- https://cybermap.kaspersky.com/stats/#country=122&type=oas&period=m,
  letöltés ideje: 2019. augusztus 7.
- http://naih.hu/files/NAIH-2019-2471-hatarozat.pdf,
  letöltés: 2019. július 12.
- https://hvg.hu/itthon/20190712_Elhagytak_egy_pendriveot_rajta_a_BRFK_osszes_rendorenek_adataival,
  letöltés: 2019. július 12.
- https://888.hu/amerika-london-parizs/sulyos-kibertamadas-tortent-franciaorszagban-4160485/,
  letöltés ideje: 2019. augusztus 2.

- https://webtv.hegnar.no/presentation.php?webcastId=97819442&fbclid=IwAR0Ze8fL-hdFw0z1_7WQSb9wl88M1GZFgZ_H-w7bSFy9Y026pqbByqwCmZqE, letöltés: 2019. augusztus 2.
- https://www.facebook.com/norskhydroasa/, letöltés ideje: 2019. augusztus 2.
- Norsk Hydro Cyber Attack Cost It Nearly $52M in First Quarter, Insurance Journal, April 30, 2019,
- https://www.insurancejournal.com/news/international/2019/04/30/525093.htm, letöltés: 2019. augusztus 4.
- Mark Burton and Jonas Cho Walsgard: Norsk Hydro Cyber Attack Exposes Risks of Global Supply Chain Disruptions, Insurance, Journal, March 20, 2019, https://www.insurancejournal.com/news/international/2019/03/20/521150.htm, letöltés: 2019. augusztus 4.
- https://www.hydro.com/en-NO/about-hydro/stories-by-hydro/employees-find-creative-solutions-in-response-to-cyber-attack/?fbclid=IwAR3jZDjePu62yhzf-j7acRX2Zwt1DpINcbRB-NtdSe61yJBMrnAaMn8OS2Ok, letöltés ideje: 2019. augusztus 11.
- https://www.youtube.com/watch?time_continue=3&v=S-ZlVuM0we0, letöltés ideje: 2019. augusztus 11.
- https://index.hu/kulfold/2017/02/01/hollandiaban_annyira_felnek_az_orosz_hackerektol_hogy_megint_kezzel_szamoljak_a_szavazatokat/, letöltés ideje: 2019. augusztus 14.
- https://korkep.sk/cikkek/kulugyek/2017/09/01/norvegiaban-tartanak-a-hackerektol-a-szavazatokat-kezzel-szamoljak-majd/, letöltés ideje: 2019. augusztus 14.

# 7. JOGSZABÁLYTÁR

## 7.1. Magyar jogszabályok

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
  https://net.jogtar.hu/jogszabaly?docid=a0100108.tv
- 2001. évi XXXV. törvény az elektronikus aláírásról
  https://mkogy.jogtar.hu/?page=show&docid=a0100035.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
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1000157.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
- 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
- 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=148205.295314
- 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.korű
- 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
  https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV
- 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
  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
- 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
- 157/2016. (VI. 13.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet módosításáról
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 2016. évi CL. törvény az általános közigazgatási rendtartásról
https://net.jogtar.hu/jogszabaly?docid=A1600150.TV
- 246/2015. (IX. 8.) Korm. rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
https://net.jogtar.hu/jogszabaly?docid=A1500246.KOR
- 330/2015. (XI. 10.) Korm. rendelet a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
https://net.jogtar.hu/jogszabaly?docid=a1500330.kor
- 359/2015. (XII. 2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről
https://net.jogtar.hu/jogszabaly?docid=a1500359.kor
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm
- 249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
https://net.jogtar.hu/jogszabaly?docid=A1700249.KOR
- 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

## 7.2. Európai Uniós jogi aktusok

- Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelv
  https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32008L0114&from=EN
- A fogyasztói jogviták alternatív rendezéséről, valamint a 2006/2004/EK rendelet és a 2009/22/EK irányelv módosításáról szóló, 2013. május 21-i 2013/11/EU európai parlamenti és tanácsi irányelv
  https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0011&from=EN
- 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 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML
- Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU
- 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 rendelet tervezete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról
  https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29
- 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 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
  https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN

- 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
- Közös Közlemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában
  http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
- Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata
  https://undocs.org/A/RES/58/32
- Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról (2011/2284(INI))
  https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&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

## 7.3. Külföldi jogi aktusok

- Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése:
  https://www.osce.org/pc/90169?download=true
- Az EBESZ bizalomépítő intézkedései: PC.DEC/1106
  https://www.osce.org/pc/109168

# 8. FOGALOMTÁR

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas, számos megjelenési formát vehet fel (például: alfabetikus, numerikus, grafikus, képi forma), és amely új ismeret forrása. [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, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – 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 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, mely 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, megváltoztatását, 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, titoktartási kötelezettség alóli felmentés, 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 néven (és az anyagban is használt) 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 fenyegetés-elemzés és információgyűjtés (threat intelligence consumption); az eszközleltár és hálózatbiztonsági monitoring; az incidenskezelés; és a fenyegetés és környezet kezelése (threat and enviroment manipulation). [8]
- **Alapvető szolgáltatást nyújtó szereplő:** Alapvető szolgáltatást nyújtó szereplőnek Magyarországon azon intézmény lehet, amely kijelölt nemzeti létfontosságú rendszerelem üzemeltetője, a NIS irányelv II. mellékletében felsorolt ágazatok és alágazatok valamelyikébe sorolható szolgáltatást nyújt, szolgáltatása elektronikus információs rendszerektől függ valamint a szolgáltatását érintő biztonsági esemény jelentős zavart okozna az általa nyújtott szolgáltatás biztosításában. Alapvető szolgáltatásoknak tekinthetők a társadalom vagy gazdaság szempontjából fontos szerepet betöltő magán- és állami vállalkozások, például vízellátás, villamosáram-szolgáltatás stb. [9]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [10]
- **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). [11]
- **Automatizált informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [12]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amelyet 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 rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [13]

- **Bejelentés- köteles szolgálgatásokat nyújtó szereplő**: Magyarországon bejelentésköteles szolgáltatásoknak nevezzük azon szolgáltatásokat, melyek a NIS Irányelv szerinti digitális szolgáltatók körébe tartoznak. Továbbá azon nem mikro- és kisvállalkozásokat, melyek online piacteret, online keresőprogramot, valamint felhő alapú számítástechnikai szolgáltatást nyújtanak. [9]
- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a minta alapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [14]
- **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. [15]
- **Biometrikus azonosítás**: Olyan eszközök és eljárások összessége, amely 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. [16]
- **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 csak az arra jogosult és csak a jogosultság szintje szerint férhet az adathoz és használhatja fel. [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. [17]

- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket 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. [14]
- **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]
- **Cloud computing**: („számítástechnikai felhő", „felhő alapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon 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 felhő alapú szolgáltatástól szabadulni. [2]
- **Digitális szolgáltatás**: Az (EU) 2015/1535 európai parlamenti és tanácsi irányelv 1. cikke (1) bekezdésének b) pontja szerinti, a III. mellékletben felsorolt típusok valamelyiknek megfelelő szolgáltatás. [18]
- **Digitális szolgáltató**: Minden olyan jogi személy, amely digitális szolgáltatást nyújt. [18]
- **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. [19]
- **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. [19]
- **EC3**: Az Europol Európai Kiberbűnözés Elleni Központja, amelynek fő feladata a szervezett bűnözés ellehetetlenítése, elsősorban a tagállamok nyomozóhatóságainak nyújtott, operatív támogatása által. [18]
- **Egyetlen kapcsolattartó pont (SPOC)**: a kapcsolattartó pont fő feladata az Európai Unión belüli nagy hatású kiber-incidensek hazai koordinálása, valamint az incidensekkel kapcsolatos jelentések fogadása, küldése az EU-s tagállamok SPOC-ai számára. [9]
- **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**: Az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese. [5]
- **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]
- **Elosztott szolgáltatás megtagadásos 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 számítógép-rendszer 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. [18]
- **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. [18]
- **Ethernet**: A DEC, Intel és 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. [18]
- **Eseménykezelő Szakterület (Event Detection Team): I**ntézmények közti megállapodás keretében a biztonság növelése érdekében folyamatosan monitorozza a hálózati forgalom különböző szegmenseit. A szakterület által végzett feladat preventív és detektív jellegű, hiszen 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. [20]
- **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]
- **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 tekinteté-

ben, 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, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, 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. [23]
- **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]
- **Hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia:** Olyan stratégiai dokumentum, amelyben legalább a NIS irányelv szerinti hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapítanak meg a tagállamok. [9]
- **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, melyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [24]
- **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 csapda rendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapda rendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapda rendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy. [20]
- **IKT-folyamat**: Valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása, illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége. [18]
- **IKT-szolgáltatás**: Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll. [18]
- **IKT-termék:** valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja. [18]
- **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, amely 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]
- **Infrastruktúra**: Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek. [18]
- **Internet of Things (Iot)**: A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra, és azok internet-szerű 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. [26]
- **Ipari irányító rendszerek (Industrial Control Systems)**: Ezek nélkül a rendszerek nélkül ma már elképzelhetetlen a közműszolgáltatások, a gyártósorok vagy éppen a közlekedés és szállítmányozás zavartalan működésének biztosítása. Mára a legtöbb ICS rendszer és berendezés ugyanolyan vagy legalábbis nagyon hasonló komponensekből épül fel, mint a más szektorok (pénzügy, államigazgatás, szolgáltatói szektorok) IT rendszerei. [8]
- **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, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [13]
- **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 működéséhezés 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. [18]

- **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, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, 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. [27]
- **Kiberkémkedés***:* Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [28]
- **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. [29]
- **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]
- **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. [20]
- **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.
- **Központi alkalmazás (Application Server)**: Olyan felhő alapú megoldás, amely gyűjti és kezeli a nagymennyiségű adatokat (Big Data) és megfelelő szoftverek segítségével felhasználja azt. [30]
- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [20]
- **Kritikus infrastruktúra**: azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon 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. [14]
- **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**: Létfontosságú rendszerelemnek tekinthetők azok a rendszerek, illetve rendszerelemek, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, (például az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális szolgáltatások biztosításához) és amelynek kiesése jelentős következménnyel járna. [31]
- **Mágneses tér**: A töltések rendezett mozgása, azaz az áram révén az áram járta vezető körül elektromágneses erőtér jön létre. Az egyirányba, egyenletesen mozgó töltések áramlásának (azaz az egyenáramnak) a hatására állandó, míg a váltakozó irányba, változó sebességgel mozgó töltések áramlásának (azaz a váltakozóáramnak) a hatására változó mágneses tér keletkezik. Ugyanakkor a folyamat visszafelé is működik, azaz a mágneses erőtér változása erőt fejt ki a vezetőben lévő töltött részecskékre, mely erő elmozdítja e részecskéket, ezzel áramot hoz létre. [21]
- **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. [13]
- **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. „Szigorúan titkos", „Titkos", „Bizalmas" és „Korlátozott terjesztésű" jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]
- **Mozgási indukció**: A mágneses mező és valamely vezető anyag egymáshoz képesti, a mágneses erővonalakat metsző elmozdulásakor mozgási indukcióról beszélünk. A mozgási indukció a feszültség létrehozásának mozgással történő módja, a villamosenergia előállítás, a generátorok működésének az alapja. [21]
- **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. [14]
- **Nemzeti Kiberbiztonsági Koordinációs Tanács**: Az e-közigazgatásért felelős miniszter (jelenleg a belügyminiszter) által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács a

Kormány javaslattevő, véleményező szerveként gondoskodik az Ibtv. hatálya alá tartozó szervezetek információbiztonsági tevékenységeinek összehangolásáról. [14]

- **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. [14]
- **Nyugalmi indukció**: • El nem mozduló, de változó mágneses mező és el nem mozduló vezető között megvalósuló indukció esetén nyugalmi indukcióról beszélünk. Ebben az esetben az el nem mozduló, de időben változó áram által létrehozott elektromágneses erőtér változó mágneses erővonalai – azaz az időben változó fluxus – révén jön létre az indukció. [21]
- **Okos mérés (Smart metering)**: Az okos mérési rendszerek lehetőséget adnak arra, hogy a szolgáltatók és a hálózat üzemeltetők a végfogyasztókra lebontva képesek egyedi adatszolgáltatása. [30]
- **Okos otthon (Smart Home):** A felhasználó otthoni készülékei (Smart Appliencies) valamilyen hálózati kapcsolat révén kommunikálnak egy központi vezérlő/szabályozó egységgel. Ennek eredményeként a felhasználói készülékek működése valamilyen szintű „intelligenciával" van felruházva. [30]
- **"Online piactér":** Olyan digitális szolgáltatás, amely a 2013/11/EU Európai Parlamenti és Tanácsi irányelv (18) 4. cikke (1) bekezdésének a) és b) pontjában meghatározott fogyasztók és/vagy kereskedők számára lehetővé teszi, hogy az online piactér weboldalán vagy valamely kereskedőnek az online piactér által nyújtott számítástechnikai szolgáltatásokat felhasználó weboldalán keresztül online adásvételi vagy szolgáltatási szerződéseket kössenek. [9]
- **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. [32]
- **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. [17]
- **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. [17]
- **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. [14]
- **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)]. [33]
- **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. [34]
- **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 számítógép-rendszer 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]
- **Stuxnet**: A kártevő még 2010 nyarán bukott le Iránban, Busehr (Bushehr) város erőművének egyik számítógépén. Akkor mintegy százezer számítógépet sikerült megfertőznie. Csak az országban legalább 45 ezer felügyeleti számítógép és szerver hordozta a vírust. Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. [35]
- **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]
- **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. [13]

- **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. [36]
- Üzletmenet-folytonosság **tervezés**: 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]
- **Válságkommunikáció**: Tulajdonképpen nem más, mint a hatóságok, a szervezetek, a média és az érdekelt személyek, illetve csoportok közötti információcsere, amely a válságesemény előtt, alatt és után történik. Az információáramlás három dolog körül összpontosul: a tényleges válság, a válság kezelésének folyamata, a válság (különféle közvéleménycsoportokban és különböző szintű nyilvánosságokban kialakuló) képe. [37]
- **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. [30]
- **Villamos erőtér**: Az elektromosan töltött részecskék és testek erőhatást gyakorolnak egymásra. Az azonos töltésűek taszítják, a különböző töltésűek vonzzák egymást. A nyugalomban lévő töltések közötti erővonalak terét villamos erőtérnek nevezzük. [21]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve az által, 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 videó lejátszó, 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 törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [13]
- **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]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

## 8.1. 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: 2018.03.22.)

*{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: 2018.03.22.)

*{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: 2018. 03. 24.)

*{8}* Pongrácz P. (2019): *Kibertámadások villamosenergetika környezetben*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

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

*{10}* Rédecsi M. – Tóth G.: (2013) *Android*. URL: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018.03.24.)

*{11}* Gyurák G. (2015): *Informatikabiztonság I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs.

*{12}* *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.*

*{13}* Haig Zs. – Kovács L. (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. URL: http://hdl.handle.net/11410/285 (utolsó letöltés: 2018.03.24.)

*{14}* Marsi T. (2018): *A célzott támadások és megelőzésük sérülékenységvizsgálattal.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.

*{15}* *A Big Data a hivatalos statisztikában*. 2016. URL: https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018.03.24.)

*{16}* Mátrai J. (2016): *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás*. URL: http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. 07. 04.)

*{17}* Oroszi E. (2008): *Social Engineering.* Budapesti Corvinus Egyetem, Budapest.

*{18}* Bonnyai T. (2019): *Kritikus információs infrastruktúra védelem*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

*{19}* Kaczur G. (2018): *Spearphishing.* In. Célzott támadások. Dialóg Campus Kiadó, Budapest.

*{20}* Marsi T. (2019): *Incidenskezelés kritikus infrastruktúrák esetén*. In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

*{21}* Görgey P. (2019): *A villamosenergia-szektor mint kritikus infrastruktúra*, In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

*{22}* Danyek M. (2019): *A villamosenergia szektor mint kritikus információs infrastruktúra,* In. Kritikus információs infrastruktúrák védelme, Dialóg Campus Kiadó, Budapest.

*{23}* Emmanuel Carabott (2011): *Hacking Motivations – Hactivism*, URL: http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2018.03. 22.)

**A Nemzeti Közszolgálati Egyetem kiadványa.**

**Kiadó:**
Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

**Felelős Kiadó:**
Prof. Dr. Kis Norbert Rektorhelyettes

**Címe:**
1083 Budapest, Üllői út 82.

**Olvasószerkesztő:**
Dorogi Katalin

**Tördelőszerkesztő:**
Friebert Máté

ISBN 978-963-498-240-1 (PDF)