híradástechnika

1945 VOLUME LXXIV. 2019

hírközlés ▪ informatika

1

HTE Infokom 2018

A Hírközlési és Informatikai Tudományos Egyesület folyóirata

HTE 70 ÉVES

Tartalom / Contents

Hírközlési és Informatikai Tudományos Egyesület • www.hte.hu

Elnök: Magyar Gábor

H-1051 Budapest, Bajcsy-Zsilinszky út 12., 5. em./502. • Tel.: 353-1027 • e-mail: info@hte.hu

Az Egyesületet a Nemzeti Hírközlési és Informatikai Tanács támogatja

Elnök: Vágujhelyi Ferenc

Főszerkesztő

SZABÓ CSABA ATTILA (BME, Hálózati Rendszerek és Szolgáltatások Tanszék)

Felelős kiadó: NAGY PÉTER

HU ISSN 0018-2028

Layout: MATT DTP Bt. • Nyomda: FOM Media

HTE Infokom 2018

21. alkalommal került megrendezésre a Hírközlési és Informatikai Tudományos Egyesület szervezésében az *Infokommunikációs Hálózatok és Alkalmazások Konferencia és Kiállítás;* a HTE Infokom 2018. Az Infokom-rendezvények középpontjában a távközlés, informatika és média aktuális műszaki, piaci és szabályozási kérdései állnak. A konferenciák célja, hogy lehetőséget teremtsen az infokommunikációs piac változásainak megismerésére, a legújabb műszaki megoldások, hálózat-, szolgáltatás- és alkalmazásfejlesztési elképzelések közzétételére, valamint a tapasztalatcserére, az együttműködés elmélyítésére, a személyes és közvetlen kapcsolatok kialakítására.

Számunk cikkeit az Infokom 2018 előadásaiból válogattuk össze. Nem volt könnyű kiválasztani a sok érdekes és jó előadás közül azokat, amelyek szerzői meghívást kaptak a Híradástechnikába. Törekedtünk arra is, hogy minden fontos témakör képviselve legyen. A cikkek sorrendje követi a konferencia szekcióinak sorrendjét.

Kovács Benedek és szerzőtársai (Ericsson Magyarország Zrt.) „Mesterséges intelligencia felhasználási esetek 5G hálózatokban” írása bemutatja, hogy milyen esetekben alkalmazható mesterséges intelligencia és gépi tanulás hálózatfelügyeletre és hálózatautomatizálásra. Bemutat egy pozíciót becslő, képfelismerő rendszert, mint alkalmazást az újgenerációs hálózatra, illetve röviden ismerteti, hogy milyen módon támogatja az 5G-hálózat az úgynevezett edge computingot.

Farkas Károly (NETvisor Zrt., BME) az „Ipar 4.0 megoldások – Gyári infrastruktúra felügyelete” cikkében bemutatja és egy demonstrációs terepasztal segítségével illusztrálja azt az Ipar 4.0 szemléletben kidolgozott, egységes gyáriinfrastruktúra-felügyeleti rendszert, amely az eszközállomány felderítését, nyilvántartását, működésének monitorozását valósítja meg. Ezen felül meghibásodás esetén támogatást nyújt a hiba forrásának meghatározásához, ezzel jelentősen csökkentve a hibalokalizálási, és ennek következtében a termeléskiesési időt.

A digitális PMR-rádiózás közel tíz éve váltja fel a hagyományos, analóg beszéd- és adatrádiózást, számos kényelmi és értéknövelő szolgáltatást kínálva. *Turcsán Zsolt* (NOVOFER Zrt.) „Ipari diszpécseri DMR-rádiózás korszerűsítési tapasztalatai az analóg-digitális átállás kapcsán” című cikkében végigkíséri a különböző méretű és összetettségű magyarországi hálózatok átalakítási tervezési, kivitelezési és üzemeltetési kérdéseit, tapasztalatait, értékeit és hátulütőit.

A mobiltelefon szolgáltatók számára a toronyinfrastruktúra birtoklásának stratégiai jelentősége fokozatosan csökken, ezzel párhuzamosan nő a hálózat-megosztási hajlandóság. Egyre több MNO dönt úgy, hogy megválik torony-portfóliójától és a tornyok üzemeltetésére specializálódott cégek kezébe adják infrastruktúrájukat. Az 5G hálózatépítésekhez közeledve e cégek jelentősége még inkább felértékelődhet. *Dóbé Sándor és Rózsás Titanilla* (Antenna Hungária Zrt.) írása a torony-infrastruktúra stratégiai szerepét mutatja be a távközlési piacon.

A „cybersecurity”, a kiberbiztonság megvalósítása az Ipar 4.0 területén számos kérdést vet fel. *Krasznay Csaba* (Nemzeti Közszolgálati Egyetem) „Kiberbiztonság a negyedik ipari forradalom korában” című cikkében áttekinti azokat az európai és hazai stratégiákat és jogszabályokat, amelyek célja a kiberbiztonság megerősítése, egyben rámutat, milyen szabályozói eszközök állnak rendelkezésre az új ipari forradalom szereplőinek támogatására és kontrollálására.

Sík Zoltán Nándor (NHIT) írása; „A blockchain és annak specifikus biztonsági kérdései” bevezetést nyújt a blockchain, mint decentralizált rendszer világába, elsősorban a Bitcoinon, mint az első blockchain-alapú rendszeren keresztül. Megkülönbözteti a blockchaint, azaz az értékek internetét, mint platformot a kriptopénzektől, valamint tárgyalja a különböző konszenzus-mechanizmusokat és rátér a blockchain biztonsági kérdéseire is.

Horváth Ádám és Virga Krisztina (Digitális Jólét Nonprofit Kft.) „Iskolai hálózat a jelenben és a jövőben” cikke arról számol be, hogy a kormány Digitális Jólét Programján belül elkészült Magyarország Digitális Oktatási Stratégiája (DOS). Ennek egyik kiemelt területe az iskolai Wi-Fi-hálózat fejlesztése, mely az üzleti szférától jelentősen eltérő kihívások elé állítja a központi szolgáltatásmenedzsmentet. A cikk rámutat arra is, hogy a jelenlegi fejlesztéseken túl el kell kezdeni a felkészülést a jövő kihívásaira.

Az Európai Elektronikus Hírközlési Kódex 2018 év végi kihirdetésével elkezdődött a tagállamok rendelkezésére álló 24 hónap visszaszámlálása, amely idő alatt nemzeti jogrendjükbe kell, hogy építsék az ágazatra vonatkozó új keretszabályokat. *Ulelay Emília* (NMHH) „Az Európai Elektronikus Hírközlési Kódex hatása a rádióspektrum-gazdálkodásra” című írása áttekinti a legfontosabb új szabályozási elemeket a rádióspektrum-gazdálkodás területén, megvizsgálva azok lehetséges hatását, különös tekintettel az 5G bevezetésére.

A Kódex fogyasztóvédelmi fejezete, a végfelhasználók jogait körülíró rendelkezések legfontosabb újdonsága az elektronikus hírközlési szolgáltatások definíciójának újragondolása, kiterjesztése az ún. OTT kommunikációs szolgáltatásokra, illetve a maximum harmonizációs megközelítés fogalma. Erről és további, az előfizetői szerződésekre vonatkozó változásokról ad áttekintést *Kovács Anita* (Telenor Magyarország Zrt.) „A végfelhasználók jogai az új európai elektronikus hírközlési kódexben” cikkében.

Szabó Csaba Attila
főszerkesztő

Mesterséges intelligencia felhasználási esetek 5G hálózatokban

KOVÁCS BENEDEK[1], SZILÁGYI LÁSZLÓ[2],
GERA ZOLTÁN, FÁBIÁN GÁBOR, CHARLES JOSE FERRARI[3]

[1]Ericsson Magyarország Zrt., [2]Ericsson, Inc., [3]ELTE Informatikai Kar
benedek.kovacs@ericsson.com

Kulcsszavak: 5G-hálózatok, IoT, edge computing, elosztott felhő, neurális hálózatok, kiterjesztett valóság

Az 5. generációs hálózatok sokféle felhasználási eset számára fognak testre szabott megoldásokat adni, olyan területeken is, mint például az ipari automatizáció, okos mérés, a dolgok internete (IoT) és fejlett médiatechnológiát használó média. A cikk bemutatja, hogy milyen esetekben alkalmazható mesterséges intelligencia és gépi tanulás hálózatfelügyeletre és hálózatautomatizálásra, illetve bemutat egy pozíciót becslő, képfelismerő rendszert, mint alkalmazást 5. generációs hálózatra. Röviden ismerteti, hogy milyen módon támogatja az 5G-hálózat az úgynevezett edge computingot.

1. Bevezetés

A mobil telekommunikációs hálózatok már a kezdetek óta rendelkeztek intelligens megoldásokkal, eleinte leginkább automatizáláshoz köthető szabályokkal, később adaptív logikával. Összességében elmondható, hogy minden hálózati generáció a kor legmodernebb gépiintelligencia-technológiáját használja fel a megbízhatóság, robusztusság, biztonság és átviteli minőség biztosítására, automatizálására. Napjaink egyik legfelkapottabb témája a mesterséges intelligencia és annak különböző alkalmazási területei, melyet a neurális hálózatok fejlődése tett lehetővé.

A cikk célja, hogy bemutassa, hogy milyen helyzetekben releváns mesterséges intelligenciát alkalmazni 5. generációs mobil hálózatok esetén. A klasszikus gépi intelligencia felhasználási esetek mellett, melyek leginkább az intelligens hálózatok és automatizált felügyeleti rendszerekre fókuszálnak, bemutatunk lehetséges alkalmazási szintű megoldásokat, illetve ezek hálózati támogatását.

A második szakaszban leginkább a neurális hálózatok hőskoráról lesz szó, illetve olyan intelligens hálózati esetekről, amelyek a gépi tanulás felhasználásával valósítottak meg hálózati automatizációt. A következő szakasz a Big Data témakörét dolgozza fel és bemutatja, hogy milyen kihívásokat jelent a nagy mennyiségű (volume), sokféle (variety), gyors keletkezésű és rövid válaszidejű feldolgozást igénylő (velocity), sokféle minőségű (veracity) adat, és az, hogy milyen felhasználási esetekben segítenek a gépi tanulásos, neurális hálózatos megoldások. A negyedik rész a számítási kapacitási igényre koncentrál és egy példán keresztül bemutatja, hogy a nagy, felhőalapú adatközpontok, melyek tipikusak az 5. generációs hálózatok esetén, hogyan segítik a neurális hálózatok tanításával foglalkozó mérnökök munkáját. Egy alkalmazási szintű felhasználási esetet mutatunk be, amely képfelismeréssel segíthet intelligens közlekedési rendszerekben és egyéb intelligens megoldásokban. Az utolsó szakasz bemutatja, hogy az 5G mobilhálózat a Distributed Cloud [1] technológiával hogyan támogatja az edge computingot és ezáltal a neurális hálózatokat használó alkalmazásokat.

2. Intelligens hálózatok és a mesterséges intelligencia fejlődése

Mesterséges intelligenciáról és intelligens hálózatokról különböző korokban és kontextusokban beszélhetünk. Az ötödik generációs hálózatokban az a különleges, hogy az elterjedőben lévő, neurális hálózatokon alapuló mesterséges intelligencia megoldásokat használja.

A mobil telekommunikációs hálózatok legelső verziói is tartalmaztak automatizálást, leginkább robusztusság és minőség biztosítására, például automatikus átkapcsolások meghibásodás esetén. Ezek a felhasználási esetek a felhasználó számára nem érzékelhetőek. Egyrészről az automatikus hálózatfelügyelet területét fedik le, automatizált újrakonfigurációval és beavatkozással (lásd [2]), másik részről pedig a hálózat elemeiben mélyen beágyazódva segítenek automatikus útvonal-választással, adaptív túlterhelés-védelemmel. Intelligens hálózatoknak hívjuk továbbá azokat a mobilhálózatokat, melyek a felhasználónak nyújtanak intelligens hálózati szolgáltatásokat (ITU Intelligent Networks) [3]. Itt már megjelenik az 5. generációs hálózatokban bevett gyakorlat, hogy a hálózat bizonyos funkciói konfigurálhatóak harmadik fél számára.

A mesterséges intelligencia és gépi tanulás témaköréből a neurális hálózatok nyújtotta lehetőségeket fogjuk bemutatni, ezeken belül is a gépi tanuláson alapuló hálózatokat. Ezek kutatása és alkalmazása a múlt századig nyúlik vissza. A 21. század elején a neurális hálózatok elérhetővé váltak jórészt népszerű matematikai programcsomagok részeként, melyeket kutatók és mérnökök alkalmaztak, különböző témakörökben, például gyógyászati kutatásokban. Az elterjedést gátolta, hogy a fel-

használók számára elérhető személyi számítógépek nem voltak alkalmasak komplex hálózatok tanítására. Egy kétváltozós differenciálegyenlet-rendszer, a Lotka-Volterra egyenletek paramétereinek becslését egy kevesebb, mint 100 neuronból álló hálózattal lehetett elvégezni, melynek tanítása egy átlagos PC-n napokat vett igénybe [4].

Ezek a kis számú neuront tartalmazó hálózatok nem voltak alkalmasak komplex feladatok megoldására, például képfelismerésre. Az ilyen próbálkozások számára szuperszámítógépeket lehetett igénybe venni, ám ez drága volt és nem volt széles körben elérhető. Ehhez képest az emberi agyban lévő neuronok becsült száma százmilliárd, a legnagyobb publikált neurális hálózat 16 millió körüli neuronból áll, míg egy tipikus mai, képfelismerésre használható hálózat százezer neuront tartalmaz. Látható, hogy a tudomány fejlődésével és a számítási kapacitás növekedésével egyre komplexebb neurális hálózatokat építhetünk, azonban ezek a praktikus használatban még nagyságrendileg elmaradnak a biológiában természetesen előfordulóktól, ami további fejlődésüket vetíti elő.

A mesterséges neurális hálózatoknak több fajtája van, a telekommunikációs hálózatokban leginkább a mintaalapú tanuló hálózatok különböző fajtáinak alkalmazása terjedt el. A jelenleg népszerű, *feature learning* hálózatok, a visszacsatolásos tanuláson alapuló hálózatok fejlesztett példái. A feature learning hálózat esetén a hálózat rejtett rétegei egy-egy értelmezhető funkciót végeznek el, így a mélytanulás *(deep learning)*, azaz a sok rejtett réteg bevezetésével lehetővé válik a komponensenkénti tanulás vagy újratanulás. A tanítás időben is eltérhet, tehát tipikus, hogy egy általános problémára megtanított neurális hálózatot később, további minták segítségével egy adott problémára szabnak.

Összességében elmondható, hogy mára elérhetőek és egyre szélesebb körben elterjedtek olyan neurális hálózatok, melyek alkalmasak komplex problémák megtanulására, megértésére. Ezek jellemzően felhasználási esetek köré csoportosulnak és a feature learning, azaz előre tanított hálózatok esetén adott, konkrét problémák, például képfelismerés, hálózati hibaanalízis, biztonsági problémák felismerése, komplexitását képesek hatékonyan kezelni.

Az első körben bevezetett, modern neurális hálózatot alkalmazó felhasználási esetek többek között a lemorzsolódás előrejelzése és a hamis vagy nem biztonságos hálózati elemek kiszűrése voltak. A hálózati biztonság eléréséhez olyan neurális hálózatokat alkalmazunk, melyek kiszűrik a különleges, vagy nem normális működési mintákat, automatikus beavatkozás vagy egy szakértő számára. A modern hálózatfelügyeleti rendszerekben alkalmazott neurális hálózatok figyelik, hogy milyen események vezethetnek hálózati forgalom vesztéséhez, kieséshez és így megtanulják, hogy milyen esetekben kell figyelmeztetést küldeni a felügyeletnek.

Ez a felhasználási eset azért érdekes, mert a jó és rossz esetek szétválasztása egyszerű szabályokkal leírható, így a tanulóhalmaz folyamatosan bővül. A *zero touch* automatizáláson alapuló ötödik generációs hálózatok intelligenciáját is hasonló, fejlett neurális hálózatok segítségével tervezik majd elkészíteni [5].

3. Az adat, a Big Data és a hálózati analitika

A jelenleg elérhető tanuló rendszerek számára az egyik legnagyobb probléma az elegendő tanításra használható adat hiánya. Egy tipikus képfelismerési alkalmazás esetén, az előre tanított *feature learning* hálózatoknál is nagy mennyiségű, az adott felhasználási esetre specifikus tanítási adatra van szükség.

A modern telekommunikációs hálózatok felügyeletét és a felhasználói élmény biztosítását jelenleg a Big Data technológián alapuló támogató rendszerek végzik. A Big Data megelőzte a neurális hálózatok technológiáját és már a 4. generációs hálózatokra is jellemző, hogy az intelligens felügyeleti rendszereik a hálózat működése során mért teljesítményjellemzőket más adatbázisokkal összevetve képesek új értéket teremtő analitikai megoldásokra, például az Expert Analitika [6]. E rendszerek által felhasznált adatok például a felhasználókra jellemző anonim statisztikák, a terminálok típusai és gyártókra jellemző statisztikák, a hálózati elemek által generált teljesítményjelentések, naplók, a forgalmi statisztikák, az átvitel, hangminőség és a hálózati jelzésforgalom adatai.

Egy Voice over LTE (VoLTE) hívás esetén, az akalmazásszintű, IP Multimedia Subsystem (IMS), Session Initiation Protocol (SIP) és Diameter protokol jelzésforgalma hívásonként 200-300 üzenet (átlagos rendszer, átlagos felhasználás). Az üzeneteket térben és időben aszinkron módon figyelhetjük meg, mely nagy mértékben nehezíti a köztük rendszerszinten megfigyelendő korrelációt (a network timeoutok beállításától függően, egy azonnal kiszolgálandó üzenet akár több másodpercet is késhet). A megfigyelt üzenetekből levolt következtetéseket nehezíti, hogy szabványos rendszerek és alrendszereik nem tartalmaznak operáció szintű azonosítót (hiszen nem biztos, hogy egy adott operációhoz minden esetben minden alrendszer bevonása szükséges, egy-egy adatbázis lekérdezése például mehet aszinkron módon, cache használatával). Az egyes üzenetek korrelációja tehát korántsem egyértelmű probléma, és a gépi intelligencia alkalmazása így elkerülhetetlen.

Gépi tanulásos felhasználási eset a jelzésforgalom elemzése, mely előnye azonban, hogy a tanító halmaz előállításához nem szükséges egyenként címkézni az elemeket, elég a hibakódokra vonatkozóan szabályokat létrehozni, ami sokszor igaz a felügyeleti alkalmazásokra. Ezzel a technikával a tanító halmaz minden esetben jó minőségű és folyamatosan bővül. Kifejezetten IMS-jelzésforgalom gépi tanulásos elemzésével pár üzenet után megállapítható, hogy egy adott híváskezdeményezés milyen valószínűséggel lesz sikeres. Egy túlterhelt hálózat esetén, amikor dönteni kell, hogy mely híváskezdeményezést (vagy csomagot) dobjuk el, kritikus, hogy a kiszolgált kérések sikeresek legyenek, hiszen a siker-

telen kiszolgálásnak értéke nincs. A végül sikertelen kiszolgálásra felhasznált hálózati kapacitást szaknyelven *blind load*-nak hívjuk.

A fent bemutatott felhasználási esetekhez kritikus a megfelelő hálózati kapacitás. A hálózatok virtualizálásának részeként a felügyeleti rendszereket is virtualizálják és a futtatási környezetük rugalmasan alakítható az aktuális igényekhez. A felhőalapú számítási és futtatási környezet több szempontból is kulcsfontosságú a neurális hálózatok tanításán alapuló megoldások számára. Egyfelől lényeges, hogy az adatot egy központi adattárházban tároljuk és érjük el, másfelől pedig fontos, hogy a tanítási folyamat elvégezhető olyan időszakokban, amikor olcsón áll rendelkezésre számítási kapacitás.

4. Az *Internet of Eyes* alkalmazás

A telekommunikációs alkalmazások és felügyeleti rendszerek tipikusan privát felhőben futnak, a nyilvános felhasználók számára viszont elérhetők az ún. *web-scale* cégek által nyújtott felhőszolgáltatások, például az Amazon Web Services, Microsoft Azure stb. A fejezet egy példaalkalmazást mutat be, demonstrálván, hogy milyen felhasználási eseteket tesz lehetővé az ötödik generációs mobilhálózat és hogyan lehet ezeket népszerű mesterségesintelligencia-eszközökkel megvalósítani. A példaalkalmazás egy demó keretében elkészült, munkacíme Internet of Eyes, és több tipikus kihívást is demonstrál, amelyek megoldása kulcsfontosságú az intelligens 5G hálózatokhoz: valós idejűség, elosztottság.

Az 5G-hálózatokkal kapcsolatban sok dolgot lehet biztosra venni már bevezetésük előtt is: nagy sávszélesség, kis késleltetés és sok eszköz együttes használata válik lehetővé segítségükkel. Ennél sokkal izgalmasabb kérdés azonban, hogy ha ezek a fejlesztések infrastrukturálisan is testet öltenek, milyen új szolgáltatásokra adnak majd lehetőséget és tulajdonképpen hogyan fogja az 5G egy átlagember életét befolyásolni. Az előző gondolat alapján érdemes főleg olyan szolgáltatásokat vizsgálni, melyek kis késleltetést, nagy sávszélességet és számításigényt követelnek meg. Az *Internet of Eyes* elérhető, nagy sávszélességet igénylő eszközöket vesz célba: az IP-kamerákat. Több kamera képének egyidejű feldolgozásával, kis késéssel képes eseményeket, mozgást, objektumokat érzékelni, térben behatárolni, felismerni, majd az érzékelt információ gyors továbbításával beavatkozni. Példa lehet erre egy gépjármű megállítása, ha a kereszteződés felé olyan ütközőpályán érkezik egy másik közlekedő – mondjuk kerékpáros – mely a vezető szemszögéből nem látható, de a rendszer a kameráknak köszönhetően mind a kerékpárt, mind a gépjárművet és ezek mozgását érzékeli.

A rendszer fő összetevői

a) Adatforrás/Kamerák:

Nagy felbontású, folytonos videojelet továbbítanak. Rendszerint az ilyen kamerákon nincs meg a megfelelő teljesítmény komoly feldolgozás elvégzésére.

b) Párhuzamos és független feldolgozás:

Bizonyos műveleteket minden kamera képén lefuttatunk. Ide nemcsak zajszűrés és előfeldolgozás tartozik, de mozgásdetektálás, objektumkövetés és mélytanulással segített objektum-felismerés is.

c) Összegző feldolgozás/Pozíció-meghatározás:

A különböző kamerák jelfolyamából kinyert adatokat azonos koordinátarendszerbe illesztjük és meghatározzuk a résztvevő események/objektumok térbeli helyzetét, irányát.

d) Modellalapú reakció, ill. Beavatkozás:

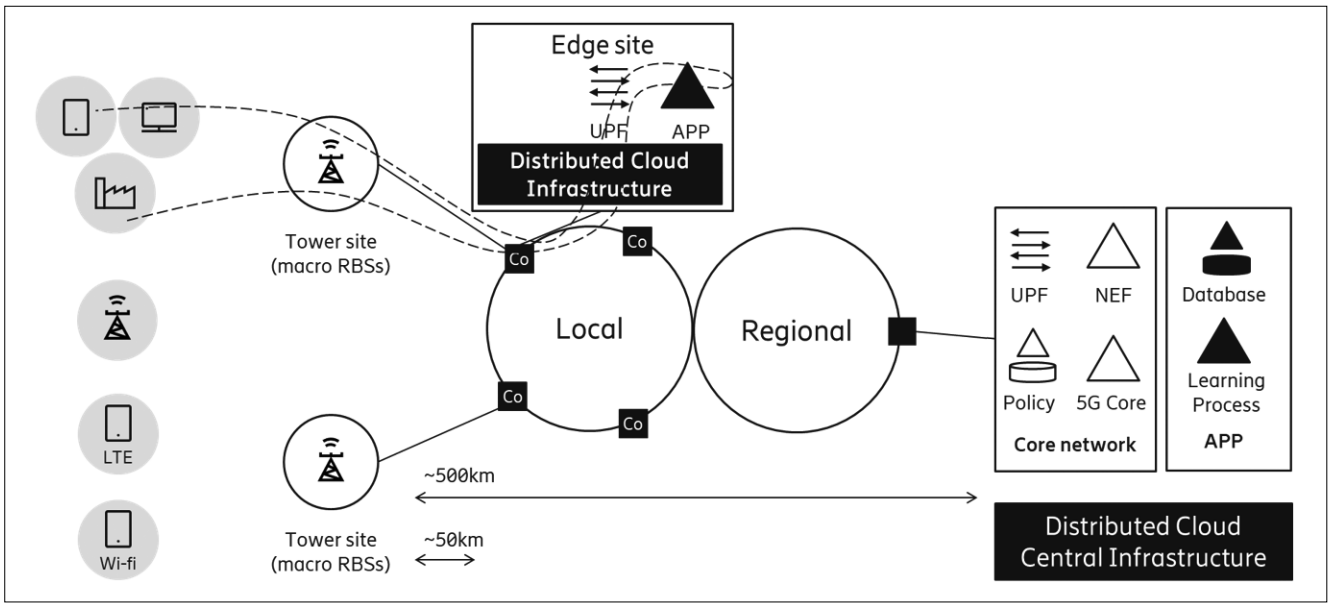
Itt történik meg a döntés, ami alapján beavatkozunk, vagy csinálunk valamit. Ez lehet aktív beavatkozás: egy autó leállítása az ütközés elkerülése érdekében, drón mozgásának megváltoztatása a lezuhanás elkerülése végett. Lehet azonban más rendszerek segítése is: egy kiterjesztett valóság kliens berajzolhatja az épületektől nem látszó tárgyakat a képre, így átláthatunk tárgyakon és valós időben láthatjuk, mi történik mögöttük.

e) 5G hálózat:

Lehetővé teszi, hogy a nagy sávszélességet igénylő kommunikáció ellenére a teljes visszacsatolási kör szinte valós időben történhessen meg. Továbbítja a jelet az adatforrásoktól a feldolgozó központok felé, ezek között, majd innen a cselekvés helyére, a beavatkozást végző eszközre. A teljes folyamat csak akkor ér valamit, ha a beavatkozás késedelem nélkül tud megtörténni. A videójel továbbítását RTP-protokollal és GStreamer [7] könyvtárral végezzük.

Videójel feldolgozására, zajcsökkentésre, objektumok követésére és mozgásérzékelésre OpenCV [8] programkönyvtárat használunk. A kis késleltetés és jó teljesítmény elérése érdekében a teljes rendszer C++-ban íródott. Ez alól a mélytanulással működő, objektum-felismerést végző TensorFlow [9] a kivétel. Ennek a komponensnek – és alapvetően minden jelenlegi mesterséges intelligencia megoldásnak – megvan az a hátulütője, hogy bár a legkomolyabb és legdrágább hardvert igényli, továbbra is a legnagyobb válaszidővel rendelkező egység a rendszerben. Ez annyira súlyos probléma a jelenlegi technikai színvonalon, hogy ha kizárólag ilyen algoritmusokra támaszkodnánk, akkor nem lenne elérhető valósidejű válaszidő a rendszer egészében a piacon kapható rendkívül drága, csúcskategóriás GPU-k használatával sem.

A közös koordinátarendszerbe helyezett rekombinációt egy saját fejlesztésű algoritmus végzi. A rendszer flexibilitását az adja, hogy valójában nem kell egy tárgyat sok kamerának látnia ahhoz, hogy tudjuk, hol van. Külön tudjuk kezelni a statikus kamerákat, melyek nem változtatják a helyzetüket. Ezek a rendszer indítása előtt kalibrálhatóak. A kalibráció lehetővé teszi, hogy a kamera saját helyzete alapján egyetlen képből is viszonylag jól lehessen becsülni, hogy a mozgás a tér mely részén, milyen térirányokban történik. Ilyen esetben egy másik kamera képe már csak pontosítja az adatokat. Dinamikus, azaz változó pozíciójú kamerák esetén pedig a többi kamera képe alapján ennek a kamerának a saját pozícióját is meg tudjuk határozni a látottak alapján.



1. ábra

Distributed Cloud, az applikáció által forgalmazott kritikus válaszidejű adatkomponens a hálózat szélén kerül feldolgozásra, az Edge Site-on: szaggatott adatút. Az Edge Site management és orkesztráció szempontból integrált része a felhő infrastruktúrának, tehát tulajdonképpen egy elosztott felhőről, Distributed Cloud, beszélünk. A konfiguráció az ábrán központban elhelyezkedő Network Exposure Function-on (NEF) keresztül végezhető el.

Ez történik egy kiterjesztett valóság kliensben (mondjuk mobiltelefon kliensen), amikor az ránéz a területre, majd ott kirajzolódnak a nem látszó objektumok is. Akárhogy mozgatjuk a mobilunkat, a berajzolt tárgyak együtt mozognak a látottakkal. A kiterjesztett valóság kliensünk C#-ban íródott, Unity3D [10] és Vuforia [11] keretrendszereket használ.

Fontos részlet a rendszer működésében a hálózati kialakítás is. Jellemzően mind az érzékelést végző kamera, mind a beavatkozást végző egység, illetve mobil kiterjesztett valóság kliens kis teljesítményű eszközök, melyeken a számítások nem lennének elvégezhetőek. Ugyanakkor az adatok nagy távolságra, a felhőbe való küldése túlságosan nagy késést okozna. Ezért van szükség a végeszközökhöz hálózati topológiában közel lévő, de nagy számítási teljesítménnyel rendelkező központokra ahhoz, hogy a kis késés ilyen jelentős terhelésnél is biztosított legyen. Az 5. generációs hálózatokban ezt a problémát a következő fejezetben bemutatott *edge computing* oldja meg, ahol a számítást végző egység nem a felhőből, hanem a szolgáltató topológiailag közel lévő egységéből választódik ki. Ezek a hálózat peremén rendelkezésre álló egységek azonban alkalmatlanak arra, hogy a komplex neurális hálózatok tanítását elvégezzék az adat és a kapacitás hiányában, így a tipikus munkafolyamat az, hogy a tanítást a központi felhőben, magát a valós idejű képfelismerést (inferenciát) pedig a hálózat peremén végezzük el.

5. Edge computing és az elosztott felhő

A 4. generációs hálózati architektúra jellemzője, hogy a klasszikus, HW alapú, vagy akár virtualizált hálózati eszközök egy központi adatfelhőben érhetők el. Egy tipikus közép-európai operátor országosan egy-két nagy adatközponttal rendelkezik. Az Amazon Web Services néhány nagy adatközpontot üzemeltet a világon, ezek közül többet Nyugat-Európában és egyet sem Kelet-Európában. Amennyiben a fent említett, alacsony késleltetésű alkalmazást szeretnénk elérhetővé tenni a mobilhálózatokban, úgy számolnunk kell azok késleltetésével.

A 1310 nm hullámhosszúságú fény egy tipikus Brand B (G.652) optikai kábelben történő terjedésének 489,34 μs/100 km sebességével számolva [12], a nyugat-európai adatközpont Magyarországról körülbelül 10 ms alatt érhető el, nem számítva a csatolók és útvonalválasztók által közbeiktatott, akár egyenként 1 ms késleltetést. Az országos adatközpontok tipikus átlagos elérése egy 4. generációs telekommunikációs hálózatban 10-50 ms. (Ezt az adatot lényegesen befolyásolja a rádiós és átviteli hálózat minősége és a felhasználás célja, például helyben telepített, privát hálózatok esetén nincs ez a típusú késleltetés.) Egyértelmű, hogy az egyes felhasználási esetek által megkövetelt 10-30 ms maximális késleltetés szükségessé teszi, hogy a csomagot feldolgozó alkalmazás a felhasználóhoz közel fusson. Ezt *edge computing*-nak nevezzük, mely technológiát lehetővé teszik az elosztott adatközpontok, melyek virtuális futtató környezetet kínálnak a hálózat peremén.

A *1. ábra* bemutatja, hogyan illeszkedik egy tipikus edge computing alkalmazás egy elosztott felhő architektúrát támogató 5. generációs hálózatba. Az ábra bal oldalán található a terminál a rajta futó alkalmazás komponensekkel. Az 5G mobil hálózatokban bevezetett Next Generation Radio hálózati hozzáférés, konfigurációtól függően az 1 ms nagyságrendű késleltetést is lehetővé teszi. A hálózat peremén futó elosztott felhő virtuális környezetének fizikai komponensei az ábrán *Central office*-ban (Co) helyezkednek el, ami tipikusan egy városi tele-

fonközpont modernizációjával alakítható ki, közel van a helyi antennákhoz. Egy ilyen adatközpont tipikus mérete 5-25 pizzabox-szerver kapacitás. Könnyített hálózatfelügyelettel rendelkező infrastruktúrát adhat virtuális gép, konténer vagy funkció mint szolgáltatás típusú felhőalapú futtató környezetben hálózati eszközök és harmadik fél által fejlesztett alkalmazások vagy platformok számára. Azzal, hogy a virtuális infrastruktúra elérhető a hálózat szélén, nemcsak a hálózati késleltetést csökkentjük le a felhasználó készüléke és az alkalmazás között, hanem jelentősen csökkenthetjük az adatforgalmat, lehetőséget adhatunk tartalomszolgáltatások hálózatok lokális csatolására.

Annak érdekében, hogy a felhasználók adatforgalma a megfelelő peremfelhőben futó applikációhoz kerüljön, a 3GPP hálózatok *local breakout* funkcióját az 5. generációs hálózati szabvány továbbfejleszti és az új funkcióval applikációk szerint lehet a forgalmat terelni és feldolgozni. Ez azt jelenti, hogy bizonyos applikációk forgalmát helyi feldolgozásra, másokét központi feldolgozásra csatolhatunk ki, de azt is, hogy egyes applikációk esetén más műveleteket végzünk a csomagokkal, amit a 3GPP szabvány *flexible mobile service steering*-ként definiál. Egy uplink videó esetén elképzelhető a *deep packet inspection* (DPI) szolgáltatás mellőzése, a kompresszió, vagy adott esetben konfigurálható, hogy titkosított vagy nem titkosított legyen a forgalom. A felhasználói adatot kezelő *User Plane Function* egyes elemei, melyek a 3GPP által definiált *flexible mobile service steering* komponensei, egy ilyen hálózatban akár szétosztott módon is futtathatók, tehát a hálózat különböző peremi vagy központi felhőjében lehetőséget adva intelligens teljesítmény optimalizálásra.

A 3GPP által szabványosított 5. generációs maghálózat *(5G Core)*, architektúrájában jelentősen eltér a 4. generációstól *(Evolve Packet Core)*. A tervezési szempontok közé tartozott a hálózati elemek, – ETSI terminológiában *Virtual Network Functions,* azaz virtuális hálózati funkciók – szolgáltatás központú architektúra *(service oriented architecture)* szerinti újratervezése, amit a szabány *service based architecture*-ként ismer. A cél a programozhatóság és a rugalmasság támogatása volt. Az edge computing és elosztott felhő rendszerek szempontjából a *Network Exposure Fuction* kap kiemelt szerepet, mely lehetővé teszi megbízható harmadik fél által fejlesztett alkalmazások számára, hogy a hálózat bizonyos funkcióit konfigurálják. Ezen funkciók közé tartozik például az említett *application influence on traffic routing* programozható interfész, mely lehetőséget ad harmadik fél által készített alkalmazások számára a *local breakout* és *flexible mobile service steering* konfigurálására. Implementációs szempontból ez egy HTTP-alapú API, amelynek szolgáltatását a hálózat implementálja.

Az edge computing architektúrájú alkalmazások egyik központi kérdése, hogy mely modulok melyik fizikai helyszínen fussanak. Ennek eldöntésére egyszerű alkalmazások esetén kézi konfigurációt alkalmazhatunk, míg bonyolult alkalmazásokat intelligens optimalizáló rendszerek támogatnak majd [13].

6. Összefoglalás

Cikkünkben bemutattuk, hogy az 5G-hálózatokban milyen felhasználási esetek vannak a mesterséges intelligencia technológiák hálózaton belüli és applikációs rétegbeli alkalmazására.

Míg az első esetben, a hálózati automatizáció és az intelligens felügyeleti rendszerek természetes evolúciója következtében kezdődött meg a tanuló neurális hálózatok és egyéb mesterséges intelligencia megoldások használata, a másik, applikációs esetben a hálózat nyújtotta új lehetőségeket – *edge computing,* elosztott felhő, *local breakout, application influence on traffic routing* – fogják majd tudni kihasználni az 5G mobilhálózatra fejlesztett alkalmazások, aminek működését egy példával is demonstráltuk.

A szerzőkről

KOVÁCS BENEDEK vezető mérnök az Ericsson-nál. MSc-fokozatát mérnök informatikusként, PhD-fokozatát a Matematika és Számítástudományok Doktori Iskolában szerezte a Budapesti Műszaki és Gazdaságtudományi Egyetemen. Az Ericsson-ba 2005-ben szoftvertesztterként lépett be, majd rendszermérnökként részt vett több termék, többek között a Voice Over LTE szolgáltatás kidolgozásában. Specializációja a magas rendelkezésre állású rendszerek robosztussága és teljesítménye. Jelenleg aktívan dolgozik az 5G fejlesztésén, az ipari alkalmazások és az edge computing területen.

SZILÁGYI LÁSZLÓ a Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai karán végzett, diplomamunkáját az ARM cambridge-i központjában végezte. Az Ericsson Magyarországnál szoftverfejlesztőként kezdett, rendszermérnöki és product owner-i szerepei után az elmúlt években innovációs projektek menedzselésével foglalkozott, IoT és edge technológiákra fókuszálva, az Ericsson Garage és az Ericsson technológiai szervezetének keretein belül. Jelenleg az Ericsson kaliforniai Santa Clara-i irodájában dolgozik, az új üzleti területek értékesítési részlegén az edge-technológiákért felel.

GERA ZOLTÁN az ELTE Informatikai Karán tanársegéd, valamint kutatás-fejlesztési projektek vezetője. Két jelentős magyar startup (NNG, Prezi) első négy évének részese volt fejlesztőként, csapatvezetőként. A kutatás és innováció motiválja, USA-ban bejegyzett szabvánnyal is rendelkezik. Szívügye az informatikai szakma jobbá tétele, ezért igyekszik alma mater-én minél többet visszaadni a közösségnek.

FÁBIÁN GÁBOR az ELTE IK-n tanársegéd, az intézmény Doktori Iskolájának doktorjelöltje. Több projekt megvalósításában végzett kutató-fejlesztő munkát, melyek az informatika olyan területeit érintették, mint a hangfeldolgozás, képfeldolgozás, vagy a 3D rekonstrukció. Kutatásában a számítógépes grafika matematikai módszereivel foglalkozik, de szívesen fordítja figyelmét más területek felé is. Gyakorta tart tudománynépszerűsítő előadásokat, ugyanúgy fontosnak tartja a tudományos módszerek és eredmények magas szintű oktatását, mint azok vonzóbbá tételét.

CHARLES JOSE FERRARI három éve PhD-hallgató az ELTE IK-n, melynek keretein belül az 5G hálózatok szoftverfejlesztési applikációit kutatja, kifejezetten az edge computing applikációk és környezet területén. Tíz éves szoftverfejlesztői tapasztalattal rendelkezik, többek között saját startup cége keretein belül végzett szakmai munkát. Számítógépes Tudományok MSc-oklevelét Innováció és Vállalkozás kiegészítéssel az Európai Innovációs és Technológiai Intézet duális képzésében az ELTE-n szerezte.

Hivatkozások

[1] C. Boberg, M. Svensson, B. Kovács, "Distributed cloud – a key enabler of automotive and industry 4.0 use cases", November 2018, *https://www.ericsson.com/en/ericsson-technology-review/archive/2018/distributed-cloud*

[2] M. Svensson, M. Agarwal, S. Terrill, J. Wallin, "Open, Intelligent and Model-driven: Evolving OSS", 7 Februar 2019, *https://www.ericsson.com/en/ericsson-technology-review/archive/2018/open-intelligent-and-model-driven-evolving-oss*

[3] ITU Intelligent Networks, *https://www.itu.int/rec/T-REC-Q.1200/en/*

[4] B. Kovacs, J. Toth, "Estimating Reaction Rate Constants with Neural Networks", 2007.

[5] E. Fersman, J. Forgeat, R. Cöster, S. K. Mohalik, V. Berggren, "Artificial Intelligence and Machine Learning in Next-generation Systems", Ericsson White Paper, June 2018, *https://www.ericsson.com/en/white-papers/machine-intelligence*

[6] Expert Analytics, *https://www.ericsson.com/en/portfolio/digital-services/automated-network-operations/analytics-and-assurance/expert-analytics*

[7] GStreamer média-streaming könvtár, *https://gstreamer.freedesktop.org/*

[8] OpenCV számítógépes látás könyvtár, *https://opencv.org/*

[9] TensorFlow gépi tanulás keretrendszer, *https://www.tensorflow.org/*

[10] Unity3D játékmotor, *https://unity3d.com/*

[11] Vuforia kiterjesztett valóság keretrendszer, *https://www.vuforia.com/*

[12] K. Miller, Calculating Optical Fiber Latency, 9 Januar 2012, M2 Optics Inc., *http://www.m2optics.com/blog/bid/70587/Calculating-Optical-Fiber-Latency*

[13] A. Reale, Kiss P., C. Ferrari, Kovacs B., Szilagyi L., Toth M., "Application Functions Placement Optimization in a Mobile Distributed Cloud Environment", In: Studia Informatica, no.2, pp.37–52, 2018, *http://www.studia.ubbcluj.ro/arhiva/cuprins_en.php?id_editie=1155&serie=INFORMATICA&nr=2&an=2018*

Ipar 4.0 megoldások – Gyári infrastruktúra felügyelete

FARKAS KÁROLY
NETvisor Zrt. / BME VIK Hálózati Rendszerek és Szolgáltatások Tanszék
karoly.farkas@netvisor.hu

Kulcsszavak: Ipar 4.0, IoT, gyár, gyártás, infrastruktúra-felügyelet

A gyári alrendszerek – mint a gyártás/gyártásfelügyelet, gyári infokommunikációs rendszer, és a gyári alapinfrastruktúra – meglehetősen komplex termelési ökoszisztémát alkotnak. Hagyományosan ezen alrendszerek működésének a monitorozását egymástól szeparált felügyeleti rendszerek végzik. Ebben a komplex ökoszisztémában könnyedén előfordulhat, hogy egy alapvető komponens meghibásodása blokkolja az egész gyártási folyamatot, és ezáltal a gyár normál működését. Egy ilyen helyzetben általában több tucat riasztást generálnak a független felügyeleti rendszerek, az üzemeltetésért és karbantartásért felelős személyek pedig jelentős időt és erőfeszítést kénytelenek fordítani a probléma valódi forrásának a feltárására.
A cikkben bemutatjuk és egy demonstrációs terepasztal segítségével illusztráljuk az Ipar 4.0 szemléletben kidolgozott, egységes gyári infrastruktúra felügyeleti rendszerünket, amely az infrastruktúra felderítését, nyilvántartását, működésének monitorozását valósítja meg, és ezen felül meghibásodás esetén támogatást nyújt a hiba forrásának meghatározásához, ezzel drasztikusan csökkentve a hibalokalizálási és ennek következtében a termeléskiesési időt.

1. Bevezetés

A jelenleg zajló, Ipar 4.0 néven emlegetett negyedik ipari forradalom célja, hogy rugalmasabbá, hatékonyabbá és ügyfélközpontúvá tegye a fejlesztési és gyártási folyamatokat. Ezen cél elérésének legfőbb eszköze a digitalizáció, a digitális rendszerek képességeinek felhasználása. Többségében mindez magas szinten integrált rendszereket vízionál és eredményez, amelynek része a gyári infrastruktúra egységes felügyelete is. Ezen rendszerek vezérlik a folyamatokat, támogatják a működést és biztosítják a magas hatékonyságot.

Azonban jelenleg még ez az átalakulás kezdeti stádiumban van és csak lassan halad előre, köszönhetően az átalakulás komplexitásának is. Például az infrastruktúra-felügyelet vonatkozásában a termelő vállalatok infrastruktúrája meglehetősen összetett, de szeparáltan felügyelt. A gyári alrendszerek, mint például a

– gyártás, beleértve a gyártósorokat/gépeket, PLC[1]-ket, az RFID[2]- és vonalkód-olvasókat, a HMI[3]-paneleket, PC-ket és a gyártásfelügyeletet (SCADA[4], MES[5], ERP[6]);
– gyári infokommunikációs rendszer;
– és a gyári alapinfrastruktúra (létesítmény, beleértve az áramellátást, a vizet, a fűtést)

komplex termelési ökoszisztémát alkotnak. Azonban hagyományosan ezen alrendszerek működésének a monitorozását szigetszerű, egymástól független felügyeleti rendszerek végzik.

1 *Programmable Logic Controller – Programozható logikai vezérlő*
2 *Radio Frequency Identification – Rádiófrekvenciás azonosítás*
3 *Human Machine Interface – Ember-gép interfész*
4 *Supervisory Control And Data Acquisition – Ipari folyamatirányító rszr.*
5 *Manufacturing Execution System – Gyártásfelügyeleti rendszer*
6 *Enterprise Resource Planning – Vállalatirányítási információs rszr.*

Alapvetően minden gyár számára a termelés minőségének és folytonosságának a biztosítása az elsődleges cél, amely a hulladék/termék aránnyal és a termeléskiesés mértékével mérhető. Viszont könnyedén előfordulhat, hogy ebben a komplex ökoszisztémában egy alapkomponens meghibásodása blokkolja az egész gyártási folyamatot, és ezáltal a gyár normál működését. Például amennyiben a gyár központi infokommunikációs eszközének – rendszerint ez egy hálózati kapcsoló vagy útvonalválasztó – áramellátása megszakad, akkor nemcsak az informatikai eszközök nem fognak tudni egymással kommunikálni, hanem a gyártóberendezéseket vezérlő PLC-k sem fognak tudni kommunikálni a felettes SCADA/MES rendszerrel, így előbb-utóbb a termelés is megakad. A problémát hagyományosan mind az infokommunikációs alrendszer működését, mind a gyártási alrendszer működését és ideális esetben a gyári alapinfrastruktúra (áramellátás) működését monitorozó felügyeleti rendszer is jelezni fogja riasztások formájában, egymástól függetlenül és elszigetelt módon. Így az üzemeltetést és karbantartást végző csapat jelentős időt és erőfeszítést kénytelen fordítani a probléma valódi okának a feltárására.

Azonban ha ezt a monitorozási és felügyeleti feladatot Ipar 4.0 szemlélettel, egységes módon kezeljük, akkor a központi hibafelügyeleti funkciót megvalósító komponens – ahogy az *1. ábrán* látható –, gyökérhiba-analízis segítségével könnyen rá tud mutatni a probléma forrására, ezáltal drasztikusan csökkenthet a hiba lokalizálásához szükséges idő, és ennek következtében a termeléskiesési idő. Ezért célszerű a gyári infrastruktúra működésének felügyeletét egy olyan rendszerben integrálni, amely a gyár minden alrendszerét egységesen kezeli. Mi kidolgoztunk egy ilyen integrált infrastruktúra-fel-

ügyeleti rendszert, amely az infrastruktúra felderítését, nyilvántartását, működésének monitorozását valósítja meg és ezen felül meghibásodás esetén támogatást nyújt a hiba forrásának meghatározásához.

A továbbiakban áttekintjük a gyári infrastruktúra-felügyelet alkotóelemeit/funkcióit, majd ismertetjük az általunk kidolgozott egységes infrastruktúra-felügyeleti rendszer komponenseit. Ezt követően bemutatjuk azt a demonstrációs terepasztalt, amelyet az infrastruktúra-felügyeleti rendszerünk működésének szemléltetése céljából dolgoztunk ki és valósítottunk meg, és amely terepasztal egyik példánya 2019 végéig állandó kiállítás keretében megtekinthető és kipróbálható a BME Ipar 4.0 Technológiai Központban [1], a másik példánya pedig a NETvisor Zrt. [2] IoT-tesztlaborjában kapott helyet. Végül egy rövid összegzést követően ismertetünk néhány referenciát, ahol telepítésre került a felügyeleti rendszerünk, vagy annak bizonyos komponensei.

2. A gyári infrastruktúra-felügyelet alkotóelemei

A gyári infrastruktúra elemei a *2. ábra* bal oldalán, az Ipar 4.0 szemléletű infrastruktúra-felügyeletet megvalósító funkciók az ábra közepén láthatók. A felügyeleti rendszer alapvető célja a hiba forrásának meghatározása meghibásodás esetén, melynek megvalósítását az alábbi funkciók támogatják:

1. Felderítés – a gyári infrastruktúra feltérképezése:

A gyári infrastruktúra-elemek konfigurációs és topológiai adatainak összegyűjtését egy automatikus felderítés biztosítja. A felderítő rendszer az eszközök közvetlen elérése mellett a hagyományos IT-, hálózat-, alapinfrastruktúra-felügyeleti rendszerekből és a gyártásirányítási rendszerekből is átveszi az infrastruktúra-adatokat.

2. Nyilvántartás – infrastruktúra-modell felépítése és nyilvántartása:

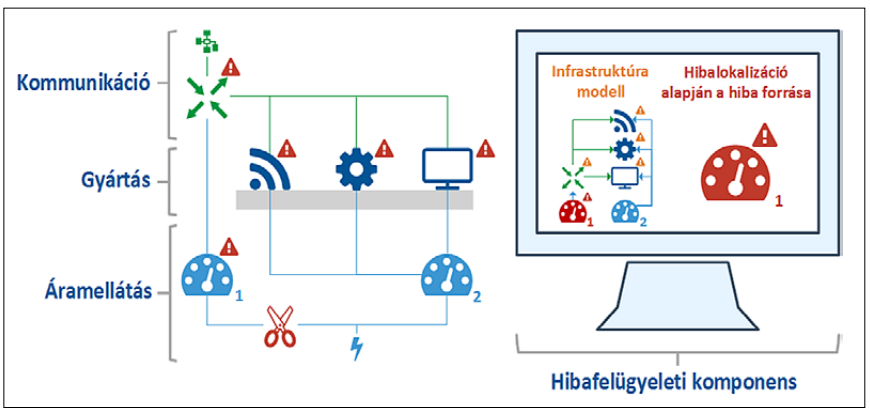
A felderítést követően a felderített adatok alapján felépül egy infrastruktúra-modell, ami a gyártáshoz szükséges összes infrastruktúra-elemet és azok függőségeit tartalmazza. A felderített adatok kiegészítésre kerülhetnek nem felderíthető, hagyományos nyilvántartásokból átvett, vagy manuálisan megadott adatokkal.

3. Monitorozás – teljesítményfelügyelet kialakítása:

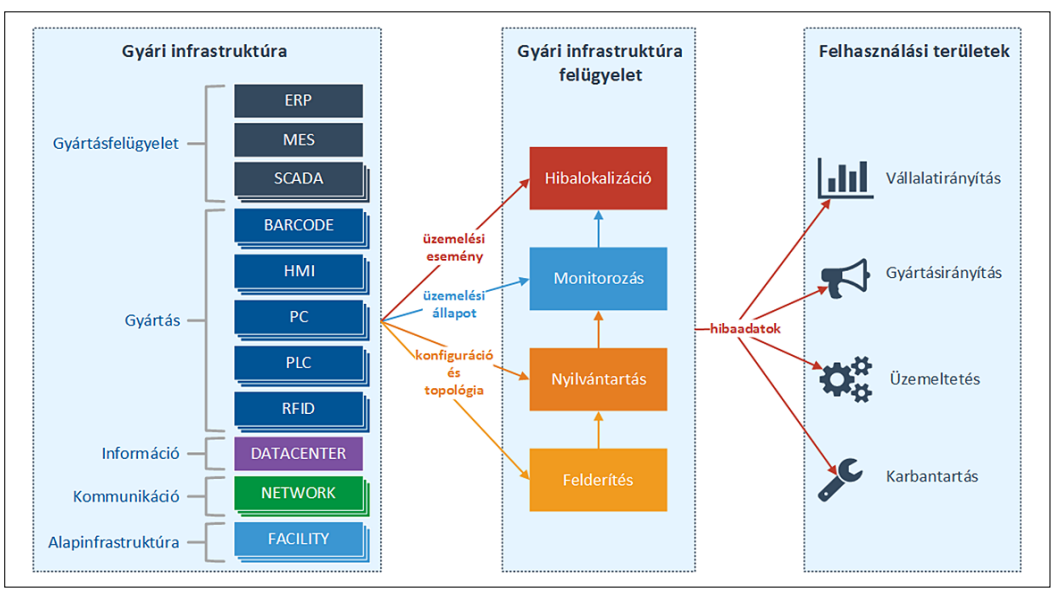
A monitorozó rendszer az elemek közvetlen lekérdezésével, vagy a hagyományos IT-, hálózat-, alapinfrastruktúra-felügyeleti rendszerekhez, illetve a gyártásirányítási rendszerhez kapcsolódva kérdezi le az egyes gyári infrastruktúra-elemek üzemelési állapotát. Amennyiben a rendszer valahol rendellenes működést észlel, akkor egy hibaeseményt generál a hibalokalizációs modul számára.

4. Hibalokalizáció – hibafelügyelet kialakítása:

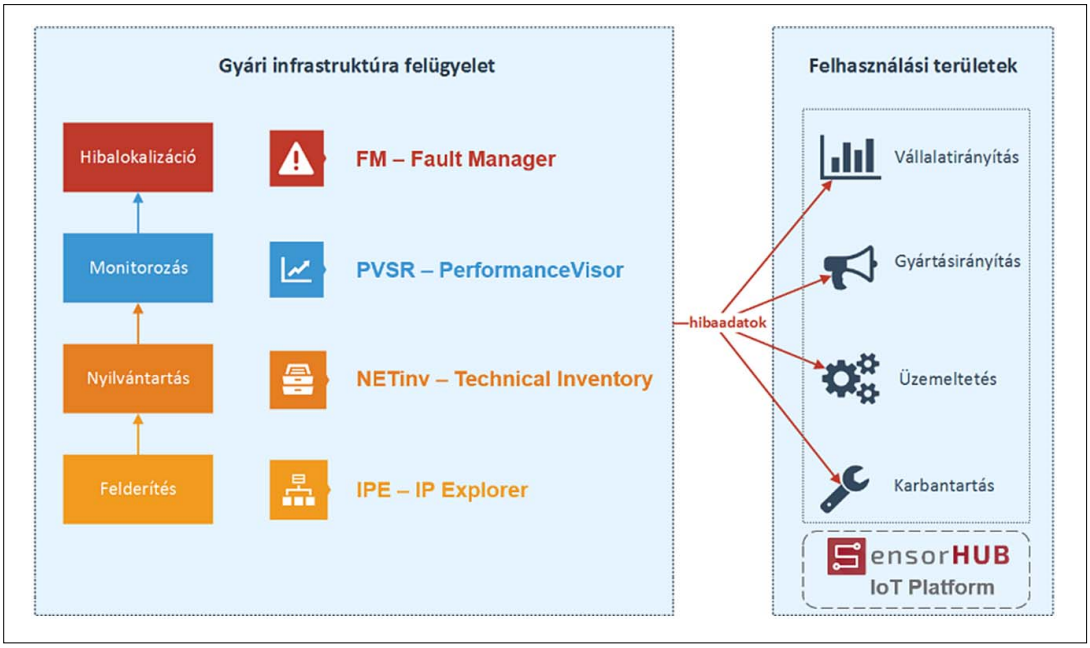
A rendszer üzemelési eseményeket fogad a gyári infrastruktúra elemeitől, a hagyományos IT-, hálózat-, alapinfrastruktúra-felügyeleti és gyártásirányítási rendszerektől, illetve az előző pontban említett teljesítményfelügyeleti rendszertől. A rendszer meghatározza, hogy melyik üzemelési esemény jelent tényleges hibát és melyik csak következménye egy másik hibának, azaz meghatározza, hogy ténylegesen melyik gyári infrastruktúra-elemmel kapcsolatban van probléma.



1. ábra Központi hibafelügyelet



2. ábra A gyári infrastruktúra felügyeletének működése



3. ábra Egységes gyári infrastruktúra-felügyeleti megoldásunk

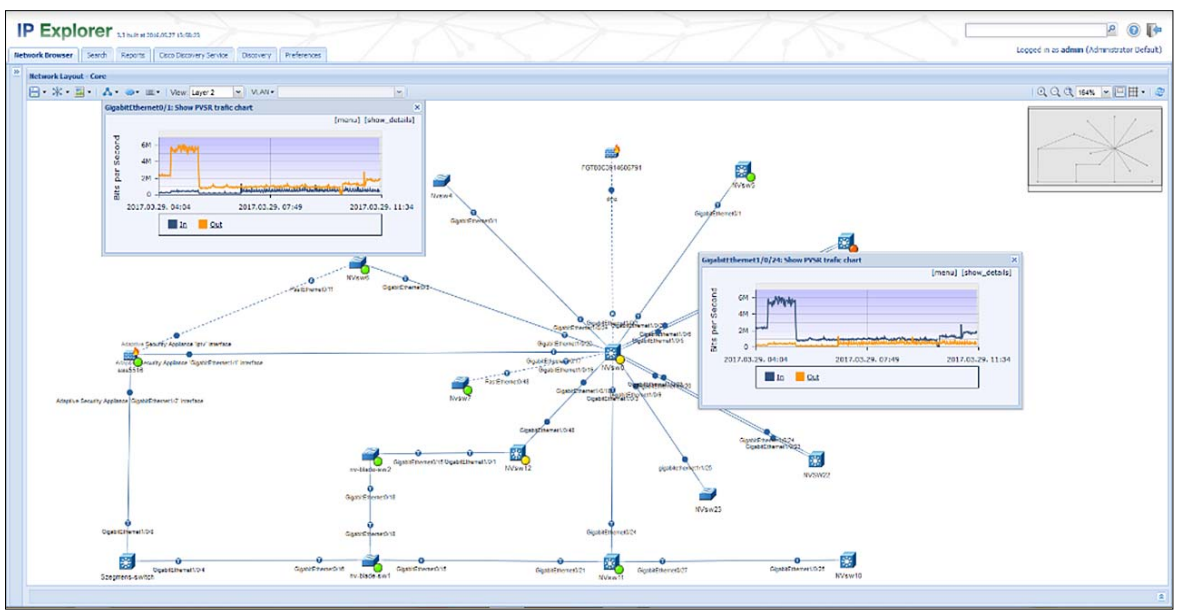
A gyári infrastruktúra felügyelete számos területen támogathatja a gyár működését, melyek közül a legfontosabbak:

– A *karbantartók* a gépek mellé elhelyezett kijelzőkön keresztül folyamatosan követni tudják a gépek, illetve a gépek működéséhez szükséges infrastruktúra-elemek üzemelési állapotát.
– Az *üzemeltetők* csak akkor kapnak riasztást, ha a meghibásodott infrastruktúra-elem üzemeltetése a felelősségi körükbe tartozik. Ez jelentősen javítja az üzemeltetés hatékonyságát.
– A *gyártásirányítás,* illetve a MES-rendszer meghibásodás esetén a hibaüzenet mellett a hibát okozó gyökérhibáról is információt kap.
– A *vállalatirányítás* vezetői riportokon keresztül átfogó információt kap a hibák számáról, jellegéről, illetve arról, hogy mely üzemeltetési szervezeteket érintettek a hibák.

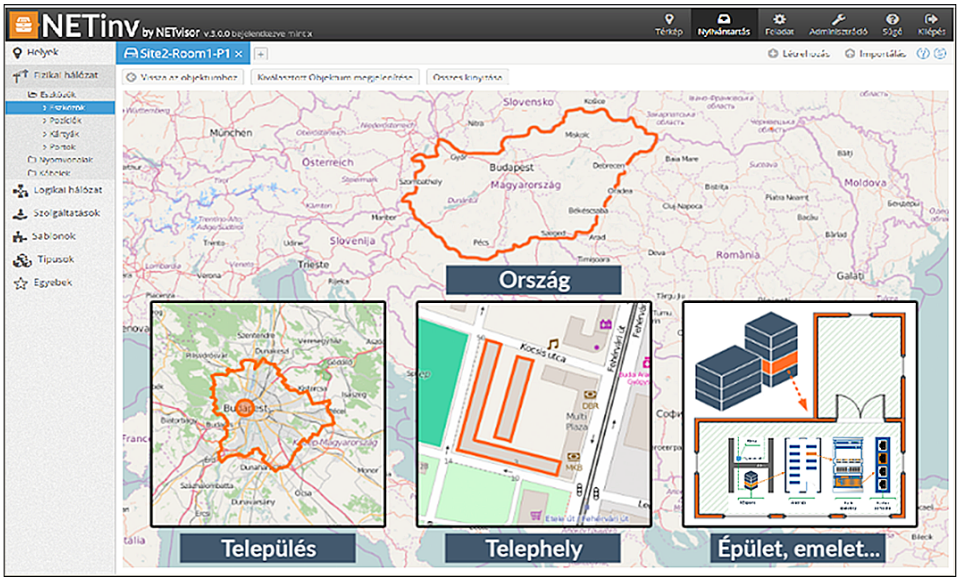
3. Egységes gyári infrastruktúra-felügyelet

A *3. ábrán* látható, Ipar 4.0 szemléletű, egységes gyári infrastruktúra-felügyeleti megoldásunk a NETvisor Zrt. üzemeltetést támogató szoftvereszközeiből és termékeiből – melyeket továbbfejlesztettünk a hagyományos infokommunikációs rendszerek üzemeltetésének támogatásán túl az Ipar 4.0 megoldások támogatásához is –, valamint a BME AUT tanszékének [3] munkatársai által fejlesztett IoT (Internet of Things – Tárgyak Internete) platformból tevődik össze.

Ezek az *IP Explorer (IPE)* [4], a *Technical Inventory (NETinv)* [5], a *PerformanceVisor (PVSR)* [6], a *Fault Manager (FM)* és a *SensorHUB* [7], amelyek a felderítés, nyilvántartás, monitorozás, hibalokalizáció, valamint a felhasználási területek támogatásának feladatait látják el. A következőkben ezeket mutatjuk be.



4. ábra IPE képernyőkép



5. ábra
Példa a NETinv által nyújtott térinformatikai támogatásra

3.1. Hálózat-felderítés

IPE • Az IP Explorer [4] egy olyan, a NETvisor Zrt. által fejlesztett szoftvereszköz, ami automatikusan felderíti az infokommunikációs hálózati erőforrásokat, automatizálja a hálózat dokumentálását és támogatja a műszaki nyilvántartási folyamatokat. Az IPE által felderített naprakész topológia- és csomópont-információk hatékonyan támogatják a modern infokommunikációs hálózat üzemeltetésének tervezési, ellenőrzési és hibaelhárítási folyamatait.

A *4. ábrán* egy tipikus IPE képernyőkép látható.

3.2. Nyilvántartás

NETinv • A NETinv [5] a NETvisor Zrt. által fejlesztett szoftvereszköz, amely térkép alapú integrált, többrétegű műszaki nyilvántartást biztosít IT-, távközlési és IoT-szolgáltatóknak, közművállatoknak, államigazgatási intézményeknek, nagyvállalatoknak és gyáraknak. A NETinv által nyújtott pontos, átfogó és hiteles IT- szolgáltatási és fizikai/logikai infokommunikációs hálózati-erőforrás-nyilvántartás elengedhetetlen a napi üzemeltetési feladatok hatékony végrehajtásához.

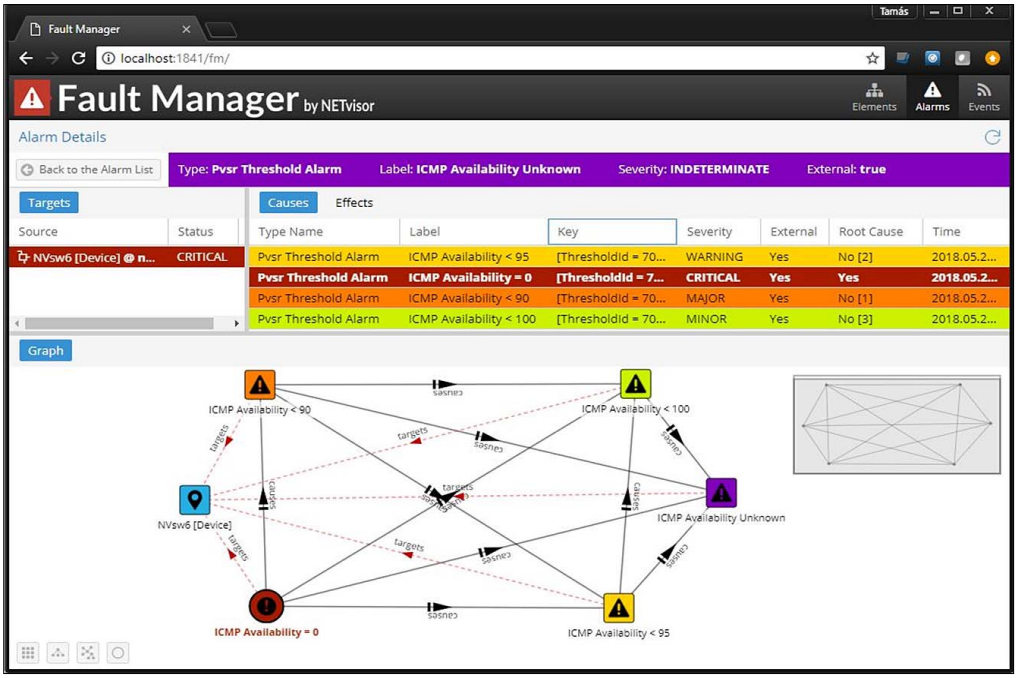
Az *5. ábrán* a NETinv által nyújtott térinformatikai támogatást szemléltető példa látható.

3.3. Monitorozás

PVSR • A PerformanceVisor [6] – egy olyan, szintén a NETvisor Zrt. által fejlesztett szoftvereszköz, – amely egységes felületen, átfogó módon, valós időben ellenőrzi és vizualizálja az IT- és infokommunikációs eszközök és szolgáltatások teljesítményét. Továbbá segíti a meghibásodások detektálását riasztások definiálásával, felgyorsítja a diagnosztikát és támogatást nyújt az erőforrás-kapacitások tervezéséhez, ezáltal csökkentve a költségeket és optimalizálva a kiadásokat. A PerformanceVisor mobil eszközökön futó változatban is elérhető, lehetővé téve ezáltal az azonnali, terepi használatot is, ami gyári környezetben számtalan előnnyel jár.

A *6. ábrán* egy tipikus PVSR képernyőkép látható.

6. ábra
PVSR képernyőkép



7. ábra
Tipikus FM képernyőkép

3.4. Hibalokalizáció

FM • A Fault Manager egy, a NETvisor Zrt.-nek még intenzív fejlesztés alatt álló szoftvereszköze, ami a NETinv-ben tárolt információkra alapozva előre megalkotja a felügyelni kívánt infrastruktúra felügyeleti modelljét, amit célirányos, gráfadatbázis alapú adattárolást és adatkezelést használva épít fel. Meghibásodás esetén a PVSR-ből és/vagy egyéb felügyeleti eszközökből érkező riasztásokat begyűjti, majd ezeken gyökérhiba-analízist végez az előre meghatározott, infrastruktúra-elemek/riasztások közötti korrelációk és szabályok alapján, feltárva ezáltal a probléma forrását.

A *7. ábrán* egy tipikus FM képernyőkép látható.

3.5. IoT platform

SensorHUB • A SensorHUB [7] egy olyan, a BME AUT tanszéke által kifejlesztett és jelenleg is folyamatos továbbfejlesztés alatt álló adatgyűjtő, elemző, megjelenítő és értékesítést támogató IoT-keretrendszer és -platform, amely különféle szak- és alkalmazási területek (pl. jármű és közlekedés, egészségügy, gyártósorok, intelligens városok) adatgyűjtését, kezelését és elemzését teszi hatékonnyá. Továbbá a SensorHUB ezen adatokra épülő alkalmazás- és szolgáltatásfejlesztést támogató keretrendszer is egyben.

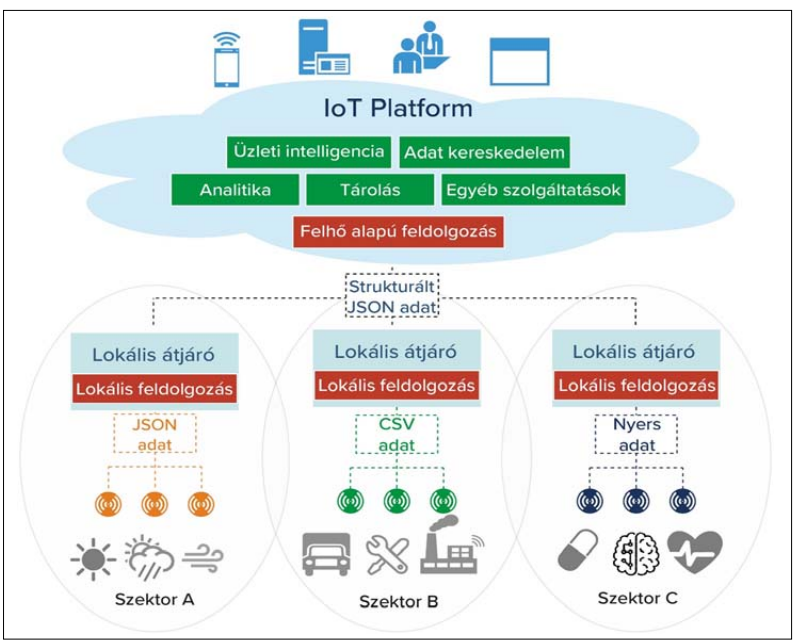
Alapvetően egy Apache Hadoop [8] alapú rendszer, mely támogatja a többfelhasználós működést (authentikációt, authorizációt, eszköznyilvántartást biztosít), valamint az üzenetek küldésére MQTT[7] és HTTP, míg azok tárolására MySQL és Apache HBase[8] támogatással rendelkezik.

A platform belső adatfolyam-kezelése grafikusan testreszabható, valamint rendelkezik integrált üzletiintelligencia alapú kimutatást készítő felülettel. Ezen felül támogatja a legelterjedtebb nyílt interfészeket és adatbázisrendszereket, továbbá a felhő- vagy saját infrastruktúra alapú telepítést. Az IoT platform általános koncepcióját a *8. ábra* illusztrálja.

4. Demonstrációs terepasztal

Az infrastruktúra-felügyeleti rendszerünk működésének a szemléltetése céljából kidolgoztunk és megvalósítottunk egy demonstrációs terepasztalt, amelynek egyik

8. ábra IoT platform általános koncepciója



7 *Message Queuing Telemetry Transport – Üzenet alapú kommunikációs protokoll*
8 *Nyílt forráskódú nem relációs (NoSQL) adatbázis*

9. ábra
A NETvisor Zrt. IoT tesztlaborjában található demonstrációs terepasztal

10. ábra
Terepasztal a demonstrált palackozóüzem szcenárióval

példánya 2019 végéig állandó kiállítás keretében megtekinthető és kipróbálható a BME Ipar 4.0 Technológiai Központban, a másik példánya pedig a NETvisor Zrt. IoT tesztlaborjában kapott helyet. A demonstráció kétnyelvű, így minden felirat, funkció, kezelő- és visszajelző felület elérhető mind magyar, mind pedig angol nyelven. A *9. ábrán* az IoT tesztlaborban található demonstrációs terepasztal látható.

4.1. Szcenárió

A terepasztalon demonstrált szcenárió egy egyszerű palackozóüzemet illusztrál, amely a következő részegységekből áll (ahogyan a *10. ábrán* is látható): Targonca, Futószalag és Tartály, Kommunkációs központ, Felügyeleti központ, Raktár, Beavatkozási konzol.

A demonstrációban monitorozzuk az illusztrált palackozóüzem Gyártás, Áramellátás és a Kommunikációs alrendszereinek, illetve ezek főbb összetevőinek a működését. Ezen monitorozott komponenseket és jellemzőket a *1. táblázat* tartalmazza.

A demonstrációt megvalósító részegységek egy lokálisan kialakított, csillag topológiájú Wi-Fi-hálózaton keresztül kommunikálnak egymással, ahogy ez a (következő oldali) *11. ábrán* látható. A csillag topológia központi eleme egy Wi-Fi AP (Access Point – hozzáférési pont), amelyhez mind a végponti eszközök, mind a Felügyeleti központ Wi-Fi-linken keresztül csatlakozik. Amikor a demonstrált üzem normál működését valamilyen meghibásodás hátráltatja, akkor a *Felügyeleti központban* futó FM (Fault Manager) komponens – begyűjtve a riasztásokat a PVSR-ből és/vagy az egyéb alrendszereket monitorozó eszközökből – összefüggéseken és szabályokon, valamint célirányos, gráfadatbázist használó adattárolás és adatkezelésen alapuló gyökérhiba-analízist végez, rámutatva a hiba valószínűsíthető forrására. Ennek köszönhetően a hiba elhárítása már célirányosan, hatékonyan történhet.

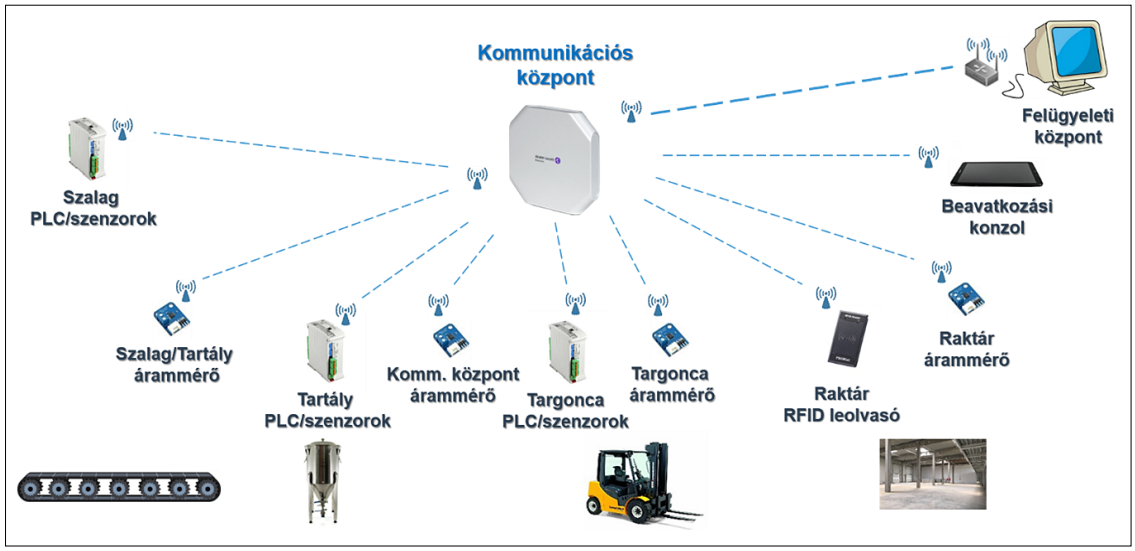
4.2. Működés

A demonstráció normál működése automatikus. Az önvezető targonca egy palackokkal teli rekeszt hordoz körbe a terepasztalon rögzített útvonal mentén, illusztrálva ezzel a főbb működési fázisait egy palackozóüzemnek, amelyek a következők:

– üres rekesz mozgatása;
– palackok feltöltése a Futószalagon;
– feltöltött palackokkal teli rekesz mozgatása;
– feltöltött palackokkal teli rekesz üres palackokkal töltött rekeszre való cserélése a Raktárban.

Gyártás	Áramellátás	Kommunikáció
• Szalag–PLC/szenzorok • Tartály–PLC/szenzorok • Targonca–PLC/szenzorok • Raktár-RFID-leolvasó	• Kommunikációs központ • Szalag/Tartály • Targonca • Raktár	• Kommunikációs központ • Kommunikációs központ elérhetősége • Szalag-PLC/szenzorok elérhetősége • Tartály-PLC/szenzorok elérhetősége • Targonca-PLC/szenzorok elérhetősége • Raktár-RFID-leolvasó elérhetősége • Kommunikációs központ árammérő elérhetősége • Szalag/Tartály árammérő elérhetősége • Targonca árammérő elérhetősége • Raktár árammérő elérhetősége

1. táblázat
A demonstrált szcenárió monitorozott komponensei, illetve jellemzői



11. ábra
A terepasztal részegységeinek lokális Wi-Fi-alapú kommunikációs hálózata

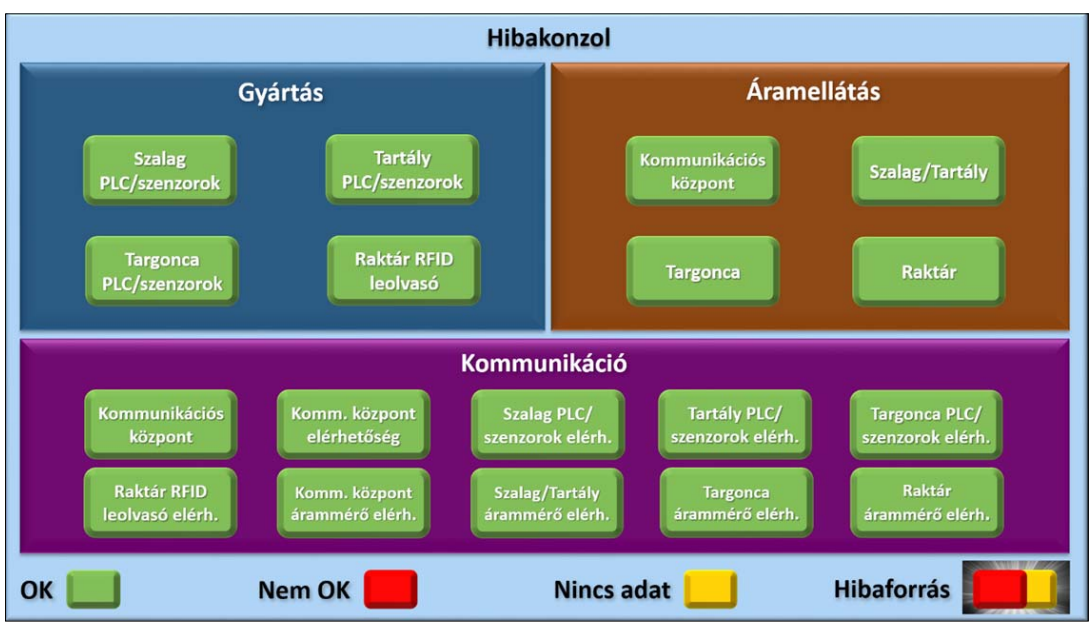
Az aktuális működési státusza a különböző alrendszerek főbb komponenseinek/jellemzőinek folyamatosan, valós időben monitorozásra kerül, amit az *FM hibakonzolja* jelenít meg vizuálisan, ahogy az a *12. ábrán* látható. A zöld szín (normális működés) jelzi, hogy az adott komponens/jellemző hibamentes. A piros szín meghibásodásra, vagy a normális működéstől való eltérésre utal. A sárga szín azt jelzi, hogy nem lehet megállapítani a normál vagy hibás működést, mert ehhez nem áll rendelkezésre megfelelő adat.

A normál működésen túl implementálásra került számos hibaszcenárió egyszerűbb és összetettebb meghibásodásokat szemléltetve, mind a három alrendszer vonatkozásában. Ezek a hibaszcenáriók két csoportba oszthatók úgy, mint programozott hibák, illetve manuális interakciót igénylő hibák.

A *programozott hibák* az automatikusan futó demonstráció részét képezik. A targonca a demonstráció elindítása után összesen 6 kört tesz meg a terepasztalon, majd *alvó* üzemmódba vált, amiből felébresztve ismét megtesz 6 kört, és így tovább. Három programozott hiba került implementálásra, mind a három alrendszerre vonatkozóan egy-egy. Ezek közül aktiválódik az egyik minden páros körben. Ezen hibákból a rendszer automatikusan helyreáll, biztosítva ezáltal a demonstráció folyamatos működését.

A *manuális interakciót igénylő hibák* lehetővé teszik az érdeklődők számára a demonstráció folyamatába való interaktív beavatkozást a *13. ábrán* látható *Beavatkozási konzol* segítségével, amely egy érintőképernyős mobil eszközön (tableten) keresztül érhető el. Itt szintén három meghibásodás – mind a három alrendszerre vonatkozóan egy-egy – idézhető elő a megfelelő hibagomb megérintésével. Ezen hibák esetén a meghibásodásból való helyreállás nem automatikus, ezt szintén itt lehet kezdeményezni a hibagomb ismételt megérintésével. Valamint ezen a konzolon keresztül van lehetőség a demonstráció alvó módból való felébresztésére és így az automatikus működés újraindítására, illetve a működés pillanatnyi felfüggesztésére/folytatására is.

Az előidézett hibák – mind a programozott, mind pedig a manuális interakciót igénylők – megjelenítésre ke-



12. ábra
Az FM hibakonzolja

13. ábra Beavatkozási konzol

rülnek úgy a terepasztalon, mint az FM hibakonzolján. A hibakonzol megmutatja az egyes hibákat és azok kihatását, ha van ilyen, a többi alrendszerre vonatkozóan, illetve a hiba forrását villogással jelzi. A *14. ábrán* látható példa a manuálisan előidézhető *Kommunikációs központ meghibásodása* hibaszcenárió hibakonzolját ábrázolja a gyökérhiba-analízis segítségével behatárolt villogó komponenssel (Kommunikációs központ), mint valószínűsíthető hibaforrással. Látható, hogy egy ilyen komplex hibaszcenárió esetén mekkora segítséget jelent, ha pontosan tudjuk, hol a hiba forrása, hova kell menni a hibát elhárítani!

A fentebb tárgyalt funkciókon túl még egy hasznos, kiegészítő funkció implementálásra került. Amennyiben a mobiltelefonunkkal felcsatlakozunk a demonstrációban kialakított lokális *guest (vendég)* Wi-Fi-hálózatra, akkor a telefon webböngészőjében automatikusan egy olyan oldal nyílik meg, amely minden egyes meghibásodásról és a hibából való helyreállásról valós időben egy-egy üzenetet jelenít meg *(15. ábra)*. Ez a funkció illusztrálja azt a kényelmi szolgáltatást, amikor az üzemben az operátor és/vagy a karbantartó meghibásodás esetén egy SMS-ben értesül az eredő hibaforrásról – ezáltal a hibaelhárítás lényegesen felgyorsítható –, illetve a hiba elhárítását követően szintén egy SMS jelzi a hibából való helyreállást.

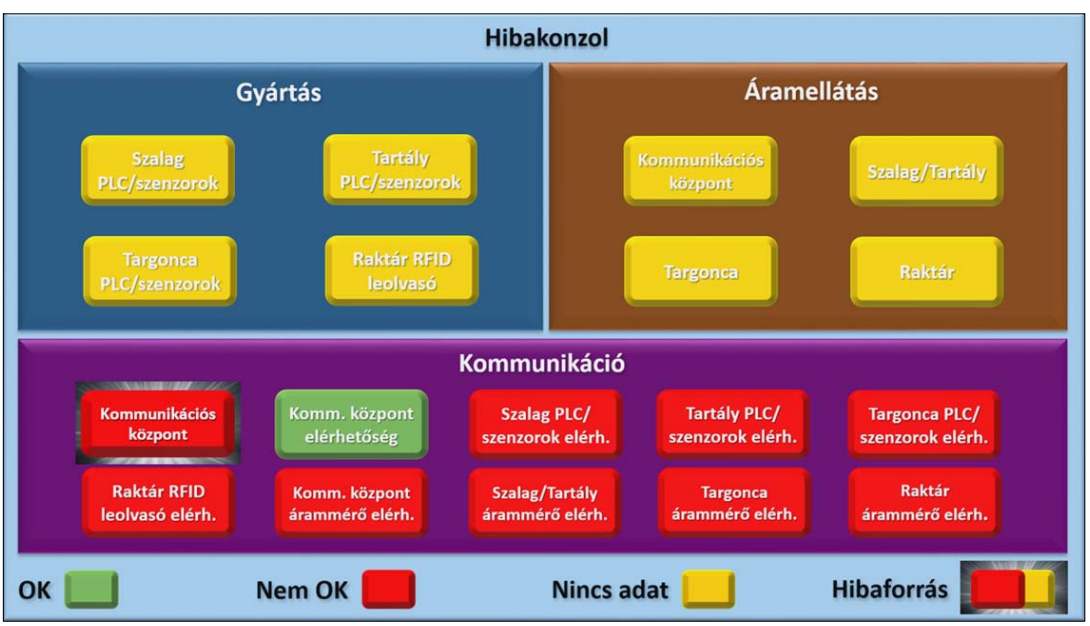
5. Összefoglalás

A vállalatoknak a versenyképességük megtartása illetve növelése érdekében elengedhetetlenül szükséges, hogy digitalizálják és automatizálják az üzleti, működési folyamataikat, melyet Ipar 4.0-ként aposztrofálunk. Ez jórészt magas szinten integrált rendszereket eredményez, beleértve a gyári infrastruktúra felügyeletét is.

A cikkben bemutatásra került az Ipar 4.0 szemléletet követő, egységes gyári infrastruktúra-felügyeleti megoldásunk. Az üzemi működés során fellépő meghibásodások valós időben való detektálását, és a hibafelügyeleti komponens segítségével az eredő hibaforrás beazonosítását egy palackozóüzem egyszerűsített működését illusztráló demonstrációs terepasztal segítségével szemléltettük.

Gyári környezetben részben vagy egészében telepítésre került infrastruktúra-felügyeleti rendszerünk referenciái közül a *2. táblázat* tartalmaz néhányat pár kiegészítő információ kíséretében.

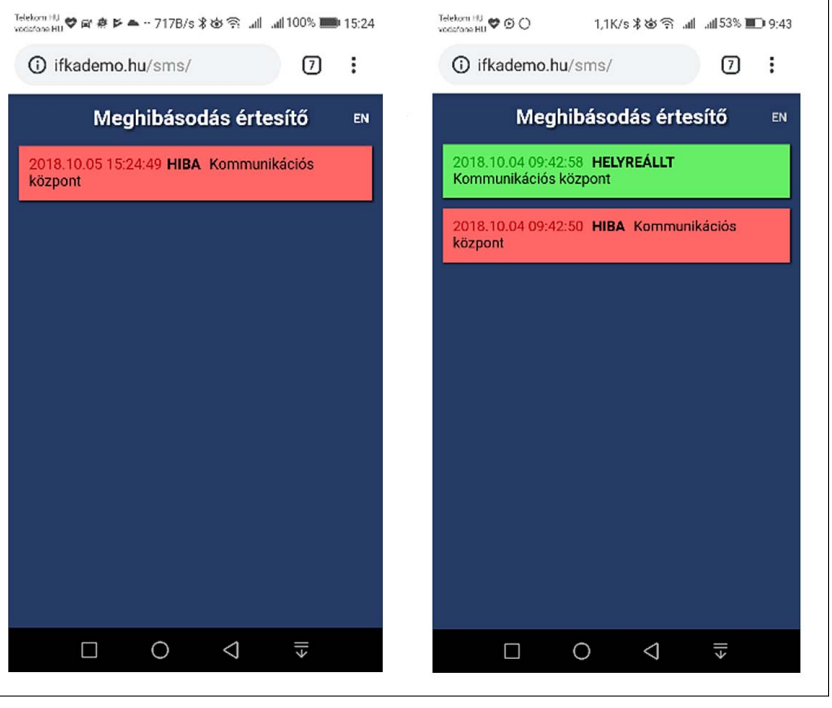
Az egységes gyári infrastruktúra-felügyeleti megoldásunkkal jelentősen csökkenthető a hibalokalizálási idő és felgyorsítható a hibaelhárítás, ennek következtében minimalizálható a termeléskiesési idő, valamint a jelentkező bevételkiesés. Ez a megoldás minden olyan termelő vállalat számára hasznos lehet, ahol a gyár működése összetett, az egyes alrendszerekben történő meghibásodások hatással vannak a többi alrendszerre is, így a hibalokalizáció hagyományos módon való kezelése valós és időigényes kihívást jelent.



14. ábra Hibák és az eredő hibaforrás megjelenítése az FM hibakonzolján

Suez Water Technologies and Solutions Kft. (Oroszlány)	Richter Gedeon Nyrt. (Budapest)	BorgWarner Oroszlány Kft. Turbo Systems (Oroszlány)
• IPE: 300 végpont; napi frissítés • NETinv: 300 eszköz / szolgáltatás; inkrementális frissítés • PVSR: 350 monitorozott eszköz / szolgáltatás; 18k mérés 5 percenként; 50 GByte adattár; nyers adat az elmúlt 90 napról, utána órás átlagok • FM: pilot telepítés	• IPE: 750 végpont; napi frissítés • PVSR: 500 monitorozott eszköz / szolgáltatás; 12k mérés 5 percenként; 50 GByte adattár; nyers adat az elmúlt 90 napról, utána órás átlagok	• IPE: 2,5k végpont; napi frissítés • PVSR: 400 monitorozott eszköz/szolgáltatás; 14k mérés 5 percenként; 50 GByte adattár; nyers adat az elmúlt 120 napról, utána órás átlagok

2. táblázat
Gyári infrastruktúra-felügyeleti rendszerünk néhány referencia-telepítése



15. ábra
SMS szolgáltatás: Eredő hiba / Hibából való helyreállás

Köszönetnyilvánítás

A cikkben bemutatott egységes gyári infrastruktúra-felügyeleti rendszert és annak demonstrációját a 2017-1.3.1-VKE-2017-00042 sz. projekt keretében a NETvisor Zrt., a BME AUT tanszéke és a CS-Process Mérnöki Kft. által alkotott konzorcium dolgozta ki és valósította meg.
A 2017-1.3.1-VKE-2017-00042 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Versenyképességi és Kiválósági Együttműködések pályázati program finanszírozásában valósul meg.

A szerzőről

FARKAS KÁROLY 1998-ban szerzett műszaki informatikus mérnök diplomát, majd 1999-ben bankinformatikus szakmérnök diplomát a BME Villamosmérnöki és Informatikai Karán. Az egyetem elvégzése után doktori tanulmányait a BME-n kezdte, majd Svájcban, a Zürichi Műszaki Egyetemen (ETH Zürich) folytatta, ahol 2007-ben megszerezte a PhD-fokozatot. 2007–2012 között a Nyugat-magyarországi Egyetem (NymE) Informatikai és Gazdasági Intézetének, 2008-tól a BME-HIT (Hálózati Rendszerek és Szolgáltatások, korábban Híradástechnika) Tanszékének docense, ahol 2017-ben habilitált. 2016 szeptemberétől a NETvisor Zrt. K+F igazgatója. A 2011/2012-es tanévet az Universitaet Zürich-en töltötte vendégprofesszorként.
Oktatási és kutatási tevékenységét elsősorban a kommunikációs hálózatok területén végzi, különös tekintettel az autonóm, önszerveződő vezeték nélküli mobil hálózatok, beltéri helymeghatározás, közösségi érzékelés, valamint az IoT és Ipar 4.0 témakörökben. Több, mint 90 tudományos publikációval rendelkezik, a publikációira történő független hivatkozások száma 700 feletti. Rendszeresen szerepel előadóként különböző eseményeken, konferenciákon, tanfolyamokon, továbbá rendszeresen részt vesz a nemzetközi tudományos életben, mint konferenciaszervező vagy a szakmai bizottság tagja.
2016-ban az MTA elismerő oklevélben részesítette, melyet az Akadémia a 2012–2015 időszakra elnyert és kiváló minősítéssel zárult Bolyai János Kutatási Ösztöndíj keretében végzett kiemelkedő kutatói munkáért adományozta. Farkas Károly koordinátora a BME-n működő lokális Cisco Hálózati Akadémiának; alapítója és koordinátora a BME-HIT-en működő Cisco IPv6 Tréning Laboratóriumnak; valamint kezdeményezője és főszervezője a felsőoktatásban hallgatók számára évente BME-Pannon NetSkills Challenge néven meghirdetett, számítógép-hálózatos témájú országos tanulmányi versenynek. A Cisco Hálózati Akadémia képesített instruktor trénere, valamint rendelkezik Cisco CCNA R&S / CCNA Security / CCNA CyberOps / CCNP R&S ipari vizsgákkal. 2017-ben Cisco Instructor Excellence Advanced Award díjban részesült a Cisco Hálózati Akadémia programjában végzett kiváló instruktori munka elismeréseként.

Hivatkozások

[1] BME Ipar 4.0 Technológiai Központ, *https://ipar4.hu/hu/page/ipar-4-0-technologiai-kozpont*
[2] NETvisor Zrt., *http://www.netvisor.hu*
[3] BME AUT Tanszék, *https://www.aut.bme.hu*
[4] IP Explorer, *http://www.netvisor.hu/termekeink/ip-explorer-halozat-felderites*
[5] NETinv, *http://www.netvisor.hu/termekeink/netinv-muszaki-nyilvantartas*
[6] PerformanceVisor, *http://www.netvisor.hu/termekeink/pvsr-performancia-monitorozas*
[7] SensorHUB, *http://sensorhub.autsoft.hu/docs/index.html*
[8] Apache Hadoop, *http://hadoop.apache.org*

Ipari diszpécseri DMR-rádiózás korszerűsítési tapasztalatai az analóg-digitális átállás kapcsán

TURCSÁN ZSOLT
NOVOFER Zrt.
tzs@novofer.hu

Kulcsszavak: dPMR, DMR, hangminőség, beszédérthetőség

A digitális PMR-rádiózás közel tíz éve váltja fel a hagyományos, analóg beszéd- és adatrádiózást. Az analóg rendszerek felhasználói igényei alapján a gyártók és integrátorok az elmúlt évtizedekben folyamatosan fejlesztették az analóg rendszerek kommunikációs képességeit, többek között csatornavédelemmel, titkosítással, trönkölési megoldásokkal, egyéni- és csoporthívásokkal, helymeghatározási képességekkel. A digitális technológiák számtalan kényelmi és értéknövelő szolgáltatást kínálnak.
Ezek egy része, mint például könnyen használható titkosítás, földrajzilag elkülönülő hálózatok költséghatékony összekötése és fejlett helymeghatározási szolgáltatások, egyértelmű előnyként jelentkeznek marketing- és technikai oldalon is, míg a digitális beszédkódolás hatása és a hálózatok összekötéséhez szükséges adatátviteli hálózatok, illetve az elosztott elemek helyett megjelenő központi elemek megbízhatósága számtalan kérdést és problémát vet fel a tervezés, megvalósítás során.
A cikk végigkíséri a különböző méretű és összetettségű magyarországi hálózatok átalakítási tervezési, kivitelezési és üzemeltetési kérdéseit, tapasztalatait, értékeit és hátulütőit.

1. Bevezetés

Az iparban is széles körben használt keskenysávú, analóg URH diszpécseri beszédátviteli megoldásokat (PMR) a 2000-es évektől kezdődően egyre szélesebb körben váltotta fel az alapvetően sávtakarékosabb, digitális modulációra épülő dPMR változat. Az új rendszerek elsősorban a meglévő, de elavult rendszerek leváltásával (migráció-korszerűsítés) jöttek létre, így a korszerűsítési-megújítási folyamatban olyan felhasználói körhöz jutottak el, akik azokat a munkájukhoz évek óta, nap mint nap használták, ezért gyakorlott felhasználóként különösen érzékenyek voltak a változások pozitív és negatív hatásaira egyaránt.

A cikk két korszerűsítéssel kapcsolatos esetet mutat be, melyek során két olyan – eltérő forrású – problémával találkoztunk, amik a korszerűsítést megelőző rövid tesztelési és bevezetési folyamatok alatt nem kerültek elő és a felhasználók korábbi rendszerekben megszokott, analóg hangminőséggel kapcsolatos elvárásaival ütköztek. A fejlődés és az egyes ismertebb dPMR megoldások első szakaszbéli bemutatása után a második szakasz egy gyakorlati eseten keresztül áttekinti a digitális kódolás-dekódolásból fakadó hangminőséggel kapcsolatos felhasználói problémákat, míg a harmadik szakasz egy területileg nagykiterjedésű rendszer összeköttetési problémáiból fakadó, hangminőséggel és rendelkezésre állással kapcsolatos nehézségeit mutatja be.

2. A dPMR rendszerek fejlődése

Az 1920-as évek végétől fejlődésnek indultak, majd rohamosan terjedtek az elsősorban beszédátviteli igényeket kiszolgáló vezeték nélküli, kétirányú kommunikációs megoldások, népszerű nevükön rádiótelefonok. Hasonlóan a vezetékes távközlési megoldáshoz, ezek a rendszerek is alapvetően a távolság miatt közvetlenül nem működőképes, emberek közötti kommunikációs igények kiszolgálására születtek. A rendszereknek – hasonlóan más ipari megoldásokkal együtt – a második világháborúhoz köthető technikai fejlődés nagy lökést adott, így az 1960-as évekre más meglehetősen kiforrott, a civil életben is elterjedt megoldások és gyártmányok jöttek létre.

A Galvani Manufacturing-ból létrejövő Motorola mellett a PYE, a Philips, a SIMOCO és az Ericsson is korán képviseltette magát megoldásaival, melyek alapvetően az analóg AM/FM/PM, keskenysávú (50 kHz alatti csatornaosztású) kialakításokkal üzemeltek évtizedeken keresztül, egyre korszerűbb kiegészítő kényelmi és kapacitásbővítést eredményező trönkölési megoldásaikkal.

A rádiótelefon-rendszerek terjedésének és az új kommunikációs megoldások térhódításának hatására az erre a célra használható frekvenciatartományok (tipikusan a 80, 160, 300 és 450 MHz-es sávok egyes részei) szűkössé váltak és a felhasználói igények között is megjelentek a kényelmi funkciók (szelektív hívás, titkosítás stb.), így kézenfekvő volt a sávtakarékosabb digitális modulációs eljárások bevezetése. Az ilyen célú digitális rendszerek a TETRA- és a GSM-technológiával párhuzamosan, némileg azok után, a 2000-es években születtek és kerültek szabványosításra, így számos jellemzőjükben követték az ottani megoldásokat.

Míg a sávtakarékosságra két eltérő filozófiájú megoldás is létrejött és a mai napig is létezik (FDMA és TDMA), addig a hang digitális előfeldolgozására, kódolására és dekódolására ezen a területen szinte egyeduralkodó vált az amerikai DVSI AMBE+2™ rendszere, illetve annak al-

változatai. Az AMBE+2 kódolás kifejezetten élőbeszéd tömörítésére lett optimalizálva, kód-tár alapon (codebook-based speech coder) és a vokóder mind hardveres, mind szoftveres változatban licencelhető, megvásárolható.

Az FDMA-rendszerek tipikus képviselője a Kenwood™ és Icom™ NXDN nyílt szabványán alapuló Nexedge™ és IDAS™ rendszerek, elsősorban az ázsiai piacokra célozva. A rendszer jellemzője, hogy a 12,5 kHz-es csatornaosztást 2 db 6,25 kHz csatornára osztja, így egyidőben párhuzamosan két kommunikáció folyhat.

A TDMA-rendszerek tipikus példája a Motorola™, Yaesu™, Hytera™ stb. által is használatos, az ETSI Standard TS 102 361-on alapuló megoldások, ahol a 12,5 kHz-es csatornaosztást időben két időrésre osztva történik a felhasználó szempontjából párhuzamosan két kommunikáció.

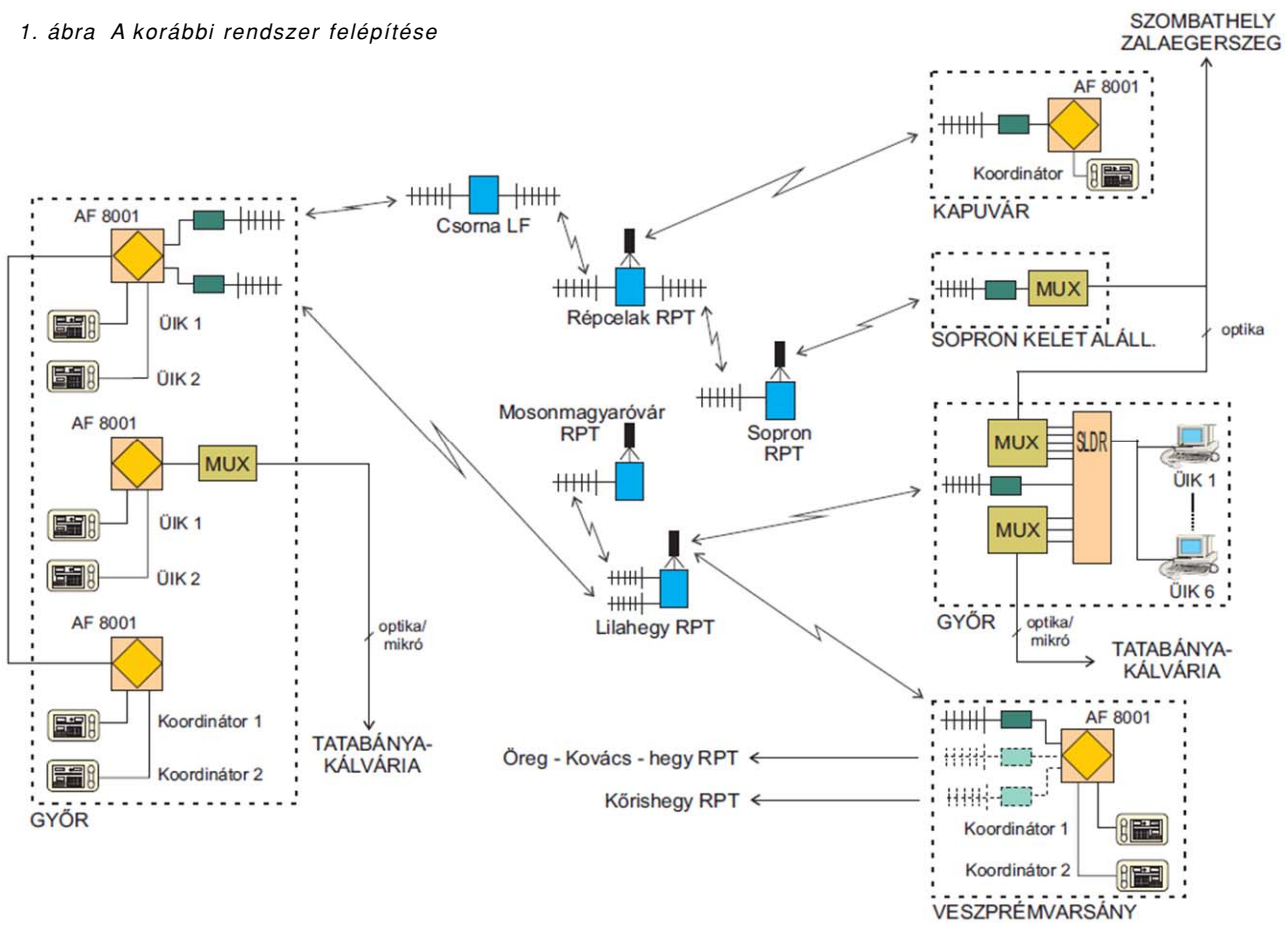
3. Ipari szolgáltatói hálózat migrációja

Az egyik vezető hazai ipari szolgáltató vállalat több megyére kiterjedő analóg diszpécseri rendszere az 1960-as években a volt BRG gyártmányait felhasználva épült fel *(1. ábra)*, majd az 1990-es évek végi rekonstrukcióját követően nyerte el jelenlegi formáját már Motorola berendezésekre alapulva. A rendszer közel 30 bázisállomást tartalmaz, melyeket hasonló vezeték nélküli berendezések segítségével kötöttünk össze rendszerré. A beszédátvitel mellett analóg jelzésekre épülő hívóazonosítással és hangrögzítéssel is kiegészítve évtizedeken keresztül kiszolgálta a felhasználói igényeket. A rendszer legnagyobb hátránya volt, hogy a felhasználóknak kézzel kellett bázisállomást (csatornát) választania, mivel a rendszer nem tartalmazott automatikus eljárást erre a funkcióra.

A rendszer amortizációjával és a digitális technológia elérhetőségével, elterjedésével együtt felmerült az igény a modernizációjára, így kiválasztásra került a rendszer egy kisebb, négy bázisállomásból álló, önállóan átalakítható része, kísérleti bevezetés céljaira. A rendszer korszerűsítése során az analóg bázisállomásokat digitális (DMR szabványú) átjátszó állomásokra cseréltük, a bázisállomások egymás és a diszpécseri munkahelyek közötti analóg, vezeték nélküli összeköttetéseit IP-alapú hálózattal helyettesítettük és teljes készülékcserét hajtottunk végre. A tesztrendszer elsődleges célja az egyes bázisállomások által lefedett területek közötti szabad és felhasználói beavatkozás nélküli átmenet, átjárhatóság (roaming) tesztelése volt.

A terepi tesztek során egyre több felhasználót vontunk be, akik jelezték, hogy a rendszer számtalan előnye mellett a hangminősége jelentősen eltér a korábban megszokott, analóg rendszerhez köthető hangminőségtől, megnehezítve ezzel a beszélgetésben részt vevő partner beazonosítását, illetve fokozottabb koncentrációt, odafigyelést igényel a beszédértés. Gyakorlatias megfogalmazásuk szerint a rendszerből kijövő hang olyan, mintha azt egy beszédszintetizátor állított volna elő.

1. ábra A korábbi rendszer felépítése



A probléma feltárására teszteket folytattunk le, melyekben a végkészülékek eltérő viselkedést mutattak ezen a kritikus területen. Míg a kézi berendezések és a mobil berendezések közötti eltéréseket egyértelműen a mikrofon és a hangszóró körüli akusztikai kialakítással magyarázhattuk és szoftveres beállítással némileg korrigálhattuk, addig a számítógépes kezelő rendszer lényegesen gyengébb hangminőséget produkált mindkét irányban. A kezelő rendszert megvizsgálva kiderült, hogy az akusztikailag kedvezőbb mikrofon és hangszóró megoldás mellett a hang kódolására és dekódolására használt szoftveres megoldás csak közelíti a végkészülékekbe épített hardveres vokóder áramkör tulajdonságait, így azt is hardveres megoldással kellett kiegészíteni, USB-felületű külső vokóder beépítésével. A probléma feltárása során irodalmi adatok alapján arra a következtetésre jutottunk, hogy a magyar nyelvű környezetben az eltérő kódolási-dekódolási eljárások jelentős mértékben ronthatják a beszédérthetőséget, így minden olyan alkalmazásnál, ahol a beszéd érthetősége kritikus, célszerű azonos kódolási- és dekódolási eszközt és eljárást alkalmazni.

A rendszer kiegészítésével és finomhangolásával elérhetővé vált egy olyan állapot, amiben a felhasználók elfogadhatónak ítélték a hangminőséget és beszédérthetőséget, de az évtizedeken keresztül megszokott analóg hangminőséget és beszédérthetőséget nem sikerült maradéktalanul teljesíteni. Ennek oka alapvetően a sávtakarékos kódolás jellemzőiből fakad, kiegészítve azzal, hogy a vokóder alapvetően az angol és hasonló nyelvekből kiindulva született, így a magyar nyelv hangzásbéli sajátosságaira kevésbé készítették fel.

A tesztelésekben számtalan eltérő orgánummal, hangszínnel és beszédstílussal rendelkező kolléga vett részt, így kiderült, hogy a vokóder kialakításából fakadóan eltérően kezeli az egyes felhasználók beszédét. A beszéd összesített spektrális felépítése egyéni jellemző, a vokóder kialakítása során az ideális beszélőt tekintve egyfajta átlagot képezve hozták létre az eljárás paramétere-zését, így néhány felhasználó hangja nagyon jól érthető és beazonosítható maradt, míg számos kolléga hangjából minden egyéni jellemző eltűnt és beszédérthetőségük is korlátozottá vált. Az általunk vizsgált felhasználók számára néhány hetes-hónapos használati időszak alatt a rendszer által biztosított hangminőség és beszédérthetőség elfogadhatóvá vált, annak ellenére, hogy a bevezetés után a rendszerben további, a hangminőséggel összefüggő változtatást nem hajtottunk végre.

Miután a DMR-rendszer szabványosított megoldása nagyon kevés finomhangolási lehetőséget kínál (elsősorban az analóg mikrofon áramkörökre összpontosítva), így a migrációs folyamat során több időt kell hagyni az erre érzékenyebb felhasználóknak a hangminőség és beszédérthetőség változásának feldolgozására, megszokására, illetve kifejezetten javasoljuk a bevezetést megelőzően terepi teszteken bemutatni a felhasználóknak a rendszer által biztosított beszédátvitel jellegzetességeit, tulajdonságait.

4. Közösségi szolgáltatói hálózat migrációja

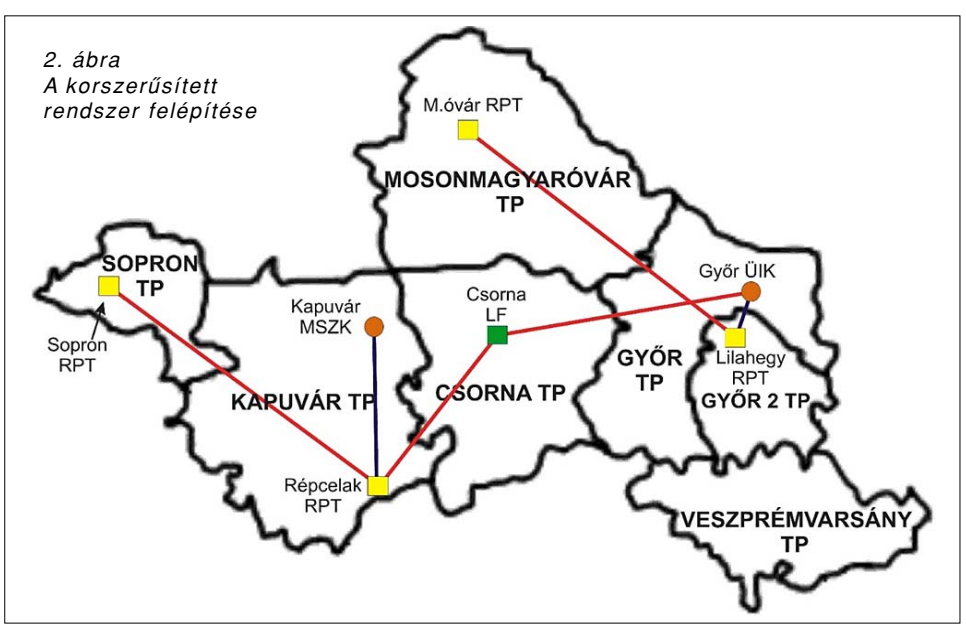
Egy, a Balaton vonzáskörzetében 15-20 évvel ezelőtt létesült többcsatornás, két bázisállomással rendelkező trönkölt diszpécseri URH-rendszer bővítését kellett végrehajtani, korlátozott anyagi és technológiai erőforrások rendelkezésre állása mellett.

Az ellátott és lefedett terület növelése, az elérhető telephelyek költségének minimalizálása és a párhuzamosan használni kívánt beszédcsatornák mennyisége miatt öt, IP-hálózattal összekötött telephellyel üzemelő, telephelyenként egy frekvenciás, két időréssel üzemelő DMR-rendszert választottunk ki, melyek összekötésére nem állt rendelkezésre dedikált hálózat, helyette 3G/LTE, illetve „vezetékes” szolgáltatói nyílt internet-hálózatokat biztosított a megrendelő.

A rendszer tesztelése során a korábban is említett hangminőséggel, beszédérthetőséggel összefüggő anomáliák mellett további problémák is mutatkoztak a beszéd szakadozottságával, időszaki kimaradásával kapcsolatban.

A problémákat elemezve kiderült, hogy az alkalmazott DMR-rendszer IP-alapú összeköttetési igénye sávszélességét tekintve ugyan alacsony, de a csomagok késleltetésével szemben korántsem megengedő, tipikusan 70-80 ezredmásodperc feletti késleltetés hatására a beszédérthetőség drasztikusan romlik, majd a késleltetés további növekedése esetén az összeköttetés megszakad.

2. ábra
A korszerűsített rendszer felépítése



A rendszerben felhasznált telephelyek mindegyike a területi rádiófrekvenciás lefedettség okán került kiválasztásra, a telephelyen jelen lévő szolgálatok korábban nem igényelték a stabil internet kapcsolatot, így a rendelkezésre álló „vezetékes” internetelérések jellemzően 2,4 és 5,8 GHz-es adatátviteli eszközökkel voltak bekötve a szolgáltatók hálózatába. A hálózatok és a felhasznált vezeték nélküli internet-eléréshez használt technológia elemzése során kiderült, hogy ezek az eszközök lényegesen magasabb késleltetést visznek a szolgáltatásba, mint a tisztán vezetékes és dedikált mikrohullámú eszközökön megvalósított megoldások. Egy-egy szakasz, átlagosan 30-40 ezredmásodpernyi késleltetése önmagában elfogadható a DMR-rendszer stabil üzeméhez, azonban a rendszer tervezett felépítéséből fakadóan (csillagtopológiával egy központi és négy tagállomás) a legtávolabbi állomások két szakasszal kapcsolódtak egymáshoz, ami együttesen és időszakosan a stabil működést meghaladó késleltetést hozott az IP-rendszerbe.

A probléma kezeléséhez megvizsgáltuk az elérhető vezetékes szolgáltatókat, ám eredménytelenül, mivel az érintett térségekbe és telephelyekre jellemzően a futó SZIP projekt keretein belül kerülnek optikai internet-eléréssel rendelkező vezetékes hálózatok. A telephelyek dedikált mikrohullámú összeköttetését a távolságok miatti többszörös átjátszás költségigénye és a megoldás kialakításának időbeni lefutása egyaránt megakadályozta.

A rendelkezésre álló publikus és zárt célú LTE-szolgáltatók megoldásait összehasonlítva megállapítottuk, hogy a csillagstruktúrát stabilan fenntartani ezen összeköttetésekkel sem lehet, így a rendszer átszervezésre került, páronként összekötött és három részre szétdarabolt alrendszerré. A bázisállomás-párokat a rendelkezésre álló IP-kapcsolatok redundáns felhasználásával kötöttük össze. A fő diszpécseri helyszín kedvező rádiófrekvenciás elhelyezkedése miatt mindhárom rész egy-egy bázisállomását közvetlenül elérhetővé tettük, így a megrendelő a szolgálati viszonyaihoz is igazodó bontással olyan megoldáshoz jutott, ami jelen körülmények között biztosítja a stabil üzemet.

A SZIP projektben megvalósulás alatt álló optikai hálózatok kialakítása és csatlakoztatása után könnyen és minimális költséggel átalakítható a rendszer annak érdekében, hogy az eredetileg tervezett funkcionalitás maradéktalanul megvalósuljon.

5. Összefoglalás

A fenti két gyakorlati példán alapuló tapasztalat segítséget nyújthat meglévő, analóg rendszerek modernizációjában előforduló nehézségek kezeléséhez. Ezek a nehézségek egyfelől az évtizedes megszokások kényszerű felhagyásának következményeiből fakadhatnak, mint például a beszédérthetőség és hangminőség változása az analóg és digitális jelfeldolgozás, kódolás hatásai miatt, másfelől a megrendelő és a térség gazdasági, alapinfrastrukturális sajátosságaiból gyökereznek.

Mindkét esetben szükség volt és lesz arra a mérnöki munkára, amellyel a prospektusokból és marketing anyagokból előre nem látható felhasználói problémákat kezelni lehet, a lehető legteljesebb módon szem előtt tartva az egymásnak némileg ellentmondó felhasználói igényeket.

Hivatkozások

[1] Dr. Gósy Mária: Fonetika, a beszéd tudománya, Budapest, Osiris Kiadó, 2004.
[2] Németh Géza, Zainkó Csaba, Bartalis Mátyás, Olaszy Gábor: Többnyelvű vasúti hangos utastájékoztatás korpusz alapú TTS módszerrel, In: Beszédkutatás, Vol. 23, 2015, pp.233–241.
[3] Christopher Redding, Nicholas DeMinco, Jeanne Lindner: “Voice Quality Assessment of Vocoders in Tandem Configuration” NTIA Report 31-386, Apr. 2001.
[4] Silage Dennis: Digital Communication Systems using SystemVue, DaVinci Engineering Press, a division of Cengage Publishing, 2006.

A szerzőről

TURCSÁN ZSOLT 1996-ban végzett a Budapesti Műszaki Egyetem Villamosmérnöki Karán, okleveles villamosmérnökként. Rádiós adatátviteli modemek fejlesztése után a NOVOFER Távközlési Innovációs Zrt-nél helyezkedett el, mint tervező, projektvezető. Munkája során több készülék- és rendszer-generáción átívelve tervezett, épített és korszerűsített több megyére kiterjedő, illetve országos keskenysávú beszéd- és adatátviteli rádiós rendszereket analóg, digitális DMR-, NXDN- és TETRA-technológiákkal. Jelenleg a NOVOFER Zrt. vezérigazgatója, tervezője, felelős műszaki vezetője, a HTE tagja.

A torony-infrastruktúra stratégiai szerepe a távközlési piacokon

DÓBÉ SÁNDOR, RÓZSÁS TITANILLA
Antenna Hungária Zrt.
dobe.sandor@gmail.com, rozsast@ahrt.hu

Kulcsszavak: toronycég, MNO, torony, infrastruktúra

A mobilszolgáltatók számára a toronyinfrastruktúra birtoklásának stratégiai jelentősége fokozatosan csökken, ezzel párhuzamosan a hálózat-megosztási hajlandóság nő. Költséghatékonysági megfontolásból egyre több MNO dönt úgy, hogy megválik torony-portfóliójától és a tornyok üzemeltetésére specializálódott toronycégek kezébe adják infrastruktúrájukat. Az 5G-hálózatépítésekhez közeledve a toronycégek jelentősége még inkább felértékelődhet.

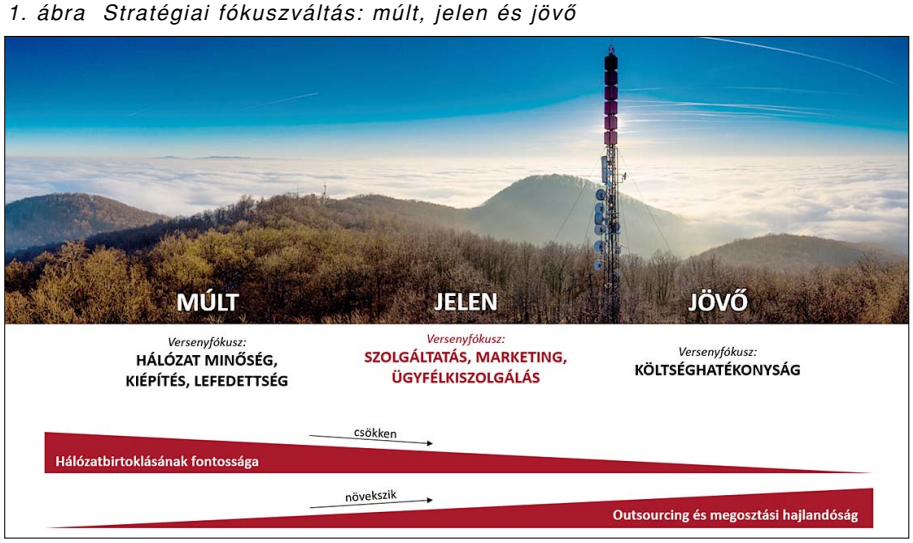
1. Bevezetés

Pár évvel ezelőtt a mobilszolgáltatók kommunikációjukban az ár mellett a hálózat minőségét, a kiterjedt lefedettséget hangsúlyozták. A 90-es években a verseny fókusza a minél nagyobb lefedettségű hálózat kiépítésére összpontosult; a mobiltelefónia kezdeti éveiben a szolgáltatók egymástól függetlenül és egymással versenyezve építették országos hálózatukat, hogy megelőzzék egymást lefedettség tekintetében. A saját hálózat és torony stratégiai jelentőségű eszköz volt, ami a versenyelőny kulcsát jelentette, és egyben azzal is járt, hogy egymással párhuzamos infrastruktúrák épültek ki.

2. Változó stratégiai fókusz

A 2000-es évek közepére a saját hálózathoz való ragaszkodás fokozatosan változni kezdett, új szemléletet hozva a piacra. Napjainkban sokkal inkább jellemzi a szolgáltatókat, hogy a hálózatépítéseket és az egyre növekvő beruházási költségeket próbálják optimalizálni.

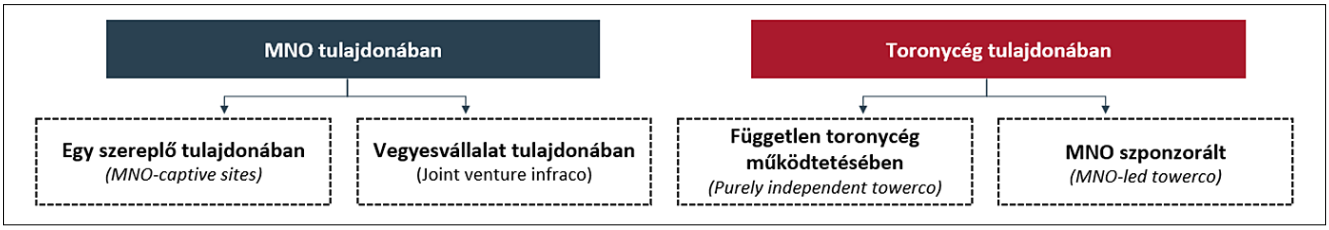
1. ábra Stratégiai fókuszváltás: múlt, jelen és jövő



A lefedettség továbbra is fontos maradt, ugyanakkor jelentős differenciálási lehetőséget már nem rejt magában, hiszen a szolgáltatók lefedettsége nagyon hasonló, közel száz százalékos. A mobiltelefónia korai időszakához képest a hálózat birtoklásának stratégiai jelentősége csökkenni kezdett. Ezt bizonyítják az MNO-k közötti megállapodások, amelyek egészen odáig vezettek, hogy a Magyar Telekom és a Telenor gyakorlatilag közösen, frekvencia-megosztásban építette ki 4G-hálózatuk egy részét. De nem ez volt az egyetlen jele a változásnak: 2010-ben az egyik MNO külföldi anyacége kezdeményezésére komolyan megfontolta a teljes hazai telephely infrastruktúrájának eladását az Antenna Hungáriának.

Napjainkra a hálózat birtoklásának stratégiai jelentősége tehát lecsökkent, ezzel együtt a verseny fókusza más irányba terelődött: a szolgáltatások, az ügyfélkiszolgálás és a marketing területére *(1. ábra)*. Az árban és értékben egymásra licitáló ajánlatok és a „tiszta vásári marketing” mellett jellemző a szolgáltatás-portfólió teljességére való törekvés, vagy más szóval a konvergencia. A Telenor OTT-ben próbál TV-szolgáltatást indítani, a Vodafone pedig a UPC akvizíciójával kerekíti ki a portfólióját.

És hogy mit hoz a jövő? Ha a szolgáltatások terén már nem lehet megkülönböztető versenyt folytatni, akkor a mobilpiaci termékek gyakorlatilag homogén árucikké válnak a fogyasztók számára, és az a szolgáltató tud sikeres lenni, amelyik a legköltséghatékonyabban tudja üzemeltetni az üzletét. Ahogy a szolgáltatásokra és még inkább a költséghatékonyságra terelődik a hangsúly, úgy a tornyok kiszervezésére való hajlandóság világszerte növekszik, ezzel pedig a távközlési toronyportfóliók jelentős része átkerül a toronycégek kezébe.



2. ábra A tornyok tulajdonlási formái
Forrás: Global Data (2017), Wireless Tower Market in Europe

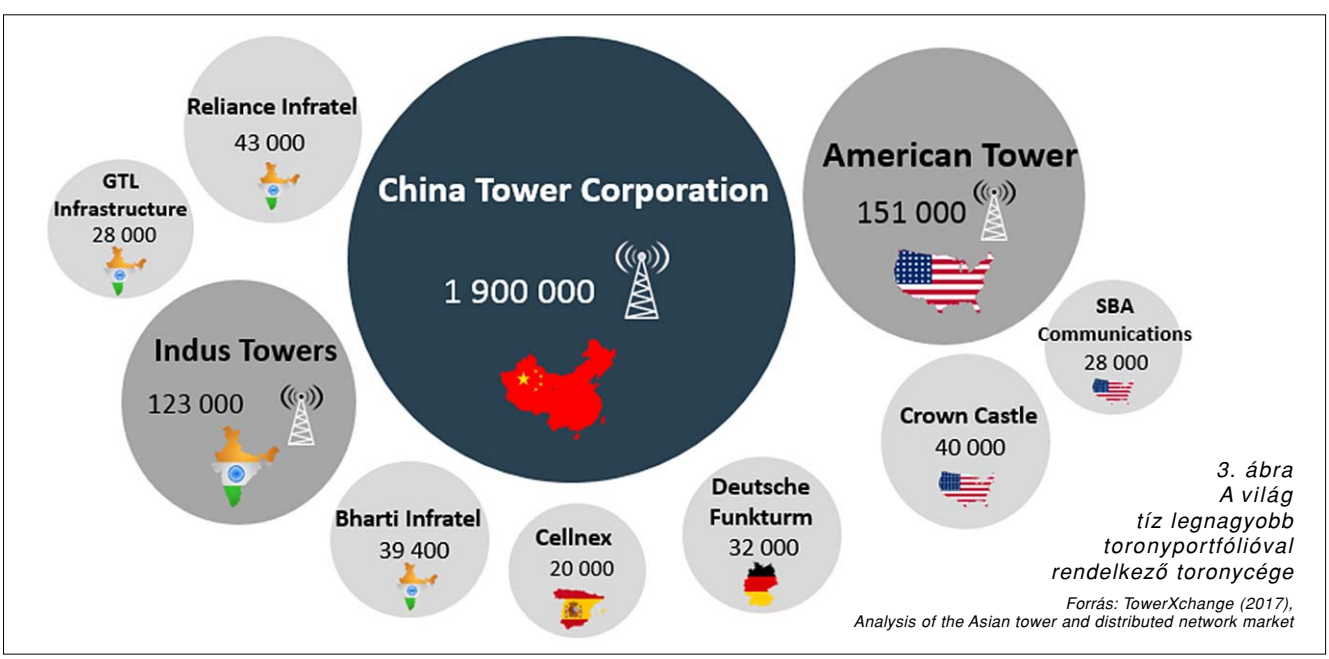
3. A toronycégek növekvő népszerűsége

A mobil operátorok számára a költséghatékonyságon túl a kiszervezés mellett szól a vállalatértékelési különbség előnye és a befektetői kedv. Míg az MNO-kat négy-, hatszoros EBITDA-szorzón értékelik, addig egy toronycégért akár 12-17, sőt 20-szoros EBITDA-szorzót is megadnak, melyek a stabil és kiszámítható cash flow miatt igen vonzó befektetési célpontokká váltak világszerte. Ez pedig erősen motiválja az MNO-kat arra, hogy leválasszák a cégről tornyaikat és kisebbségi tulajdonosként monetizálják azokat, vagy jó pénzért közvetlenül eladják a tornyaikat egy független toronycégnek.

A távközlési tornyok a tulajdonlási formák tekintetében alapvetően két típusra oszthatóak annak függvényében, hogy MNO-k vagy toronycégek birtokolják az infrastruktúrát. Mindkét esetben két altípus különböztethető meg *(2. ábra)*. Az előbbi kategóriában a torony lehet kizárólag egy MNO tulajdonában, ha a mobilszolgáltatók maguk építik és tartják fenn saját tornyukat, megtartva a kizárólagos kontrollt az eszközök felett, vagy lehet több MNO által közösen létrehozott vegyesvállalat tulajdonában, amelyek így közösen felelnek az építésért, fenntartásért és működtetésért, miközben termék-, marketing- és egyéb stratégiáikat függetlenül tartják egymástól. A toronycégek általi infrastruktúra-birtoklást megkülönböztethetjük aszerint, hogy a torony egy valódi független toronycég, vagy egy MNO-szponzorált cég kezében van-e. Utóbbi esetben egy mobilszolgáltató a domináns többségi tulajdonos vagy jelentős részvényes a toronytársaságban [1].

Az elmúlt években a stratégiai fókuszváltás a telco infrastruktúra birtoklását tekintve a toronycégek felemelkedését hozta magával. Becslések szerint jelenleg a világ 3,5 millió műsorszóró és távközlési tornyainak 66 százalékát toronycégek tulajdonolják. Számunkra Európában ez a statisztika megdöbbentő lehet, hiszen a globális átlaghoz viszonyítva ugyanezen statisztika nálunk mindössze 30 százalék körül alakul [2].

A világ számos részén – például Észak-Amerikában, Indiában valamint Kínában – már egy érett toronypiacról és több tízezer tornyot számláló toronyportfólióval rendelkező toronycégekről beszélhetünk. A kínai piac kiemelkedik a sorból 100 százalékos penetrációjával, köszönhetően Kína egyetlen, mobilszolgáltatók által tulajdonolt toronycégének. A China Tower Corporation közel 2 millió tornyot számláló toronyportfóliója ugyan ráfogható a kínai gazdaságpolitika irányított természetére, ám a világ második legnagyobb toronycége, a teljesen liberalizált piacon működő American Tower Corporation is csak körülbelül 150 ezer, és az őt követő indiai Indus Towers is „mindössze” mintegy 120 ezer tornyot kezel [3] *(3. ábra)*. Ezen számok pedig akkor lesznek még inkább lenyűgözőek, ha Magyarországot vesszük összehasonlítási alapként, hazánk körülbelül 2500 távközlési tornyával.



3. ábra A világ tíz legnagyobb toronyportfólióval rendelkező toronycége
Forrás: TowerXchange (2017), Analysis of the Asian tower and distributed network market

Bár az európai penetráció jelenleg még elmarad a globális átlagtól, de az előrejelzések szerint a következő években az MNO-któl független toronycégek működtetésében álló tornyok száma jelentős növekedésnek indulhat a mi kontinensünkön is, és 2020-ra arányuk elérheti a 34 százalékot. Egyes európai országokban a független toronycégek piaci részesedése már most is túlszárnyalja ezt az előrejelzést; a legérettebb európai piac Csehország a maga 60 százalékos penetrációjával [2], ahol 2015-ben a magyar Telenor jelenlegi tulajdonosa, a PPF Csoport az O2-ből kivette a tornyokat és a Cetin nevű vállalat üzemeltetése alá helyezte [4].

A legnagyobb toronyportfóliót számláló toronycégek top10-es listájába a kínai China Tower mellé három az Egyesült Államokból, négy pedig az indiai piacról kerül ki. Európát képviselő, a top10-ben is megtalálható két legnagyobb cég – a maga 30 ezer tornyot meghaladó infrastruktúrájával – a Deutsche Funkturm, illetve a Cellnex. A kontinensünk legnagyobb, kizárólag Németország területén működő toronycége 2002-ben a Deutsche Telekom leányvállalataként jött létre azzal a céllal, hogy a legnagyobb német mobil operátor tornyait üzemeltesse. Ezzel a lépéssel a DT egyfajta divatot teremtett a nagy európai MNO-k körében; a Deutsche Funktrurm mellett az MNO-k által kiszervezett és irányított cégekre jó példa még a Telefónica toronycége, a Telxius vagy a Telekom Italia toronycége, az INWIT [2].

Míg a Deutsche Funkturm MNO-szponzorált cég, addig Európa második legnagyobb toronycége, a spanyol székhelyű Cellnex több európai piacon is megtalálható, független vállalat. Spanyolország mellett jelen van Hollandiában, az Egyesült Királyságban, Svájcban, Olaszországban és Franciaországban is. A Cellnex az utóbbi években több európai toronycégben szerzett tulajdonosi részesedést, továbbá átvette néhány mobilszolgáltató infrastruktúráját. 2017 februárjában a francia Bouygues Telecom 3000 tornya, 2017 szeptemberében pedig a holland Alticom 30 tornya került a Cellnex portfóliójába [5].

Míg Európában maximum ezres nagyságrendű felvásárlásokról beszélhetünk, addig a tengerentúlon egy-egy tranzakció keretében több tízezer távközlési torony cserél gazdát. Az Észak-Amerika második legnagyobb toronyportfóliójával rendelkező Crown Castle két év leforgása alatt két nagy értékű, mintegy 17 ezer toronyra kiterjedő megállapodást kötött MNO partnereivel, az AT&T-vel, valamint a T-Mobile-lal [6]. A T-Mobile főként 4G-hálózatának fejlesztését támogatta a befolyó pénzből, míg az AT&T a pénzügyi mozgásterét javítva, több felvásárlást is végrehajtott az adott időszakban.

A fenti tranzakcióra válaszul 2015-ben a Verizon is átadta több mint 11 ezer tornyának üzemeltetési jogát a Crown Castle fő versenytársának, az American Towernek. Ezzel az MNO tornyainak többsége az American Towerhez került [7].

4. ábra
Adott környezetbe illő, álcázott multifunkcionális tornyok

Forrás: www.calzavara.it

A fenti tranzakciókhoz és a legnagyobb toronyportfólióval rendelkező toronycégekhez viszonyítva a magyarországi toronypiac kicsinek tekinthető. Összesen körülbelül 2500 torony található Magyarországon, amelyek 90 százaléka mobilszolgáltatók tulajdonában van. Hazánk egyetlen nagyobb – mobilszolgáltatóktól független, de állami tulajdonban levő – távközlési infrastruktúra cége az Antenna Hungária, amelynek a tornyok méretét és földrajzi elhelyezkedését tekintve kiemelt telephelyei vannak, azonban számosságban elmarad a hazai mobilszolgáltatók toronyinfrastruktúrájától.

Magyarországon a jelenlegi generáció mobilhálózatai nagyjából kiépültek és általánosságban elmondható, hogy nincs szükség a tornyok számának jelentősebb bővítésre. Az építések a 2008-as válság hatására teljesen leálltak egy időre, majd az elmúlt pár évben valamelyest újra beindultak, azonban a 4G-s fejlesztések nem hozták el a várt növekedést (a korábbi tervek szerint több mint száz új torony épült volna).

Napjaink kiemelt témája, az 5G kapcsán ismét középpontba kerül a hálózatépítés: ki, illetve kik fogják építeni, milyen finanszírozási konstrukcióban, hogy fog kinézni az engedélyeztetés stb... Mindez különösen fontos, hiszen az 5G esetében nem a hagyományos telco tornyok fogják a központi szerepet játszani. A 700 MHz és 3,5 GHz frekvenciák mellett az 5G-re kijelölt 26 GHz-es spektrum nagyon nagy sávszélességű, ugyanakkor rendkívül sűrű városi hálózatokat feltételez, melyhez új, városi környezetben elhelyezendő telephelyekre lesz szükség. A várható hálózatkiépítés óriási beruházásigénye és a párhuzamos hálózatok esztétikai hátrányai miatt érdemes fontolóra venni egy független infrastruktúra szolgáltató által épített, közös, „közmű-szerű” 5G-hálózat megtervezését.

A lakossági averzió és a rövid távon felmutatható előnyök hiánya miatt az 5G esetén különösen fontos lesz, hogy a városi környezetbe jól illeszthető telephelyeket lehessen majd kialakítani. Egyes cégek, többek között az olasz Calzavara új, innovatív és esztétikus tornyok kivitelezésére specializálódott a telekommunikációs szektor számára és álcázott, az adott környezetbe jól illeszkedő bázisállomások tervezését-megvalósítását biztosítja ügyfeleinek. Városi bútornak álcázott torony lehet közlekedési tábla, buszmegálló, hirdetési felület vagy utcai lámpa is. A *4. ábrán* néhány érdekes példa látható a különféle megoldásokra [8].

4. Összefoglalás

Az MNO-k stratégiai fókuszának változása a hálózatbirtoklás jelentőségének csökkenését, ezzel együtt az infrastruktúra-kiszervezés és hálózat-megosztási hajlandóság növekedését hozta magával.

A cikkben a magyar telefónián keresztül bemutattuk a stratégiai fókuszváltás lényegét, majd ismertettük az új irány nyomán megerősödött toronypiacot, annak legnagyobb globális és európai szereplőit, illetve az elmúlt évek néhány kiemelt tranzakcióját. Kitértünk az európai toronypiachoz képest alacsony toronypenetrációval rendelkező magyar piacra, amelynek kapcsán említést tettünk a jövőbeni 5G-hálózatépítésnek egy lehetséges, független infrastruktúracég általi megépítéséről, hangsúlyt helyezve a kivitelezés esztétikai szempontjaira.

Hivatkozások

[1] Global Data (2017): Wireless Tower Market in Europe.
[2] ToweXchange (2017): Europe Dossier.
[3] TowerXchange (2017): TowerXchange's analysis of the Asian tower and distributed network market.
[4] www.ppf.eu
https://www.ppf.eu/en/case-studies/telefonica-o2-czech-republic-and-its-uniquevoluntary-division
[5] www.cellnextelecom.eu
https://www.cellnextelecom.com/en/who-we-are/
[6] www.crowncastle.com
http://investor.crowncastle.com/news-releases/news-release-details/crown-castle-and-t-mobile-usa-announce-24-billion-tower
[7] www.fiercewireless.com
https://www.fiercewireless.com/wireless/verizon-offloads-towers-to-american-tower-for-5b
[8] www.calzavara.it

Szerzőinkről

DÓBÉ SÁNDOR diplomáját a Budapesti Corvinus Egyetem befektetés-elemző és kockázatkezelő szakán szerezte. Távközlési és média stratégiai menedzser, 2018-ig az Antenna Hungária stratégiai és üzletfejlesztési ágazatát vezető igazgató, ezt megelőzően ugyanitt a Stratégiai osztály vezetője, illetve vezető szakértője volt. Kompetenciái közé tartozik a távközlési és médiapiaci stratégiai irányok meghatározása, valamint kiemelt üzletfejlesztési és akvizíciós projektek teljes körű menedzselése. Korábban stratégiai tanácsadóként tevékenykedett, 2003 és 2005 között az Accenture kötelékében számos projektben vett részt változatos iparágakban, majd ezt követően független tanácsadóként, főként távközlési cégeknél dolgozott.

RÓZSÁS TITANILLA alapdiplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerezte, majd 2014-2016 között elvégezte a Budapesti Corvinus Egyetem Vállalkozásfejlesztés mesterszakát. Stratégiai elemző az Antenna Hungáriánál, főbb feladata a stratégiai projektek támogatása és piacelemzések készítése.

Kiberbiztonság a negyedik ipari forradalom korában

KRASZNAY CSABA
Nemzeti Közszolgálati Egyetem
krasznay.csaba@uni-nke.hu

Kulcsszavak: Ipar 4.0, IoT, kiberbiztonság, NISD, GDPR, Ibtv., Cybersecurity Act, kiberfizikai rendszerek

A negyedik ipari forradalom alapvető építőkövei kétségkívül a hálózatba kapcsolt digitális eszközök, melyek milliárdszámra jelentek meg az elmúlt években. Az okos városok, okos otthonok és okos gyártás elterjedésével számuk bizonyosan exponenciálisan fog növekedni a következő évtizedben. Biztonságos működésük éppen ezért alapvető követelmény mind gazdaságunk, mind társadalmunk szempontjából. A „biztonság" kifejezés azonban a tervezők fejében leginkább a „safety", azaz üzembiztonság értelemben jelenik meg, melyre természetszerűen komoly erőforrásokat fordítanak. A „cybersecurity", azaz kiberbiztonság megvalósítása viszont az Ipar 4.0 területén inkább kérdéseket vet fel egyelőre, tekintettel arra, hogy sokkal kevesebb tapasztalat áll rendelkezésre a komplex ipari rendszerek, azaz a kiberfizikai rendszerek informatikai szempontú védelmével kapcsolatban, mint a hagyományos, fizikai térben történő fenyegetések kezelésében. Jelen tanulmány áttekinti azokat az európai és hazai stratégiákat és jogszabályokat, melyek célja a kiberbiztonság megerősítése, egyben rámutat, milyen szabályozói eszközök állnak rendelkezésre a negyedik ipari forradalom szereplőinek támogatására és kontrollálására.

1. Bevezetés

Az átlagos hírfogyasztó ma már nem nagyon tudja úgy megnyitni kedvenc hírportáljának kezdőoldalát, hogy azon ne lenne híradás valamilyen komoly kiberbiztonsági incidensről. Folyamatosan olvashatunk országok elleni kibertámadásokról, százmilliókat érintő adatszivárgásokról vagy éppen olyan egzotikusnak tűnő információs rendszerek manipulálásáról, mint egy erőművi rendszer ipari irányítástechnikája. 2017 márciusában azonban a Wikileaks által közzétett, az amerikai hírszerző ügynökségtől, a CIA-tól származó kiszivárgott anyagokból az is kiderült, hogy akár az okostévék vagy személygépjárművek informatikai rendszerei ellen is léteznek sikeres támadási technikák [1]. Tekintettel arra, hogy az egyik az okos otthonok, a másik az okos városok tipikus eszköze, felmerül a kérdés, mennyire lehetnek informatikai értelemben biztonságosak az úgynevezett Internet of Things (IoT), azaz Dolgok Internetét alkotó megoldások? Tágabban értelmezve, megvalósítható-e a Dolgok Internetére épülő negyedik ipari forradalom olyan eszközökkel, melyek támadhatók és megfelelő erőforrásokkal rendelkező entitások sikerrel is támadják azokat?

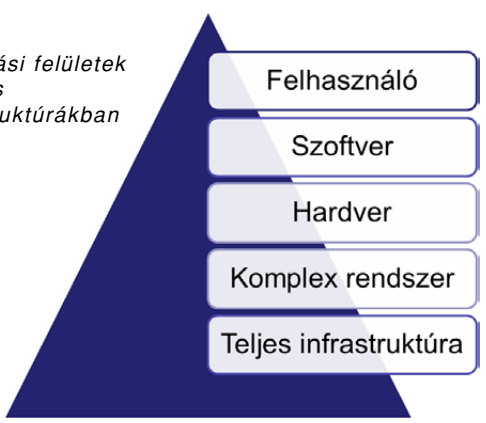
Az információbiztonsági szakértők körében az IoT rövidítés közkeletű feloldása az Internet of Threats, azaz a Fenyegetések Internete, utalva arra, hogy a szakértői közösségnek komoly aggályai vannak mind az egyes eszközök, mind pedig az ezekből felépülő ökoszisztéma védelmi szintjével kapcsolatban. Az elmúlt évek kibertámadásainak köszönhetően ebben a félelemben ma már a stratégiai védelemmel foglalkozó szakemberek is osztoznak, így egyre több ország nemzeti biztonsági és kiberbiztonsági stratégiája említi a kibertéri fenyegetéseket kiemelt nemzetbiztonsági problémának. A kockázatok enyhítése céljából pedig folyamatosan jelennek meg azok a szabályozók, melyek kötelezik az okos infrastruktúrák építőit és üzemeltetőit bizonyos informatikai védelmi intézkedések megtételére.

2. Ipari rendszereket érintő fenyegetések

Mérnöki nézőpontból hajlamosak vagyunk arra koncentrálni, hogy az egyes rendszerelemek biztonságát vizsgáljuk, nem véve figyelembe, hogy az adott rendszerelem egy komplex rendszer részeként működik, melyet emberek üzemeltetnek. Így bár egyes modulokat lehet, hogy a rendelkezésre álló legátfogóbb információbiztonsági szemlélettel valósították meg, azonban a teljes ellátási lánc valamelyik elemének gyengesége aláásható az egyes részegységek nyújtotta megfelelő védelmi szintet.

Az *1. ábra* bemutatja, milyen támadási felületek mutatkoznak egy komplex kiberfizikai rendszer esetén.

1. ábra
Támadási felületek az okos infrastruktúrákban



Vegyük példaként az okos közlekedést, és vizsgáljuk meg, mit jelent az ábrán vázolt támadási felület egy autonóm, önvezető gépjármű szempontjából! A hardver az egyes szenzorokat, beavatkozóegységeket jelenti, melyek tömegével találhatók meg az autóban. Ezek hálózatokon keresztül juttatnak el adatot a gépjármű központi számítógépéhez, mely az adatokból a szoftver segítségével információkat állít elő, ezzel irányítva a személygépjárművet, mint komplex rendszert. Ez a komplex rendszer azonban egy okos közlekedési infrastruktúra esetén folyamatosan kommunikál az őt körülvevő környezettel, így a közlekedés-irányító infrastruktúrával és a többi autóval, melyek a teljes rendszert alkotják. Ebben az infrastruktúrában pedig jelen vannak az emberek, mint sofőrök vagy mint rendszerüzemeltetők.

Ennyire komplex ökoszisztémában kiberbiztonsági szempontból hibátlan rendszert megvalósítani szinte lehetetlen. Sokszor már az egyes rendszerelemek is tartalmaznak olyan sebezhetőségeket, melyeket a megfelelő motivációval és szakértelemmel rendelkező támadó ki tud használni és ezzel a teljes rendszert nem tervezett működésre tudja bírni. Az ipari irányítástechnikai rendszerek fejlesztői gyakran hivatkoznak arra, hogy rendszereik zárt környezetben működnek és speciális szakértelem szükségeltetik azok megismeréséhez. Ehhez képest az amerikai kritikus információs infrastruktúrák incidenskezeléséért felelős ICS-CERT szervezet statisztikái alapján évről évre egyre több olyan sebezhetőség kerül napvilágra, mely a speciális kiberfizikai rendszerelemek szoftvereinek hibáit tárja fel, ahogy az a *2. ábrán* is látható.

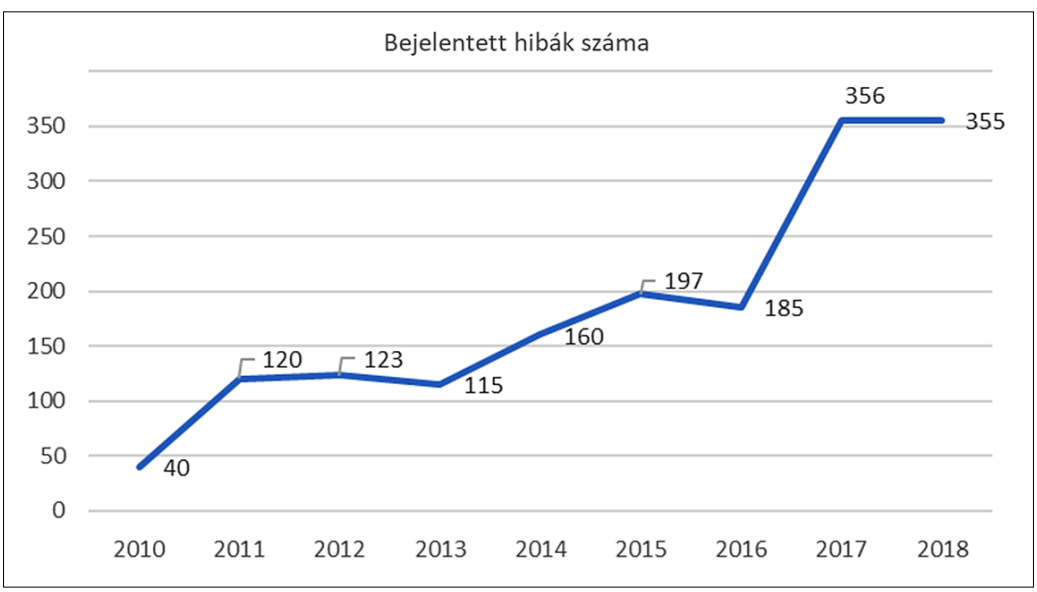
Nincs okunk kételkedni abban, hogy a negyedik ipari forradalom kiberfizikai eszközeit egyre inkább a biztonságos szoftverfejlesztés elveit felhasználva fogják létrehozni, ám ezek számosságuk és hálózati kapcsolatuk miatt könnyebben elérhetők lesznek, így feltételezzük, hogy a bennük felfedezett hibák száma az évek során monoton növekedni fog, hasonlóan az ipari irányítási rendszerekhez.

De ki kell emelni az emberi tényező fontosságát is! Bányász Péter az ellátási láncok kiberbiztonságáról szóló művében a következőket példát említi: *„Tegyük fel, a külső támadás lehetetlenné vált, olyan mértékű védelmet valósítottak meg. Ilyen esetben van szerepe a social engineeringnek, hiszen, maradva a hipotetikus példánál, a kikötő takarítószemélyzetéből egy dolgozó megzsarolásával/megtévesztésével a támadók elérhetik, hogy a takarító az informatikai eszközökhöz hozzáférést biztosítson egy pendrive számítógépbe történő helyezésével, amivel a támadók olyan hátsó kapukat nyithatnak, amellyel átvehetik az irányítást az eszköz felett."* [3] A napvilágra került, kritikus infrastruktúrákat érintő támadások során szinte minden esetben sejthető, hogy szándékos vagy gondatlan emberi tevékenység nélkül a támadás kivitelezése lényegesen nehezebb vagy egyenesen lehetetlen lett volna.

A támadási felületek közül nem került megemlítésre a hardver, a komplex rendszer és a teljes infrastruktúra. Nem véletlenül. Ezek esetében ugyanis hiányoznak azok a megbízható statisztikák, adatforrások, melyekkel szemléltetni lehet a kitettségüket. A hardverek esetében például tudjuk, hogy tervezési sajátosságok miatt számos CPU elméletileg lehetőséget biztosít a számítógépen feldolgozott bizalmas adatokhoz való hozzáféréshez (lásd a Spectre és Meltdown hibákat), de csak elképzeléseink lehetnek arról, hogy ezek valójában mekkora kockázatot jelentenek. De a kínai távközlési gyártók angolszász országokból való távoltartásának szándéka is mutatja, milyen nemzetbiztonsági kihívást érzékelnek a stratégiai védelemért felelős vezetők abban, ha az 5G távközlési rendszerek infrastruktúráját ellenérdekelt országok gyártói szállítják.

3. Kiberbiztonság az Európai Unióban

Belátható, hogy a támadási felületek csökkentése, pusztán a mérnökök eszköztárával csak tyúklépésekben lenne megvalósítható, a veszély viszont reális és azonnali, széles körű cselekvést kíván. Be kell tehát vonni azokat a közpolitikai és diplomáciai eszközöket, melyek egy-



2. ábra
Az ICS-CERT-hez bejelentett SCADA/ICS sebezhetőségek száma éves bontásban.

Forrás:
ICS-CERT Annual Vulnerability Coordination Report [2]

részt a támadók motivációját törik le, másrészt rendszerszinten várnak el cselekvést az Ipar 4.0 szereplőitől. Fogalmi szinten ez azt jelenti, hogy az egyes rendszerelemeket érintő információbiztonság mellett az ennél szélesebb körű kiberbiztonság megvalósítása is kívánatos.

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról jól mutatja a két fogalom közötti különbséget. Eszerint az 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", míg a kiberbiztonság „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez" [4].

Hasonló következtetésekre jutottak az Európai Unió döntéshozói is. Szükséges az információbiztonság erősítése termék- és szervezeti szinten, de támogatni kell a kiberbiztonsággal kapcsolatos lépéseket is. Ennek érdekében az elmúlt években számos olyan szabályozás született, illetve lett előkészítve, melyeket minden EU-tagországnak kötelező honosítani. Az Európai Unió kiberbiztonsági reformról szóló összefoglalójában az alábbi területeket emeli ki, utalva a Kiberbiztonsági Jogszabály, vagyis a Cybersecurity Act által lefedett területekre:

• **Kiberbiztonsági tanúsítási rendszer:** Az Európai Bizottság a 2017. szeptemberi reformcsomagban javaslatot tett az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése. E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Szerepük az lenne, hogy csökkentsék a piac széttagoltságát és felszámolják a szabályozási akadályokat, továbbá segítsék a bizalomépítést is. A rendszereket valamennyi tagállam elismerné, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

• **Az uniós kiberbiztonsági ügynökség megerősítése:** A Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy erősebb uniós kiberbiztonsági ügynökség. Az új ügynökségnek az lenne a feladata, hogy segítséget nyújtson a tagállamok, az uniós intézmények és a vállalkozások számára a kibertámadások kezelésében.

• **A kompetenciatámogatástól a csalás elleni küzdelemig:** Az Európai Bizottságnak az uniós kiberbiztonság megerősítését célzó javaslata további kezdeményezéseket is tartalmaz:

– A nagy kiterjedésű kibertámadásokra adandó válaszlépéseket meghatározó terv.
– Európai Kiberbiztonsági Kutatási és Kompetenciaközpont, kiegészülve a hasonló központok tagállami szintű hálózatával.
– Hatékonyabb büntetőjogi fellépés a kiberbűnözéssel szemben a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló új irányelv révén.
– A globális stabilitás erősítése nemzetközi együttműködés útján [5].

Fontosak tehát mind az információbiztonsági, mind a kiberbiztonsági szempontú tevékenységek. Első lépésben az Európai Unió két olyan szabályozást alkotott, melyek komoly hatással vannak a nemzeti jogrendre is és az Ipar 4.0 szereplőinek is érdemben figyelembe kell ezeket vennie. Ezek egyrészt az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, közkeletű nevén a GDPR), másrészt az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, azaz az NIS Direktíva.

Míg a GDPR célja a személyes adatok védelmének biztosítása, akár olyan környezetben is, ahol nagy mennyiségű adat keletkezik, tehát tipikusan egy IoT-rendszerekből álló okoskörnyezetben, az NIS Direktíva kijelöli azokat a kritikus információs infrastruktúrákat, melyek védelme európai szinten kiemelten fontos, amilyenek például az olyan digitális infrastruktúra szolgáltatók, mint az Internet Exchange Point-ok, DNS-szolgáltatók vagy legfelső szintű doménnév-nyilvántartók (TLD). A közlekedési infrastruktúra tekintetében a 2010/40/EU európai parlamenti és tanácsi irányelv 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetőit nevesíti a Direktíva, mely a meghatározás szerint *„olyan rendszerek, amelyekben információs és kommunikációs technológiákat alkalmaznak a közúti közlekedés területén, beleértve az infrastruktúrát, a járműveket és a felhasználókat is, a forgalomirányításban és a mobilitás kezelésében, valamint a más közlekedési módokhoz való kapcsolódási pontok vonatkozásában"* [6].

Ha ezekhez hozzávesszük a Kiberbiztonsági Jogszabályt is, egyértelműen kirajzolódik az Európai Unió törekvése. Olyan termékek és szolgáltatások kialakítását szeretnék ösztönözni innovációs és regulációs eszközökkel az európai piacon, különösen a kritikus információs infrastruktúrát alkotó kiberfizikai rendszerek esetében, melyek egyszerre veszik figyelembe az adatvédelmi és kiberbiztonsági szempontokat. Tekintettel arra, hogy a negyedik ipari forradalom infrastruktúrája és szolgáltatásai éppen kialakulófélben vannak, az európai okosinfrastruktúrában érintett szereplőknek ezt a politikai szándékot mindenképpen érdemes figyelembe venni!

4. A magyar kibervédelmi szabályozás változása

Természetesen a hivatkozott európai szabályozások mélyen érintik a magyar jogrendet is. 2018 folyamán a GDPR végrehajtásához szükséges részletszabályozásokkal módosult a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.), az NIS Direktíva miatt pedig pontosításra került a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), és a 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ektv.) is. A 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól pedig tovább centralizálta a hazai intézményrendszert, kiemelt szerepet adva a Nemzeti Kibervédelmi Intézetnek.

Jelen cikk szempontjából azonban a legfontosabb új jogszabály a *1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról,* ugyanis ez részletezi, hogy hazánk milyen stratégiai lépéseket kíván tenni az NIS Direktíva és általánosságban az európai kiberbiztonsági stratégia végrehajtása érdekében. Mindezt oly módon teszi, hogy ágazati stratégiaként illeszkedik a továbbra is hatályban maradó korábbi, 1139/2013. (III. 21.) Korm. határozathoz, mely Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szól. Az új stratégia főbb területeit a *3. ábra* foglalja össze.

Sajnálatos módon az új magyar stratégia explicit módon nem foglalkozik a negyedik ipari forradalom jelentette technológiai változásokkal, kiolvasható belőle viszont az a szándék, hogy Magyarország részese legyen az Európai Unió kezdeményezéseinek.

A Kiberbiztonsági Jogszabály tervezete így fogalmaz: *„Az új technológiák, például a mesterséges intelligencia, a dolgok internete, a nagy teljesítményű számítástechnika, a kvantum-számítástechnika, a blokklánc és a biztonságos digitális személyazonosításhoz hasonló koncepciók nem csupán új kihívásokat támasztanak, de megoldásokat is kínálnak a kiberbiztonság területén. A meglévő és jövőbeni IKT-rendszerek ellenálló képességének felméréséhez és igazolásához szükséges lesz, hogy a biztonsági megoldásokat nagy teljesítményű és kvantumszámítógépekről levezényelt támadásokkal szemben teszteljék. A kompetenciaközpont, a hálózat és a kiberbiztonsági kompetenciaközösség feladata az is, hogy segítséget nyújtson a legújabb kiberbiztonsági megoldások kifejlesztéséhez és elterjesztéséhez. Emellett fontos, hogy a kompetenciaközpont és a hálózat a létfontosságú szektorokban (pl. közlekedés, energetika, egészségügy, pénzügy, kormányzat, telekommunikáció, gyártás, védelem és űrkutatás) tevékenykedő fejlesztők és szolgáltatók rendelkezésére álljon, és segítse őket a kiberbiztonsági kihívások leküzdésében."* [7]

Magyarország ehhez egyrészt a hazai innováció támogatásával, másrészt a kritikus információs infrastruktúra védelmével kíván csatlakozni. A hálózati és információs rendszerek biztonságáról szóló stratégia a következő intézkedéseket tűzi ki a kibervédelmi intézményrendszer számára:

- 33.) legyenek szabadon hozzáférhetők ágazatközi, illetve ágazat-specifikus konszenzust képviselő ajánlások és jó gyakorlatok a biztonsági célok elérésére vonatkozóan;
- 35.) álljon a kritikus infrastruktúrák üzemeltetőinek minél szélesebb köre rendelkezésére a védelmet kiegészíteni képes egységes szolgáltatáscsomag;
- 36.) a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség

3. ábra A hálózati és információs rendszerek biztonságáról szóló stratégia főbb területei

fejlesztésére célzott pályázati lehetőségek biztosítása szükséges az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére;

- 45.) létre kell hozni egy kiberbiztonsági szakterületet érintő kutatási stratégiát, melynek célja – a magyar intézményrendszer kiberbiztonságának erősítése érdekében – a magyar fejlesztésű kiberbiztonsági eszközök, szoftverek és termékek alkalmazásának fokozása;
- 46.) kerüljenek azonosításra a kapcsolódó kutatás-fejlesztési témakörök, továbbá kerüljenek megteremtésre az állami ösztönzési lehetőségek, beleértve a magyar korai fázisú vállalkozások ösztönzését is;
- 47.) a 45. pontban leírt kiberbiztonsági kutatás-fejlesztési-innovációs stratégia kiemelten kezelje az Európai Unió 2021-2027 között meghirdetésre kerülő K+F+I felhívásainak témáit, ezzel segítve az innovatív magyar szervezeteket abban, hogy a kiemelten tudjanak részt venni a nemzetközi projektekben. [8]

5. Összefoglalás

A negyedik ipari forradalom elengedhetetlen előfeltétele a (kiber)biztonságosan működő digitális infrastruktúra létrehozása. Ez azonban nem csupán műszaki feladat, a digitális ökoszisztéma minden szereplőjének, így az államoknak is komoly feladatai és felelősségei vannak a kibertéri fenyegetések kezelésében. Mivel az Ipar 4.0-át érintő fejlesztésekben az amerikai és kínai vállalatok jelentős előnyre tettek szert az európai versenytársakkal szemben, nem utolsósorban a célzott állami beavatkozásnak köszönhetően, az Európai Unió elemi érdeke olyan környezet létrehozása, mellyel az európai vállalkozások is versenyben tudnak maradni és az európai gazdaságok képesek lehetnek csökkenteni a tengerentúli digitális megoldásoktól való függőségeiket, ezzel pedig az államilag támogatott kibertámadásokkal szembeni kitettségüket is.

Az Unió ezt felismerve olyan szabályozások megalkotása mellett döntött, melyek ösztönzik az okosinfrastruktúrák üzemeltetőit a kiber- és adatvédelem implementálására már a tervezési szakaszban. Magyarország, mint minden EU-s tagország, adaptálta a már létrejött jogszabályokat és részt vesz az új szabályozások megalkotásában. A már elfogadott joganyag, így elsősorban a hálózati és információs rendszerek biztonságáról szóló stratégia konzervatív módon közelít a negyedik ipari forradalom jelentette kiberbiztonsági kihívásokhoz, azt nem nevesíti, csak közvetve utal arra, hogy a hazai fejlesztők és szolgáltatók sem maradnak ki az Uniós tevékenységekből.

Figyelembe véve az olyan hazai kormányzati törekvéseket, mind például az okos városok létrehozásának szándéka, ez az óvatos megközelítés nem feltétlenül szerencsés és magában hordozza a kockázatát annak, hogy direkt szabályozási lépések nélkül az újonnan létrejövő okosinfrastruktúrák nem készülnek fel a 2020-as évek kibertérből érkező kihívásaira.

Hivatkozások

[1] A. Greenberg,
"How the CIA can hack your phone, PC, and TV (says Wikileaks)" Wired, March 7, 2017.
https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/ [Accessed January 10, 2019.]

[2] National Cybersecurity and Communications Integration Center, ICS-CERT Annual Vulnerability Coordination Report.

[3] Bányász P.,
Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In: Csengeri János; Krajnc Zoltán (szerk.) Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése,
Budapest, Nemzeti Közszolgálati Egyetem,
Hadtudományi és Honvédtisztképző Kar, (2016) p.918.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[5] European Council, Council of the European Union,
"Reform of cybersecurity in Europe",
General Secretariat of the Council,
https://www.consilium.europa.eu/en/policies/cyber-security/ [Accessed: January 11, 2019.]

[6] Az Európai Parlament és a Tanács 2010/40/EU Irányelve az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről.

[7] Javaslat Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról.

[8] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról.

A szerzőről

DR. KRASZNAY CSABA a Nemzeti Közszolgálati Egyetem adjunktusa, kutatási témája a kiberbiztonság, jelenleg az egyetem Kiberbiztonsági Akadémiájának programigazgatója. A Magyary E-közigazgatástudományi Egyesület és az Önkéntes Kibervédelmi Összefogás elnökségi tagja. 2003-ban szerezte meg diplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar villamosmérnöki szakán, majd PhD-jét az NKE-n 2012-ben katonai műszaki tudományok területén. 2011-ben az „Év Útmutató Biztonsági Szakemberének" választották. Felsőoktatási tevékenysége mellett folyamatosan dolgozik piaci közegben is.

A blockchain és annak specifikus biztonsági kérdései

SÍK ZOLTÁN NÁNDOR
Nemzeti Hírközlési és Informatikai Tanács
sikzoltan@gmail.com

Kulcsszavak: Blokk-lánc, blockchain, Bitcoin, kriptopénz, kriptográfia

A cikk bevezetés a blockchain, mint decentralizált rendszer világába, elsősorban a Bitcoinon, mint az első blockchain alapú rendszeren keresztül. Megkülönbözteti a blockchaint, azaz az értékek internetét, mint platformot a kriptopénzektől, valamint tárgyalja a különböző konszenzus-mechanizmusokat. Végül rátér egyes biztonsági kérdésekre, amelyek alapvetően a blockchain centralizált környezeti elemeinek bennfoglalt sérülékenységeiből, valamint a blockchain protokollbeli hibákból adódó sérülékenységeinek kihasználásából adódnak.

A *blockchain,* magyarul a blokklánc egy kb. tízéves technológia neve. Mivel a magyar fordítás nem terjedt még el, ezért a továbbiakban a blockchain kifejezést használjuk. De mielőtt erre rátérnénk, érdemes egy kissé távolabbról kezdeni. Egészen pontosan az elosztott főkönyvi technológiától *(Distributed Ledger Technology, 1. ábra*).

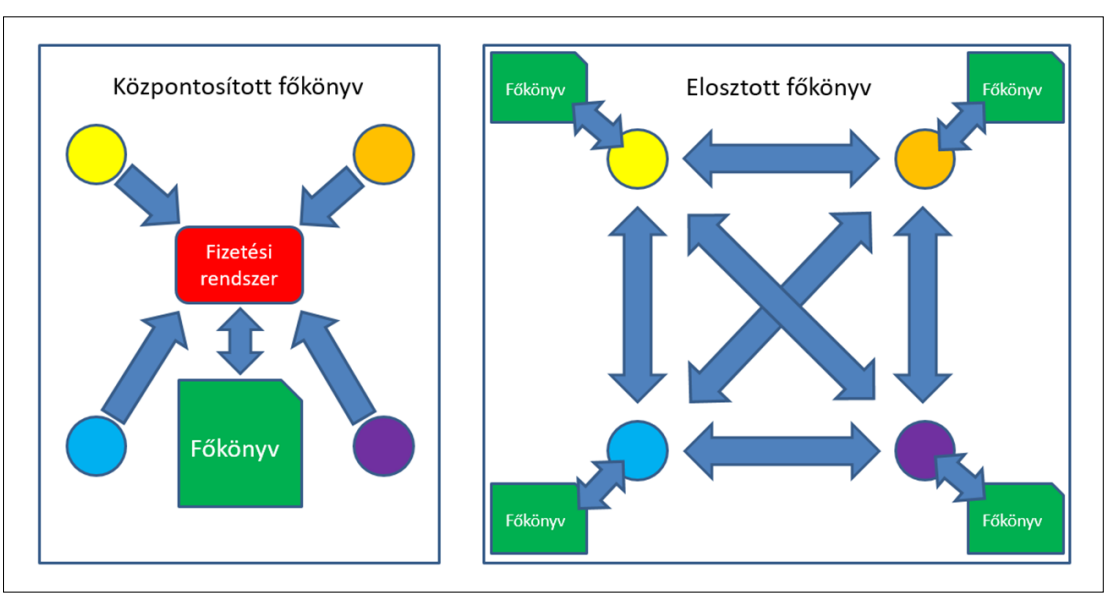
A DLT olyan decentralizált adatbázis, amelyet a különböző résztvevők kezelnek és nincs olyan központi hatóság, mely bíróként, vagy megfigyelőként közreműködne. Példa a jól ismert „torrent" protokoll (igaz, ott a torrent keresőknek kitüntetett funkciójuk van, de ez nem bírói vagy megfigyelői funkció).

A blockchain olyan infokommunikációs rendszer, amely központ nélküli (decentralizált), adatbázisaként láncba rendezett adatblokkokat kezel, működése egyenrangú felek konszenzuskényszerére, valamint kriptográfiai algoritmusok használatára alapul. A blockchain tehát a DLT-nek további feltételekkel rendelkező változataként fogható fel.

Ezek a feltételek így a következők:
– láncba rendezett adatblokkok,
– egyenrangú felek,
– konszenzuskényszer,
– kriptográfiai algoritmusok.

A blockchaint más néven az „értékek internetének" is nevezik, mivel a fenti plusz feltételek alkalmazásával egy-egy, benne tárolt adathoz egyértelműen egy tulajdonos tartozik. Az adat „tulajdonjogát" pedig a decentralizált rendszer egyes, akár egymásban nem bízó szereplőinek a blockchain szabályrendszerén (protokollján) alapuló konszenzuskényszere biztosítja. A legelső, és máig a legismertebb blockchain: a *Bitcoin-rendszer*.

Mindamellett léteznek a blockchain mellett más DLT típusú rendszerek is, csak említésként a tangle, az IPFS (Inter Planetary File System), a hashgraph, amelyekkel a továbbiakban nem foglalkozunk. Ugyanúgy nem foglalkozunk a blockchain egy olyan speciális funkciójával, hogy olyan adatok is tárolhatók benne, amelyek végrehajtható programkódot tartalmaznak és a blockchain,



1. ábra Központosított és elosztott főkönyv közötti különbség

mint rendszer végre is hajtja azokat. Ezek az ún. okos szerződések (*smart contract* – lásd például az Ethereum blockchain rendszert).

A blockchain ötlete annak a problémának a megoldásaként merült fel, hogy központi elem, azaz megbízható harmadik fél részvétele nélkül működve mégis értékeket (kvázi virtuális pénzt) lehessen közvetíteni, azaz tranzakciókat lehessen végrehajtani a blockchain felhasználói, mint szereplők között. Ez az igény abból fakadt, hogy a 2008-as bankválság után sokan úgy gondolták – nem minden alap nélkül –, hogy a mindenki által megbízhatónak hitt bankok mégsem megbízhatóak, ezért őket „ki kell kapcsolni" a rendszerből és központ nélküli, mégis funkcióiban hasonló rendszert kell létrehozni.

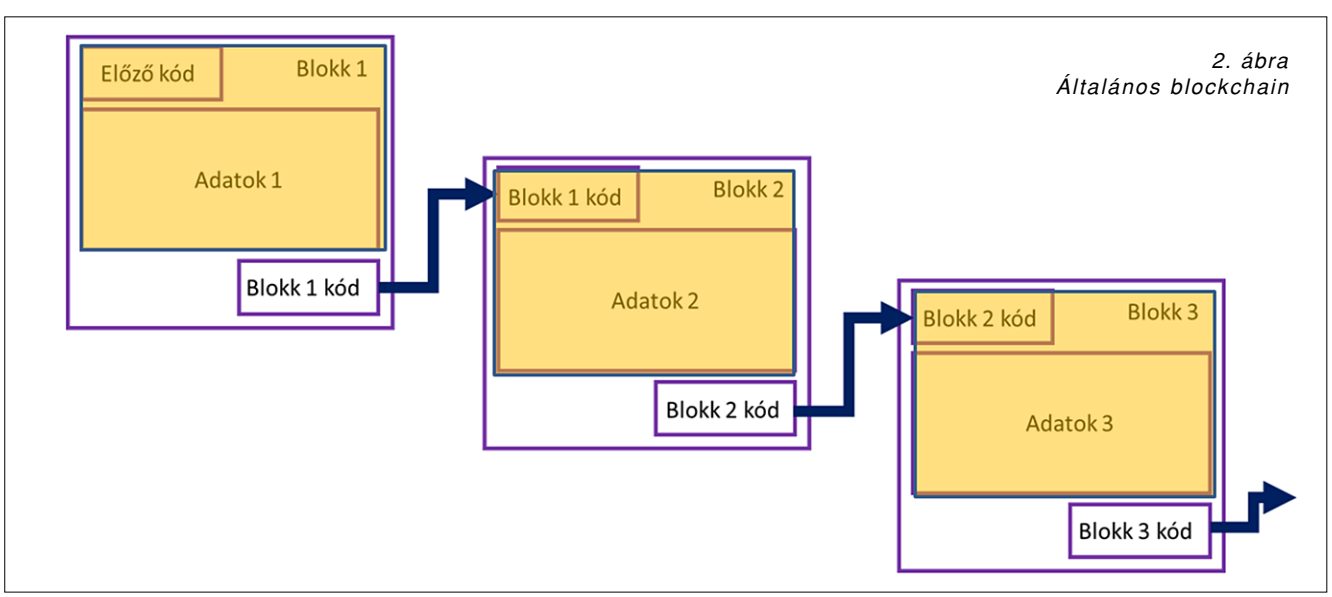
A blockchainben különböző adatokat, azaz a blockchainben tárolt elemeket ún. blokkokba foglaljuk. Mivel egy blokkba maximált mennyiségű adat tehető be – hiszen azért adatblokk –, ezért az így blokkokba foglalt, azaz „blokkosított" adatokból a legtöbb blockchain esetén egy, csak erre az adathalmazra jellemző, de a teljes befoglalt adatnál lényegesen rövidebb, az adatmennyiségtől függetlenül fix hosszúságú ellenőrző kódot, ún. *hash*-t (magyarul kivonatot, lenyomatot, zanzát) képeznek. Ezzel azonosítják az az adathalmazt és a hash tulajdonságai miatt annak változatlanságát. Ez a hash kód kerül az adott blokk ún. fejlécébe. Ezek után a következő blokk elejére ezt a kódot építik be, majd csak utána jön a következő blokkba teendő többi adat, illetve az arra a halmazra jellemző hash kód, és így tovább *(2. ábra)*.

Így végül a blokkoknak egy adott láncolata keletkezik, amelyeket ezek a hash kódok kötnek össze, gyakorlatilag megszakíthatatlanul, hiszen az előző blokk adatainak hash kódja beépül a következő blokkba. A hash kód pedig, bár egyedi módon jellemző az adott adathalmazra, ebből a kódból az adathalmaz mégsem található ki, azaz visszafelé nem működik az algoritmus.

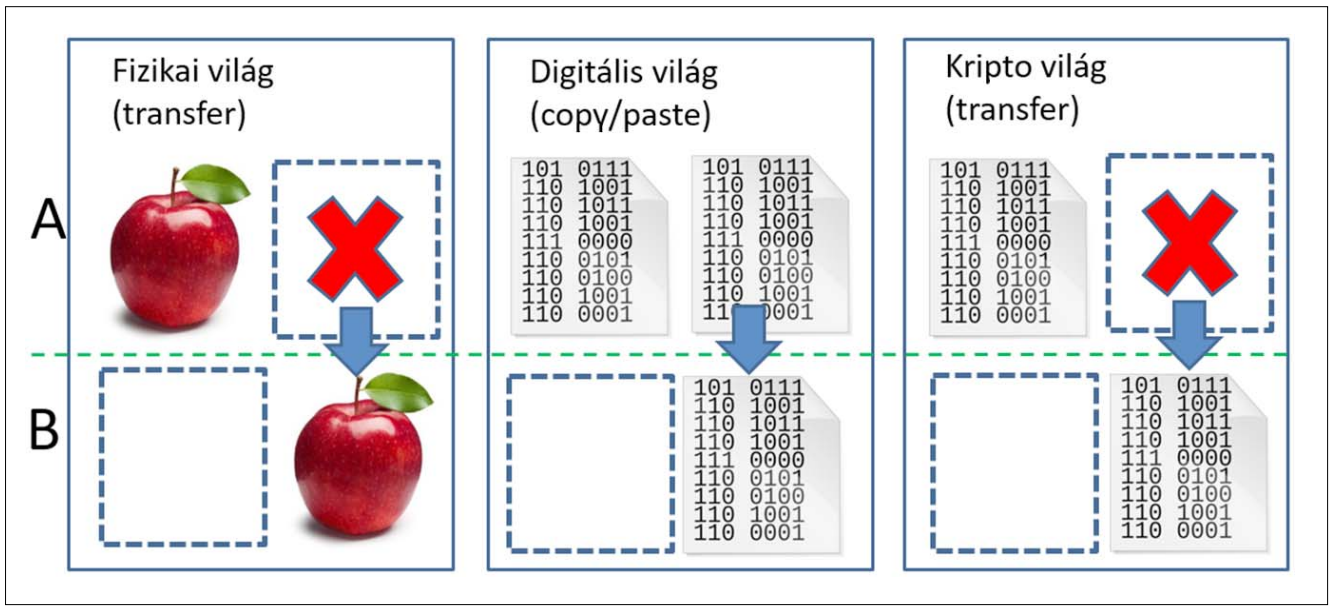
A hash kód ugyanis egy olyan, igen bonyolult algoritmus alapján számolt, megfelelően hosszú számsorból álló ellenőrző összeg, amely gyakorlatilag megjósolhatatlan módon megváltozik, amennyiben azokban az adatokban, amelyekből ez a lenyomat, a hash készült, csak egyetlen egy bitben is megváltozna. Ezért mindazon adat, ami a blockchain blokkjaiban szerepel, a gyakorlatban nem változtatható meg visszamenőleg, sem szándékosan, sem véletlenül, mivel ez esetben a blokkok nem „követik" egymást, így a blockchain megszakad és ez minden résztvevő számára nyilvánvalóvá válik. A blockchainben tehát minden adat, amely a fentiekben leírt láncolatba bekerül, valamilyen módon „le van könyvelve" és így hitelesnek tekinthető és tekintendő. A hitelességet a blockchain rendszer tehát informatikai megoldással kínálja úgy, hogy ez nem egy „egyszerű" adatbázis.

A blockchain, mint technológia a fentiek szerint biztosítja azt, hogy minden szereplő egyszersmind főkönyvelővé (blokk-lezáróvá), sőt revizorrá (validátorrá) is válik azzal, hogy mindenki ellenőrzi mindenki adatait. Ezzel lehet biztosítani, hogy a rendszerben ne kelljen központ, azaz megbízható harmadik fél. A lekönyvelt adatok, mint a felek közti adatáramlást, adatcserét (tranzakciót) bizonyító adatok (ezeket több esetben *token*eknek nevezik) kerülnek a blockchainbe, amivel el lehet kerülni, hogy valamelyik szereplő a saját tulajdonában lévő, immár kvázi pénzként funkcionáló egyedi adatot kétszer tudja felhasználni, azaz „elkölteni" *(double spending)*. Így egy-egy specifikus adatnak értéke lesz, hiszen egyszerre csak egy tulajdonosnál szerepel (és nincs „copy-paste", vagyis az információ, az adatsor nem tud duplázódni).

Végeredményben maga a blockchain szabályrendszere (a *protokoll*) biztosítja azt, hogy az internet világában is létezhessen a fizikai világban megszokott pénzhez hasonló fizetési eszköz. Mivel kriptográfiai algoritmusok használatával érik el azt, hogy a blockchainben szereplő adatok egyediek és a fenti módon láncba rendezettek legyenek, ezért ezt a világot ma már kriptovilágnak, a fenti, pénzhez hasonló adatokat *kriptopénznek* nevezik, mindezt úgy, hogy a kriptovilág kriptopénze a fizikai világban nem létezik *(3. ábra)*.



2. ábra
Általános blockchain



3. ábra A „dolgok” közvetítése fizikai, digitális és kripto-világban

A blockchain a fentiek szerint központ nélküli rendszer, amely minden szereplőt egyedileg azonosít (ezeket nevezzük *wallet*-eknek, virtuális pénztárcáknak, amelyeket nyílt kulcsú rejtjelezési technikával állítanak elő). A pénztárcák tulajdonosait azonban senki más nem tudja azonosítani, mint maga a pénztárca tulajdonosa (illetve a tranzakcióban szereplő két fél, amelyek a tranzakciókat szintén a nyílt kulcsú rejtjelezési technikán alapuló elektronikus aláírással „jegyzik”). A saját pénztárcáját minden szereplő maga állítja elő (generálja) ún. nyílt kulcsú rejtjelezési technológiával.

Mindemellett a központ nélküli működés esetén is egyetlen főkönyvet kell vezetni, amely minden szereplőnél azonos (ez maga a blockchain). Ahhoz, hogy ez megvalósuljon, a szereplők, akik általában nem is ismerik egymást, nem is bíznak egymásban *(trustless system)*, mindemellett egyenrangúak. Ezért valamilyen módon konszenzusra kell jutniuk abban, hogy mi van a főkönyvben, azaz milyen blokkokból áll a blockchain. Ennek keretén belül azt is biztosítani kell, hogy egy-egy tranzakció egyszer, és csak is egyszer legyen lekönyvelve.

Ezért a konszenzus lényege az egyetlen főkönyv kialakításában az, hogy az egyes szereplők (ún. csomópontok, *node*-ok) közül ki az, aki megmondja, hogy melyik a következő főkönyvi lap (azaz blokk). Ahhoz pedig, hogy a csalás, „összebeszélés” lehetősége a gyakorlatban ki legyen zárva, az kell, hogy véletlenszerűen alakuljon ki, hogy ki lesz a következő blokk lezárója.

A konszenzus azonban kényszerű, hiszen az a szereplő, amelyik nem tartja be, a rendszerből automatikusan kizárásra kerül, a többi szereplő zárja ki (ez a blockchain protokolljának, végső soron programkódjának része). A konszenzus kialakításának sokféle módja lehet, ezek közül ma a két legelterjedtebb a munkabizonyíték *(Proof of Work, PoW)*, illetve az érdekeltség alapon való konszenzuskényszer egyes fajtái *(Proof of Stake, PoS)*.

A PoW alkalmazása egy nagyon bonyolult matematikai feladat próbálkozások alapján történő megoldását jelenti (ezt használja a Bitcoin rendszer mellett például az Ethereum, a Litecoin, a Zcash, vagy a Monero). Ahhoz, hogy valaki előállíthassa (lezárhassa) a következő – az előző blokkokhoz a fentiekben leírt módon illeszkedő – blokkot, elsőnek kell megoldania ezt a feladatot. Ezután minden szereplő ezt a blokkot fogadja el hivatalosnak (azaz kialakult a konszenzus), egyes szereplők (a node-ok) pedig validálják is. A feladat olyan nehézségű, hogy véletlenszerűen alakul ki, ki lesz a következő blokk lezárója.

A megoldandó feladat az adott összeállítandó – tehát még készítés alatt lévő – blokkhoz, a benne lévő adatokon, valamint az előző blokk hash kódján kívül hozzá kell tenni még egy számot (ezt nevezik *nonce*-nak), melynek a blokkba való beillesztésével, valamint a blokkon ezzel a számmal együtt képzett hash kóddal a teljes készülő blokk hash kódja speciális értéket vesz fel (pl. adott számnál kisebbnek kell lennie). Ez, a fentiek szerint algoritmussal nem, csak igen sok próbálgatással megoldható feladat, amelyhez igen nagy számítási kapacitásra van szükség (ez a bányászat, a *mining*). A befektetett számítási kapacitás azonban megéri, hiszen a nyertes node (a tranzakciókba foglalt kis könyvelési díjon felül) a semmiből „teremthet”, azaz – központi bank híján – bocsáthat ki pénzt, amelyet a saját pénztárcájában írhat jóvá (ún. *coinbase* tranzakció).

A fenti megoldás azonban igen nagy áramfogyasztást jelent. Ezért kezdtek elterjedni más konszenzust kialakító megoldások, amelyek közül a leginkább használatos az érdekeltség alapú (PoS) *konszenzuskényszer*. Ennek keretén belül azok a csomópontok zárhatnak le egy adott blokkot, amelyek minden egyes körben befizetnek egy bizonyos – nem kicsi – kriptopénzben lévő összeget. Ez azonban azt is jelenti, hogy nem minden szereplő jogosult blokkot lezárni, csak azok, akiknek elég kriptopénz áll rendelkezésükre, azaz eléggé „gazdagok”. Ez tehát egy nem teljesen elosztott rendszer, hiszen nem mindenki egyenrangú, azonban sokkal kevesebb energiát

fogyaszt. Mindemellett ez is biztosítja a véletlenszerűséget, amelyre különböző, igen bonyolult algoritmusok léteznek. Ha ugyanis meg lehetne jósolni a következő blokk lezáróját, akkor fennállna a csalás, összebeszélés lehetősége. A *PoS-algoritmusok* széles, itt nem tárgyalandó skálája áll rendelkezésre (az egyszerű PoS-t használja például a Reddcoin, Navcoin blockchain, az ún. delegated PoS-t (dPoS) az EOS, Steem, Bitshares, az ún. delegated Byzantine Fault Tolerante (bBFT) rendszert pedig a NEO).

A blockchain fenti leírásából következik, hogy a benne tárolt adatok nem kizárólag tranzakciók lehetnek, hanem bármiféle más is, így többek között a fentebb jelzett okosszerződés-kódok, de bármilyen egyéb adatok is. Több cég és szervezet is foglalkozik a felhasználási területek osztályozásával, vagy magukkal az egyes blockchain-ek jellemzőivel (kriptopénzek, blockchain-platformok, „szolgáltatási" – utility tokenek, „értékpapír" – security tokenek). Egy adott blockchain működőképessége így végső soron „csak" az adott résztvevők tárolóhely-kapacitásától és az igénybe vett hálózat sávszélességétől függ.

Mindemellett léteznek olyan blockchain-hálózatok, amelyekhez nem kapcsolódhat bárki (publikus blockchain), hanem csak egy előre meghatározott, „privát", vagy „engedélyezett" *(permissioned)* szereplői kör (privát blockchain). Privát blockchaineket akár vállalatok együttműködése során, akár vállalatokon belül, valamint állami, kormányzati, egészségügyi, oktatási, szerzői jogi területeken is lehet alkalmazni. Mind a publikus, mind a privát blockchaineknek megvannak a maga előnyei és hátrányai, amelyekkel itt most részletesebben nem foglalkozunk.

A blockchain az első olyan innováció, amely nem csak az informatikára, hanem más iparágakra, sőt a társadalmi berendezkedésre is felforgató (diszruptív) hatással van. Eredetileg a bankrendszer „kikerülése" volt a cél, de például az okos szerződéseknek köszönhetően a jogra is hatással van, elosztott rendszer lévén olyan szolgáltatásokat tud biztosítani, amelyek mögött nincs egy-egy vállalat, sőt, például választási rendszer is létrehozható segítségével, így a politikai berendezkedést is érinti. Ezért a blockchain napjaink talán legjelentősebb infokommunikációs innovációja az internet megjelenése óta.

Mivel azonban, mint technológiai megoldás a fentiek szerint értékeket tárol és közvetít, ezért különösen kitett az ellene irányuló támadásoknak. A támadások mindegyike azonban valamilyen sérülékenységet használ ki, természetesen olyat, aminek kihasználása gazdaságilag, vagy valami másért megéri a kockázatot. A blockchain esetén figyelembe kell venni, hogy az új technológia olyan sérülékenységeket is hordoz, amelyekkel az infokommunikációs világ eddig még nem szembesült. Mindemellett, miután „közvetlen" anyagi értéket is képviselnek a benne tárolt adatok, valamint többnyire anonim módon történnek a tranzakciók, ezért más – nem feltétlenül infokommunikációs – területek is érintettek, illetve támadásoknak kitettek a blockchain megjelenése okán. Ez utóbbi esetre példa a zsarolóvírusok *(ransomware)* megjelenése, vagy akár egy váltságdíj kriptopénzben való megváltásának igénye.

A blockchain mindazonáltal – legalábbis az eddig leírtak szerint – bombabiztosnak tűnik, de mégsem az. Vannak ugyanis olyan sérülékenységek, amelyeket a blockchain „környezetének" centralizáltsága okoz, vagy maga a blockchain válik valamilyen módon centralizálttá, holott pont ennek az elkerülésére jött létre.

Centralizált, és így nagyobb sikerrel támadhatók pl. az egyes felhasználók pénztárcái. Nem maga a kriptográfiai algoritmus, hanem a pénztárcában lévő rejtjelező kulcs (az ún. privát kulcs) védelme érdekében használt jelszavak és egyéb védelmi mechanizmusok (még a hardveresek is). Minél több kriptopénz van egy tárcában, annál inkább megéri azt valamilyen módon feltörni, igaz, ezt leginkább az infokommunikációban már hagyományos módszerekkel kísérlik meg (a brute forcetól egészen a keyloggerekig).

Ugyanúgy centralizáltak a *kriptotőzsdék* is, ahol a különböző kriptopénzekkel kereskednek, illetve a kriptopénz és hagyományos pénz (fiat) közti váltók is. Csak az utóbbi időben fejlesztettek ki szintén blockchain alapú, decentralizált kriptotőzsdéket (pl. a Waves blockchain platformon). A centralizált kriptotőzsdéken igen nagy pénzek forognak, és ahhoz, hogy ezzel a felhasználók kereskedni tudjanak, szükségképpen kriptotőzsdén is kell, hogy legyen pénztárcájuk, amelynek rejtjelező kulcsát ezért maga a kriptotőzsde tárolja. Egy kriptotőzsde feltörése tehát gazdaságilag igen kifizetődő, dollármilliók, -tízmilliók vesznek oda, igen kevéssé lenyomozható módon (szintén hála a blockchainnek). A centralizált tőzsdék szoftvermegoldásai ráadásul sokkal sérülékenyebbek, mint a blockchain-en futó okos szerződések kódjai, hiszen csak egy helyen hajtódnak végre, nincs egy közösség, amelynek számítógépei validálják a helyes programfutást. Egy-egy ilyen centralizált tőzsde hagyományos módszerekkel való feltörése ily módon is kifizetődő.

Ugyanígy PoW esetén az ún. *bányásztársaságok* is sérülékenyek. Ezek azok a – szintén centralizált szoftvert használó – vállalkozások, amelyek az egyes kisebb kapacitással rendelkező (pl. otthoni gépeket használó) bányászok számítástechnikai kapacitását összegyűjtve, sokkal nagyobb eséllyel indulnak a fentiekben már említett speciális szám *(nonce)* megtalálásáért, így a sikeres blokk lezárásáért és az érte járó nem kevés jutalék begyűjtéséért.

Ezek a bányásztársaságok, bár nem tárolnak közvetlen pénztárca-kódokat, a begyűjtött jutalékot elosztják egymás között a megadott algoritmus alapján. Ezért náluk, ha ideiglenesen is, de igen nagy kriptopénzben kifejezett összegek vannak tárolva, így ezek feltörése is kifizetődő. Továbbá az egyes kisebb bányászok által futtatott kódot is feltörik (egy-egy gépen az a kód is csak egy példányban, tehát centralizáltan működik), és az általa termelt kriptopénzt mintegy „átirányítják" más pénztárcára. De ugyanígy bányászatra is tudják fogni azokat a számítógépeket – természetesen a tulajdonos tudta

nélkül –, amelyek eredetileg más feladatot végeznek és semmi közük a kriptopénz bányászathoz (az ilyen támadások neve a *cryptojacking*).

Ezt kisebb gépeknél vírus telepítésével el lehet érni, nagyobb kapacitású gépeknél pedig akár fizikai hozzáféréssel is lehetséges bányászszoftvert telepíteni. Bár ez utóbbi gyorsan kiderül, ha egy szuperszámítógép az egyik pillanatról a másikra éjjel-nappal teljes kapacitással kezd dolgozni, az ezzel járó villanyáram fogyasztással együtt (2017-ben el is fogtak négy orosz számítógépes szakembert, akik egy ilyen gépet bányászatra kezdtek használni). A teljesség igénye nélkül még megemlíthető az a példa is, amikor az egyetemi kollégisták a nyári szünet idejére „véletlenül" bekapcsolva hagynak egy bányászgépet az ágyuk alatt, természetesen a kollégium villanyszámlájának terhére.

Szintén a PoW-rendszert használó blockchain-ekhez tartozik még több féle támadás (attack) is, amelyek közül ma már több helyen is felbukkant az ún. *51%-attack*. Ez a gyakorlatban azt jelenti, hogy az adott kriptopénz bányászatához szükséges számítástechnikai kapacitás egy kézbe kerül, irányítás alá vonva így magát a blockchain-protokollt. Hiszen így az tudja megmondani a „szabályokat", aki többségben van, így a kisebbséget tudja kizárni (ez igen hasonló a parlamenti demokráciák egyszerű többséget igénylő szavazati rendszeréhez). Az 51% összegyűjtése mindemellett nem is mindig derül ki azonnal (legutóbb az Ethereumból kivált Ethereum Classic rendszer esett ennek áldozatául, lehetővé téve az eredetileg elkerülendő dupla költést). Az így összeállt többség mögött ugyanis nem kell ugyanannak a pénztárcának állnia (ahová a jutalékot begyűjtik), hiszen az nem ellenőrizhető, hogy egy-egy pénztárcának fizikailag ki a tulajdonosa. Az ilyen, többszöröződésen alapuló támadást nevezik *Sybill-attack*nak, amely nevét egy Sybill nevű betegről kapta, akinek állítólag többszörös személyisége (Multiple Personality Disorder, MPD) volt.

A PoS-rendszereknél azonban az 51%-attack nem működik, hiszen ott előre kiválasztott, és nagy összegeket kockáztató, ezért mindenki által legalább pénztárca szinten ismert szereplők közt kell konszenzusra jutni. A konszenzus a legtöbb esetben a kétharmad (66,66...%), hasonlóan a parlamenti demokráciák minősített többséget igénylő szavazásaihoz. Itt leginkább az *összebeszélés* esete áll fenn, ami legutóbb az EOS blockchain-rendszerben fordult elő, itt a megkövetelt 26 kiválasztottból 16 beszélt össze, biztosítva ezzel, hogy nagy többségben közülük kerüljön ki a sikeres blokklezáró (megjegyzendő, hogy a PoW-rendszertől eltérően itt nem bányászok *(miner)*, hanem ötvözők és kovácsok *(minter,* illetve *forger)* a blokklezárást végzők nevei).

A centralizált területeket tekintve igen fontos szólni még az adott blockchain-rendszer kitalálóiról, fejlesztőiről. Ők egy adott szűk kört képviselnek, akik végül is a protokollt lefektetik, amely alapján az általuk kitalált blockchain-rendszer működik. Bár mindenki egyenlő, ők itt az „egyenlőbbeket" képviselik, hiszen a blockchain továbbfejlesztéseinél is ők vannak előnyben, mivel ők látják át a rendszer- és a programkódokat. Például a Bitcoin-rendszert kitaláló, azonban ilyen néven nem létező Satoshi Nakamoto személy volt a kitalálója a protokollnak és a köré gyűlt fejlesztők értettek hozzá annyira, hogy akár továbbfejlesztéseket is tudjanak javasolni *(Bitcoin Improvement Proposal, BIP)*, illetve a javaslatokat elfogadni és beépíteni a protokollba (végül is bárki javasolhat továbbfejlesztést, de beláthatóan szűk az a kör, akinek erre esélye van). Ezen még az sem segít, hogy a blockchain-rendszerek protokollja és megvalósítási programkódjai nyílt forráskódúak (pl. a Github-on elérhetők). Ez a megközelítés egyébként minden blockchain-rendszerre igaz (pl. az Ethereumnál az Ethereum Improvement Proposal, EIP révén). A fentiekben említett EOS-rendszernél is a rendszer kitalálói egyeztek meg abban, hogy 26 partner kell (és abból kell kétharmadnak egyezségre jutnia).

Az „egyenlőbbek" sem értenek azonban mindig egyet. Ha mondjuk jelentős számú fejlesztő, illetve számítási kapacitást birtokló node például két összemérhető nagyságrendű táborra oszlik, akkor ún. elágazás *(fork)* alakul ki, és az adott blokkig egy blockchain egy idő után két (bár közös gyökerű) blockchainre oszlik. Így alakult ki a Bitcoin mellett 2017 augusztus elején a *Bitcoin Cash,* valamint 2014-ben az Ethereum rendszerből kivált *Ethereum Classic*. Ezek a rendszerek így külön kriptopénztípust képviselnek, illetve keltenek életre (amelyek tőzsdei árfolyama is különbözik attól, amiből forkoltak).

Az ilyen forkok viszont újabb sérülékenységi pontokat is jelenthetnek, hiszen a fork egyik ágán más a protokoll, mint a másikon és az új ágon lévő protokoll nem biztos, hogy olyan kiforrottan, megbízhatóan működik, mint amelynek működőképességét az idő igazolta (más kérdés, hogy a fenti két esetben pont azért váltak ki, mivel az eredeti protokoll nem működött az idő közben, a tapasztalatok alapján kialakult új kívánalmak szerint).

Megjegyzendő, hogy blockchain-protokoll megvalósítási hiba nem fordulhat elő, hiszen a helyes kódot futtató többség a helytelen kódot futtatót azonnal kizárja (kivéve a már fent említett 51%-attack-ot, de a protokollmódosítást akkor is csak sikeres attack után lehet bevezetni).

Azonban, ha már a forkoknál tartunk, egy jelentős sérülékenységi ponthoz érkeztünk, ezek pedig a protokollhibák. Azok az esetek, amelyekre nem gondoltak, vagy előfordulásukat igen elenyészőnek tartották, de az idők folyamán a fenyegetettség jelentősen megnőtt. Satoshi Nakamoto nem gondolta volna, hogy a Bitcoin-rendszer tranzakciószáma egyszer olyan mértékű lesz, hogy az 1 MB-ban megállapított blokkméret, valamint a 10 percben megállapított *blokkidő* (az egymást követő blokkok sikeres bányászatához számított és a feladat bonyolultságát megfelelően ehhez állító időintervallum) egyszer kevésnek bizonyul. Ezt a skálázhatósági gondot akarta kiküszöbölni sok javaslat (BIP), amelyek közül az eddig egyetlen, ténylegesen sikeresnek bizonyuló a Bitcoin Cash lett.

Ugyanígy nem gondolták volna, hogy a blokkba való bekerülésre váró tranzakciókat még módosítani lehet *(transaction malleability* – magyarul tranzakció képlékenység), amely hibának a kihasználása 2014-ben a bitcoin kereskedés 70%-át lebonyolító Mt.Gox kriptotőzsde órák, illetve percek alatt való összeomlásához, és így hihetetlen mennyiségű kriptopénz odaveszéséhez vezetett. Mivel a blockchainekben, természetüknél fogva nincs storno tranzakció, ezért a veszteséget nem lehetett visszahozni, hiszen a pénztárcák mögött anonimek a tényleges résztvevők, akiket szép szóval igen nehéz rávenni arra, hogy adják vissza az ellopott kriptopénzt (mert kit is szólítanánk meg egyáltalán?).

Ugyanígy, Vitalik Buterin (ő viszont létezik), az Ethereum rendszer akkor 19 éves feltalálója sem gondolta volna, hogy a rendszerébe beépített okos szerződések kódját is meg lehet írni hibásan. Egy ilyen programozási hiba az okos szerződésben (rekurzív jóváírás a terhelendő számla nullázását megelőzően) vezetett oda, hogy a 2014 május-júniusában létrehozni kívánt központ nélküli szervezet *(Decentralized Autonomous Organisation, DAO)* – amit, mivel az első volt, egyszerűen csak „The DAO" névre kereszteltek, – áldozatául esik egy ilyen programhiba szándékos kihasználásának. A The DAO esetén a részvénykibocsátásokhoz hasonlóan kriptopénzben (inkább tokenben) kifejezett pénzgyűjtést szerveztek, amihez bárki csatlakozhatott. Az ilyen tőkebevonás neve az *Initial Coin Offering* (ICO) a hagyományos részvénykibocsátáshoz (Initial Public Offering, IPO) hasonlóan, bár jelentős különbségek vannak köztük. A The DAO-hacker a fenti módon a begyűjtött pénzt kb. egyharmadát átirányította egy másik, általa birtokolt pénztárcába és ha nem figyelnek fel erre, akár az egészet is átirányíthatta volna anélkül, hogy bárki bármit tehetett volna ellene (mivel a blockchainben minden node-on ugyanaz az okos szerződés kód fut, ezért azt megváltoztatni nem lehet, ha hibás, akkor sem). Így alakult ki az Ethereum Classic fork, amikor is Vitalik Buterin egyszemélyben megmondta, hogy a könyvelés az x-edik blokkig visszafejtendő és attól kezdve érvénytelen. Akik ezt elfogadták, maradtak az Ethereum rendszerben, akik pedig abban hittek továbbra is, hogy „a protokoll szent", azt centralizált erő nem változtathatja meg, még ha maga a kitaláló is az, egy fork révén létrehozták a fentebb már többször is említett Ethereum Classic rendszert. Az Ethereum rendszerben azóta is figyelik, hogy azzal a pénztárcával, ahová a The DAO hacking-ból származó, mintegy 3,641,694 ether-t átirányították (ether az Ethereum rendszer kriptopénzének neve), nehogy valamilyen tranzakciót végezzenek.

Az eset csattanója pedig az, hogy a The DAO-hacker nyílt levelet írt a közösségnek, amelyben kéri, hogy fizessék ki neki ezt a „díjat", mivel ő részletesen tanulmányozta a kódot és sok munkája fekszik benne, valamint, ha valaki egy személyben megmondhatja, hogy mi történjen egy blockchainnel, akkor a blockchainbe, mint technológiába vetett hit és bizalom inog meg. A helyzet pedig az, hogy még igaza is volt. A The DAO-hacker egyébként 2017-ben elnyerte a blockchain-rendszerek legbefolyásosabb személyiségei közt az első helyet a kriptovilággal foglalkozó meghatározó online folyóiratok szerint (CoinTelegraph, CoinDesk).

A szerzőről

SÍK ZOLTÁN NÁNDOR jogi szakokleveles villamosmérnök, MBA, politikai szakértő. Tőzsdei szakvizsgával és értékpapír-kereskedői szakvizsgával rendelkezik. Villamosmérnöki diplomájának 1986-os megszerzését követően a versenyszférában látott el különböző vezetői pozíciókat. 1999-től a Hírközlési Főfelügyelet (ma Nemzeti Média és Hírközlési Hatóság) informatikai igazgatója volt, 2000–2002-ig informatikai kormánybiztos. 2000–2003-ig a Nemzeti Hírközlési és Informatikai Tanács (NHIT) tagja, majd szakértője, 2011-től a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) tanácsadója, 2015–2019-ig az NHIT alelnöke. 2018-tól a Magyar Államkincstár tanácsadója. Jelenlegi kutatási témája a blockchain.

Iskolai hálózat a jelenben és a jövőben

HORVÁTH ÁDÁM, VIRGA KRISZTINA
Digitális Jólét Nonprofit Kft.
horvath.adam@dpmk.hu

Kulcsszavak: Digitális Oktatási Stratégia, iskolai hálózatfejlesztés, a jövő iskolai hálózata

A fiatalok munkaerőpiaci esélyei szempontjából elkerülhetetlenné vált az oktatási rendszer digitalizálása. A kormány ezt időben felismerve, a magyar társadalom és nemzetgazdaság fejlesztését célzó Digitális Jólét Programon belül elkészítette Magyarország Digitális Oktatási Stratégiáját (DOS). Ennek egyik kiemelt területe az iskolai Wi-Fi-hálózat fejlesztése, melynek kialakítása az üzleti szférától jelentősen eltérő kihívások elé állítja a központi szolgáltatásmenedzsmentet. A jelenlegi fejlesztéseken túl pedig el kell kezdeni a felkészülést a jövő kihívásaira is, hiszen már most végig kell gondolni, hogy a jövőben vajon milyen lesz az iskola: milyen térben és milyen eszközökkel fog a tanulás megvalósulni, fel kell készülni az integrált rendszerek folyamatos szinkronizálására, az IoT-val a virtuális gépek, szenzorok, robotok széleskörű terjedésére, valamint a 3D és VR terjedésével a robosztus sávszélességi igényekre is.

1. Bevezetés

Ma már szinte közhelynek tűnhet, de napjainkban a digitalizáció a fejlődés és versenyképesség egyik legfőbb hajtóereje, ezért a felnövekvő generáció munkaerőpiaci esélyei szempontjából elkerülhetetlenné vált az oktatási rendszer digitalizálása. A kormány ezt időben felismerve, a magyar társadalom és nemzetgazdaság fejlesztését célzó Digitális Jólét Programon belül elkészítette Magyarország Digitális Oktatási Stratégiáját (DOS), hiszen a 21. században már nem lehet 20. századi módszerekkel tanulni és tanítani. A feladat hatalmas, a jövő iskolájában minden tanár és diák digitális eszközökkel (sajáttal vagy iskolaival) digitális hálózatra kapcsolódik, a tanárok digitális módszertanokkal digitális tananyagokat oktatnak, a diákokat önálló kutató (projekt)munkára, valamint tartalomelőállításra ösztönzik, ráadásul az oktatási adminisztráció és a tanárok továbbképzése is digitális alapon történik. Ennek infrastrukturális háttere most van kialakítás alatt, a 2019/2020-as tanévet már minden iskolában úgy kezdhetik, hogy jól menedzselt, belső Wi-Fi-hálózat áll a diákok és tanárok rendelkezésére.

A DOS 2016-os elkészítésekor az akkori legmodernebb iránymutatásokat és nemzetközi tapasztalatokat vettük figyelembe, de amilyen mértékben és sebességgel változik a digitális világ, már most is látható, hogy rövid- és középtávon is olyan kihívások elé néz a jövő iskolájának hálózati kialakítása, amilyenre még nem volt példa a közoktatásban.

2. Iskolai hálózatok

Magyarország Digitális Oktatási Stratégiája (2016-ban) az iskolai hálózatokkal szemben az alábbi főbb paramétereket határozta meg:

– 500 fő alatti iskolákban legalább 100 Mbit/s, 500 fő feletti iskolákban pedig 1 Gbit/s sávszélesség legyen elérhető;
– minden tanteremben, iskolai könyvtárban, közösségi térben, gyakorlati helyen menedzselhető Wi-Fi-lefedettség biztosítsa a tanulók számára a megfelelő sávszélességet;
– strukturált, védett hálózat és határvédelmi eszközök kerüljenek a rendszerbe, legyen naprakész vírusvédelem, spamszűrés, tartalomszűrés és védett webes felület;
– a felsőoktatásban már meghonosodott eduroam/eduid hálózat keretén belül biztosítva legyen, hogy a közoktatásban tanuló diákjaink is bármely európai, eduroam hálózatra bekapcsolódott intézményben saját felhasználó azonosítójukkal csatlakozhassanak az ottani hálózatra *(1. ábra)*.

A TIOP 1.1.3-as pályázat keretén belül már 2013-ban megkezdődött az iskolai Wi-Fi-hálózat fejlesztése, ekkor 1,1 milliárd Ft értékben 1700 iskolának szereztek be átlagosan 2,3 Access Pointot. A DOS megvalósítására az EU-s átlagnál alacsonyabb szinten álló konvergencia régiókban, az EFOP 3.2.4.-16 Digitális kompetencia fejlesztése pályázat keretén belül jelenleg több mint 2500 intézménybe átlagosan 8-14 AP-t telepítenek ki, illetve hazai forrásból az EU-s átlagot meghaladó Közép-Magyarországi Régióban várhatóan 1000 intézményben, szintén iskolánként 8-14 AP kitelepítése történik – mindkét régióban 100%-os iskolai lefedettség biztosításával.

3. A hálózatok menedzselése

Az eszközök kitelepítése azonban csak az első lépés; a hálózatot, a hálózatra csatlakozó eszközöket menedzselni is kell, a központi Wi-Fi- és szolgáltatásmenedzsment kialakítása a Kormányzati Informatikai Fejlesztési

Ügynökség (KIFÜ) feladata. Azt, hogy ez mekkora feladat, talán jól érzékeltetik az alábbiak: amennyiben a teljes közoktatásban kiépítésre kerül a Wi-Fi-hálózat, ennek a hálózatnak több mint 1 millió tanulót és több mint százezer tanárt kell egyszerre kiszolgálnia. Bár már ezek a számok is hatalmasak, de még mindig nem igazán jelzik a feladat nagyságát, hiszen a felhasználók akár több eszközzel is regisztrálhatnak a hálózaton, ami megtöbbszörözi a menedzselendő csatlakozások és eszközök számát, ennek minden nehézségével (hálózatvédelem, spamszűrés, tartalomszűrés stb.) együtt. Központi szolgáltatás-menedzsmentként fog működni a Wi-Fi-végpontok menedzsmentje, a felhasználó-menedzsment, a help desk és a hálózatvédelem.

Mivel mindez központilag lesz kezelve, ugyanezen központ alkalmas lesz a különböző analitikák elkészítésére, mint például kapacitáskihasználtság, látogatott tananyagok, oldalak stb. kapcsán, ezzel célzottan, akár intézményspecifikusan is lehet majd javaslatot tenni a digitális eszközökkel támogatott oktatás fejlesztésére. A központi szolgáltatásmenedzsmenthez tartozik a CSIRT (Computer Security and Incident Response Team) kezelése is, melynek feladata az informatikai infrastruktúra védelme. Intézményi szinten marad a tantermi eszközök, belső hálózat/tárhely kezelése (ennek szerepe idővel csökkenni fog), illetve az iskolai felhőszolgáltatások (private, community, public) kezelése.

Az iskolai hálózat kialakításában, struktúrájában, a használt eszközök és alkalmazások terén nagy mértékben eltér az üzleti felhasználástól. A hálózati aktivitást, annak jellegét, irányát, nagyságát jelentősen befolyásolja a használt alkalmazások köre, ezen a téren is jelentős eltérés van az üzleti és az oktatási hálózatok között.

Az üzleti hálózat jellemzői, hogy célja az üzletmenet kiszolgálása (csoportmunkát, üzletet támogató szakrendszerekkel), jellemzően vezetékes hálózattal (Wi-Fi-elérhetőség mellett), a felhasználói eszközsűrűség alacsony, az eszközök megoszlanak a PC-k és mobil eszközök között, saját eszköz használata jellemzően megengedett, a forgalom munkaidőben egyenletes, az otthonról elérés támogatott, forgalomszűrés nem jellemző (csak a kártékony szoftverkódok ellen) és a felhasználókezelés a cég méretétől függően az ad hoc-tól a szigorúan szabályozott, központi felhasználókezelésig terjed.

Ezzel szemben az iskolai hálózatokra az jellemző, hogy célja az oktatás támogatása (tanulást támogató eszközökkel/alkalmazásokkal, melyek folyamatosan változnak, oktatási adminisztráció kezelésével), a hálózat inkább Wi-Fi-n keresztül érhető el, a felhasználói eszközsűrűség nagyon magas (1-3 eszköz/m^2), a saját eszközök bevitele (BYOD) kifejezetten szükséges lenne (de megfelelő mobile device management nélkül a hasznossága megkérdőjelezhető), a forgalomra csúcsidőszakok jellemzőek, az otthonról elérés még nem kialakult, nagyon fontos a forgalomszűrés/tartalomszabályozás kérdése, valamint a hozzáférés és felhasználókezelés központilag történik. Ezek alapján is látható, hogy az iskolai központi Wi-Fi-hálózatnak olyan feltételeknek kell megfelelnie, amelyekre még nem igazán ismertek gyakorlati példák.

Folyamatosan figyeljük, milyen trendek jellemzőek a tanulást támogató eszközökben, a toptools4learning.com alapján idén az alábbi trendek erősödtek: web (youtube, google, audio, könyvkivonatok), felhő (irodai alkalmazások, adattárolás/megosztás), webes tanfolyamok, kurzus- és tartalomfejlesztés, kollaborációs eszközök, interaktív szavazórendszerek, Microsoft ökoszisztéma tovább terjedése, illetve videokonferenciák használata, ezek használatára is kifejezetten alkalmasnak kell lennie a hálózatnak.

A célunk az, hogy a digitális eszközökkel támogatott oktatás ne csak egyes projektekre, témanapokra korlátozódó, kivételes eset legyen, hanem folyamatosan segítse a 21. századra való felkészülést, ezért már most látjuk, hogy a továbbiakban mely területekre kell fókuszálni annak érdekében, hogy a jelenlegi hálózatunk a későbbiekben is megfeleljen a jövő kihívásainak.

1. ábra A hálózattal szembeni elvárások

Már a közeljövőben tovább fejlesztendő a sávszélesség, a mostani iskolai létszámhoz kötött sávszélesség helyett (500 főnél kisebb iskoláknak 100 Mbit/s, 500 főnél nagyobb létszámú iskoláknak 1 Gbit/s) a sávszélességet 2-4 Mbit/s/főre lesz szükséges növelni (pl. a jövő egyértelműen a VR/AR, 3D elterjedése felé mutat, ami robosztus sávszélességet igényel, ennek kezelésére is fel kell készülnünk). A vezeték nélküli képernyőmegosztás is hamarosan elvárássá válik, amely akár 150-300 Mbit/s sávszélességet is igényelhet a minőségtől függően.

Mindennek együtt kell járnia a Wi-Fi-lefedettség minőségének javításával és a központi szolgáltatásmenedzsment kapacitásának növelésével *(2. ábra)*.

4. Felkészülés a jövőre

Közép- és hosszútávon végig kell gondolni, hogy a jövőben vajon milyen lesz az iskola, hol és milyen eszközökkel fog a tanulás történni? Egyre inkább terjed az irányzat, amelynek lényege, hogy a tanulási tér kilép/átlép az iskola falain kívülre, tanulási térré és környezetté válik a diák közvetlen és távoli környezete is, amire szintén fel kell készülni.

Ezért már a középtávú kihívások közé tartozik a Virtual Learning Environment (VLE) kezelése, ahol a diákok virtuális osztályokban kapják meg a feladatokat, tananyagokat, feldolgozandó ismereteket, valamint a mérés-értékelés is ezen kereteken belül történik. A VLE elterjedése az oktatási hálózati forgalmat az iskolán kívülre is kiterjeszti, tehát az iskolán kívülről indított forgalmat is kezelni kell majd valamilyen módon. Ehhez és a jövőbeni eszköz- és tartalomkezeléshez jellemzően divergáló forgalom tartozik, az integrált rendszereknek folyamatosan szinkronizálniuk kell a felhasználók eszközei és a felhasználói tartalmak között. Az integrált rendszerekkel való kapcsolattartás állandó forgalmat generál, hiszen eszközeink nem pusztán az ad hoc kommunikációs igényeket, hanem egyre több automatizált háttértevékenységet (pl. fájljaink feltöltése) is kiszolgálják.

Egyre jellemzőbb az Internet of Things (IoT) eszközök és alkalmazások használata is, például amerre a diák jár, rögzíteni, szinkronizálni fog az okosórája, okostelefonja, így még több saját eszköz fog a hálózatra csatlakozni. Az IoT magával hozza a virtuális gépek, szenzorok, robotok széleskörű terjedését, a hálózatokkal kapcsolatban pedig fel kell készülnünk a hibrid mobilhálózatok és az IPv6 kezelésére, illetve a versenyképesség megőrzése és javítása érdekében általánossá, megszokottá kell tenni a felhőben való távoli adatokkal és távoli alkalmazásokkal történő munkát.

5. Összefoglalás

Összességében elmondható, hogy bár már jelenleg is hatalmas munka folyik az iskolai hálózat kialakításával és korszerűsítésével kapcsolatban, de a jövőben olyan infrastrukturális kihívásoknak és fejlesztéseknek nézünk elébe, amelyhez elengedhetetlen a 21. századi technikai és módszertani fejlesztések követése és az ipari megoldások alkalmazása az iskolákban is.

Szerzőinkről

HORVÁTH ÁDÁM a Pázmány Péter Egyetem Jogtudományi Karán tanult, a European Business Polytechnics Cambridge-en szerzett üzleti, közgazdasági végzettséget. 2002–2003 között az Educatio Kht. igazgatója volt, 2003–2006 között az Oktatási Minisztérium informatikai tanácsadója. 2006–2010-ig a Nemzeti Fejlesztési Ügynökség, 2010–2011 között a PNO Magyarország Kft., 2011-től pedig az AdWise 2000 Szaktanácsadó és Szolgáltató Kft. vezető tanácsadója volt. 2012–2014 között a Commitment Zrt-nél mérés-értékelési szakértő és vezető tanácsadó, 2015–2017-ig az Informatikai Vállalkozások Szövetségénél (IVSZ) volt oktatási igazgató. 2017 márciusa óta a Digitális Jólét NKft.-n belül, a Digitális Pedagógiai Módszertani Központ divízióvezetője.

VIRGA KRISZTINA gazdasági mérnöki, számítástechnika tanári, okleveles informatikus végzettségekkel rendelkezik. 1995–2001 között a Postabank Rt-nél dolgozott, 1998-as gazdasági mérnöki diplomájának megszerzése után termékfejlesztőként, illetve lakossági üzletági elemzőként. 2002–2009 között az OTP-Garancia Biztosítónál (ma Groupama Biztosító) volt termékmenedzser. Miután 2010-ben megszerezte okleveles informatikus diplomáját is, egy hirtelen váltással a közoktatásban helyezkedett el informatika tanárként, ahol 2018-ig dolgozott, az utolsó három évben informatikai munkaközösség-vezetőként is. 2018 augusztusa óta a Digitális Pedagógiai Módszertani Központ digitális fejlesztője.

2. ábra
A közeljövő és a középtáv fejlesztési feladatai

Az Európai Elektronikus Hírközlési Kódex hatása a rádióspektrum-gazdálkodásra

ULELAY EMÍLIA
Nemzeti Média- és Hírközlési Hatóság
ulelay.emilia@nmhh.hu

Kulcsszavak: Európai Elektronikus Hírközlési Kódex, rádióspektrum-gazdálkodás, 5G, Peer review – szakértői áttekintő eljárás

Az Európai Elektronikus Hírközlési Kódex 2018. decemberi kihirdetésével elkezdődött a tagállamok rendelkezésére álló 24 hónap számítása, amennyi idő alatt nemzeti jogrendjükbe kell, hogy építsék az ágazatra vonatkozó új keretszabályokat. A rádióspektrum-gazdálkodás területén is számos változás történt, melyek közül a legfontosabb új szabályozási elemek áttekintésére törekszik a cikk, vizsgálva annak lehetséges hatását, különös tekintettel az 5G bevezetésére.

1. Bevezetés – a Bizottság 2016-os szabályozási céljai

Valóban reform szabályok születtek az elektronikus hírközlési ágazat keretszabályozásának második felülvizsgálata eredményeként? A Bizottság 2016-ban tett szabályozási javaslatában a „Jobb rádió-frekvenciahasználat" cím alatt a következőket hirdette meg: *„A szabályozás terén folytatott gyakorlatban EU-szerte jelentkező eltérések csökkentése különösen fontos a vezeték nélküli kommunikáció legfőbb 'nyersanyagát' jelentő rádiófrekvencia-spektrum vonatkozásában."*[1]

A Bizottság elismerte a jól működő rádióspektrum-szabályozási eszközöket[2], melyek mellett javaslatot tett az 5G hálózatok mielőbbi kiépítése, a gigabites nagyságrendű adatforgalmat lehetővé tevő hozzáférés általánossá tétele érdekében a keretszabályozás felülvizsgálatának eredményeként az új szabályozási alapokra. Továbbra is a tagállamok a rádióspektrum-vagyon tulajdonosai, de joggyakorlásuk kereteit az unió egyre szélesebb körben, egyre nagyobb mértékben egységesíti a beruházásvédelem, a fogyasztói jogok kiterjesztése érdekében, valamint a méretgazdaságosság jegyében. A tagállami körülmények mind piaci, mind jogi szempontból eltérőek, így az azokhoz illeszkedő harmonizált szabályok kialakítása, a közös minimum megtalálása állt a viták középpontjában. A témakör kiemelt jellegét mutatta az is, hogy a Bizottság szövegjavaslatának tematikus tárgyalása a spektrum témakörével kezdődött. A spektrumpolitikai kérdésekben született megállapodás volt az első az intézmények között.

Jelen cikk az elfogadott szabályozás spektrummal összefüggő lényeges elemeinek a tagállamok rádióspektrum-gazdálkodására gyakorolt hatásának áttekintésére törekszik, különösen azon szabályozási elemekre fókuszálva, melyek a frekvenciafelhasználókat érintik, nem elemezve a hatásköri szabályokat és az intézményrendszeren belüli munkamegosztási kérdéseket.

A Bizottság a következő gondolatokkal indokolta szabályozási javaslatát 2016. szeptemberében. Az elektronikus hírközlési szolgáltatásokhoz fontos erőforrás a rádióspektrum, mely iránt a piaci szereplők érdeklődése egyre fokozottabb, sőt az érdeklődői kör is fokozatosan bővülő. Az eddigi végfelhasználók egy része maga is frekvencia-felhasználói pozícióra törekszik. Az 5G megvalósításához további frekvenciák szükségesek. A spektrum uniós szintű, időben történő rendelkezésre bocsájtását célozta a Bizottság a spektrumgazdálkodás célirányos fejlesztésével. A cél az egyszerűsített szabályozási beavatkozással a tagállamok közötti nagyobb összhang és kiszámíthatóság biztosítása volt. A befektetések biztonsága érdekében hosszú távú engedélyekre van szükség. A hosszú érvényességi időtartam kiszámíthatóságot biztosít a befektetőknek, ezzel is elősegítve a fejlettebb hálózatok építésének gyorsaságát. A Bizottság azt is megcélozta, hogy az egyedi engedélyek módosításának feltételeit csak az érdekeltekkel történt egyeztetést követően lehessen megtenni. A díjazás szabályozásának módosításával is a befektetési biztonság növelése volt a cél.

A Rádióspektrum Politikai Csoport (Radio Spectrum Policy Group, a továbbiakban: RSPG[3]) intézményén keresztül kívánta a Bizottság a tagállamok közötti együttműködést erősíteni, így a spektrumpolitikák, spektrumgazdálkodási stratégiák RSPG keretei közötti összehangolásának, valamint az RSPG meglevő jószolgálati tevékenységének irányelvi szintű szabályozását kezdeményezte a Bizottság. A tagállami értékesítési eljárásainak kontrolljára tett javaslatot a Bizottság a Peer Review (Szakértői áttekintő) eljárás bevezetésével.

1 *Európai Bizottság – Sajtóközlemény: Az Unió helyzete 2016-ban: a Bizottság megteremti a feltételeit annak, hogy növekedjen a polgárok és a vállalkozások rendelkezésére álló internetkapcsolatok száma és minősége, Strasbourg, 2016. szeptember 14. europa.eu/rapid/press-release_IP-16-3008_hu.pdf*

2 *676/2002/EK határozat (rádióspektrum-határozat), 622/2002/EK határozat (rádiófrekvencia-politikával foglalkozó csoportra vonatkozó határozat), valamint a többéves rádióspektrum-politikai program létrehozásáról szóló 243/2012/EU határozat.*

3 *RSPG: Radio Spectrum Policy Group – Rádióspektrum Politikai Csoport. (A rádiófrekvencia-politikával foglalkozó csoport létrehozásáról szóló 2002. július 26-i 622/2002/EK bizottsági határozattal létrehozott Rádióspektrum Politikai Csoport (RSPG) tanácsadói minőségben a rádióspektrum európai stratégiai kérdéseivel foglalkozik.)*

2. Spektrumpolitikai célok az új Kódex-beli szabályokkal

A spektrumhasználat és gazdálkodás határokon átnyúló vonatkozásai, a méretgazdaságossági szempontok miatt, a belső piacra gyakorolt széles körű hatásokkal összefüggésben erősebb, szélesebb körű uniós szintű koordinációs eljárások váltak szükségessé. A harmonizáció mélysége és köre azonban éles vitát váltott ki az uniós döntéshozatal során.

A szabályozás egyik indoka az 5G volt, az 5G mihamarabbi megvalósításában Európa vezető szerepének biztosítása. A szabályozási csomagnak csak egyik eleme volt az Európai Elektronikus Hírközlési Kódex (a továbbiakban: Kódex[4]), mely mellett a „Gigabit társadalom" kezdeményezés[5] és az 5G cselekvési terv[6] is megjelent. Az 5G Cselekvési tervben a Bizottság mérföldköveket határozott meg, például hogy 2018-ra minden uniós tagállamon belül legalább egy nagyvárosban elérhető legyen az 5G, valamint hogy 2020-ban történjen meg a kereskedelmi 5G szolgáltatás meghirdetése, továbbá hogy 2025-re a városokban, valamint a főbb közlekedési útvonalak mentén és vasútvonalakon legyen folytonos 5G-lefedettség. A Kódex szabályozási keretei között a tagállamok alakíthatják nemzeti spektrumgazdálkodási politikáikat, eljárásaikat. Abban minden szabályalkotásban érdekelt fél egyetértett, hogy a befektetőknek kiszámítható szabályozási környezetet kell biztosítani a magas színvonalú és nagy sebességű, vezeték nélküli széles sávú internet-lefedettség elérése érdekében, a lehető legkevesebb terhet okozó engedélyezési rendszer választása mellett.

A Kódex alapelvi szinten nem hozott változást, azaz továbbra is a technológiasemlegesség mellett tört pálcát az uniós döntéshozatali rendszer. De megszületett a Kódex 54. cikke, melynek már a címe is („A frekvenciaelosztás időbeli összehangolása konkrét 5G-frekvenciasávok esetében") szakít a technológiasemlegesség elvével és nevesíti az 5G-t, ami mindenképpen kötöttséget jelent, ha nem is nevez meg konkrét technológiát. Egy irányelvi szintű, eljárási szabályozási alapokat lefektető jogforrásban, konkrét frekvenciasávokkal (3400–3800 MHz, valamint 26 GHz) kapcsolatos 5G-célok kerültek rögzítésre, melyek ráadásul azonnal hatályba lépnek. A Kódexbeli 5G-intézkedések alapján a tagállamoknak minden szükséges intézkedést meg kell tenniük annak érdekében, hogy 2020 végéig a frekvencia-felhasználók részére rendelkezésre bocsássák az RSPG által azonosított 5G úttörő sávokat, azaz azon frekvenciasávokat, melyek esetében az 5G felhasználását lehetővé tevő műszaki harmonizált szabályok megalkotása leghamarabb történik meg a nemzetközi szervezetekben. A 3400–3800 MHz-es sáv esetén a defragmentáció megszüntetése, azaz a nagy egybefüggő, 5G-re felhasználható spektrum rendelkezésre állása érdekében kell az elsődleges lépéseket megtenni. A 26 GHz-es frekvenciasáv vonatkozásában a tagállamoknak a piaci igényekre tekintettel legalább 1 GHz használatát kell lehetővé tenni, amennyiben meglevő felhasználók migrációjának, illetve a sáv felszabadításának nincs jelentős akadálya.

3. Változatlan uniós rádióspektrum-szabályozási elemek

A Bizottság 2016-ban rögzítette, hogy a szabályozási csomag nem érinti a következő uniós jogi aktusokat:

- 676/2002/EK határozat (a továbbiakban: Rádióspektrum-határozat)[7],
- 2002/622/EK határozat (rádiófrekvencia-politikával foglalkozó csoportra vonatkozó határozat)[8], és
- a többéves rádióspektrum-politikai program létrehozásáról szóló 243/2012/EU határozat[9].

A Rádióspektrum-határozat alapján 2016-ban hivatalosan is elindult az 5G megvalósítását, azaz az új generációs mobil szolgáltatások megvalósítását szolgáló harmonizációs folyamat. Az 5G-sávokra vonatkozó első EU-mandátumot[10] a Bizottság 2016 végén bocsátotta ki. A Mandátummal a Bizottság felkérte a CEPT-et[11], hogy tanulmányozzák a dokumentumban megadott sávokra vonatkozóan az 5G bevezethetőségét, figyelembe véve a jelenlegi felhasználásokat. A folyamat eredményeként 2019 első hónapjaiban jelenhet meg a 3400–3800 MHz-es frekvenciasávra vonatkozó új, az 5G megvalósítását is lehetővé tevő harmonizált szabályozás. Az RSPG jelenleg már a defragmentáltság és a vertikumok kérdéseivel foglalkozik. 2020 végéig teszik meg a tagállamok a szükséges lépéseket a sáv rendelkezésre állásának biztosítása érdekében, míg a Kódexben szabályozott intézkedések tagállami jogrendbe építésére 24 hónap áll a tagállamok rendelkezésére.

Így ugyan a Kódex egyik indikátora az 5G mihamarabbi bevezetése érdekében szükséges keretek megalkotása volt, de az úttörő sávok rendelkezésre bocsátása a meglevő, jelenleg hatályos szabályok között valósul meg a tagállamok többségében *(1. ábra)*.

4 Az Európai Parlament és Tanács 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (HL L 321, 2018.12.17., 36.o.).

5 Bizottsági közlemény (összefoglaló keretdok.): "Connectivity for a Competitive Digital Single Market – towards a European Gigabit Society" – Az összekapcsoltság a versenyképes digitális egységes piac szolgálatában: úton a gigabitalapú európai információs társadalom felé c. bizottsági közlemény, COM(2016) 587 végleges.

6 Bizottsági közlemény (cselekvési terv): "Action Plan Communication and Staff Working Document: 5G for Europe" – 5G Európa számára c. cselekvési tervről szóló bizottsági közlemény, COM(2016) 588 végleges.

7 Az Európai Parlament és a Tanács 676/2002/EK határozata (2002. március 7.) az Európai Közösség rádióspektrum-politikájának keretszabályozásáról (rádióspektrum-határozat) (HL L 108., 2002.4.24. 1.o.).

8 A Bizottság 2002. július 26-i 2002/622/EK határozata (2002. július 26.) a rádiófrekvencia-politikával foglalkozó csoport létrehozásáról (HL L 198., 2002.7.27., 49.o.).

9 Az Európai Parlament és a Tanács 243/2012/EU határozata (2012. március 14.) egy többéves rádióspektrum-politikai program létrehozásáról (HL L 81., 2012.3.21., 7.o.).

10 https://ec.europa.eu/digital-single-market/en/news/radio-spectrum-cept-mandates-0

11 CEPT: Conf. européenne des Administrations des postes et des télécommunications – Postai és Távközlési Igazgatások Európai Értekezlete

4. Változó keretszabályok

Számos új, a frekvenciafelhasználással összefüggő szabályozási módosítás történt a spektrumgazdálkodás területén. A leglényegesebb változások a *2. ábrán* tekinthetők át.

4.1. A versenyeztetési eljárás által elérni kívánt célok listája

A versenyeztetési eljárások (árverés, pályázat) kapcsán a Kódex 55. cikkében foglalt rendelkezések jelentenek keretszabályokat a tagállamok számára. Abban az esetben, ha valamely tagállam a használati jogok számát korlátozza, meg kell határozza a versenyeztetési eljárás által elérni kívánt célokat. A célokat, amennyiben lehetséges, számszerűsített adatokkal kell megfoghatóvá tenni az új szabályozás alapján. A tagállam által választható célok jegyzékét is rögzíti a Kódex, ezek között a versenyélénkítés mellett szerepel:

a) a lefedettség előmozdítása;
b) szolgáltatás elvárt minőségének biztosítása;
c) a rádióspektrum hatékony használatának ösztönzése, többek között figyelembe véve a használati joghoz kapcsolódó feltételeket és a díjak szintjét;
d) innováció és a vállalkozásfejlesztés elősegítése.

4.2. A frekvenciaelosztási eljárások időbeli összehangolása

A tagállami frekvenciaelosztási eljárások időbeli összehangolását szolgálja a Kódex 53. cikke. A jelenleg hatályos uniós jogforrások alapján egyrészt a Rádióspektrum-határozat alapján alkotott harmonizációs szabályokat rögzítő döntések tartalmaztak kijelölési és rendelkezésre bocsájtási határidőket. Másrészt a többéves rádióspektrum-politikai program létrehozásáról szóló 243/2012/EU határozat rögzített engedélyezési eljárások lefolytatására vonatkozó határidőket. E mellett a 700 MHz-es frekvenciasáv vonatkozásában született parlamenti és tanácsi határozat[12], mely a jelenleg műsorszórásra használt teljes 470–790 MHz sáv további felhasználására, valamint a 700 MHz-es frekvenciasáv műsorszórástól eltérő elektronikus hírközlési szolgáltatási célú felhasználására tartalmazza a tagállami kötelezettségeket, határidőkkel.

Az 53. cikk alapján általános szabály került megalkotásra azon frekvenciasávok felhasználására, melyeket uniós szinten harmonizálták elektronikus hírközlési hálózatok és elektronikus hírközlési szolgáltatások céljaira. A Rádióspektrum-határozat alapján harmonizált frekvenciasávok használatát a lehető leghamarabb lehetővé kell tenni az új előírásoknak megfelelően, azaz a tagállamnak meg kell tenni minden olyan intézkedést, ami a használathoz szükséges, beleértve a jogalkotást, sávkiürítést, engedélyezési, vagy akár versenyeztetési eljárás lefolytatását. A tagállamoknak az említett harmonizációs döntés elfogadását követően legfeljebb 30 hónap áll rendelkezésükre ezen lépések megtételére. Kivételes esetben ez a határidő 30 hónappal meghosszabbítható.

A meghosszabbítás taxatív feltételei között két eset szerepel. Az egyik a megoldatlan, határövezeti koordinációs probléma. Azonban ennek is vannak további peremfeltételei. A tagállamok között káros zavarást kell, hogy eredményezzen ez a megoldatlan koordinációs probléma, valamint a tagállamnak a koordinációra vonatkozó valamennyi Kódexbeli szükséges intézkedést időben meg kell hoznia. A másik határidő-hosszabbítást lehetővé tevő eset, ha a szóban forgó frekvenciasáv meglévő felhasználóinak műszaki migrációját is biztosítania kell a tagállamnak, és ez összetett feladat. Egy további kivételes eset is nevesítésre került a Kódex intézkedései között, amikor is a tagállamban a harmonizált szabályok helyett mást alkalmaznak, mégpedig az alternatív felhasználás.

Az alternatív felhasználás részletes szabályai a Kódex 45. cikkében találhatók. A nemzeti sajátosságokat elismerő intézkedésről van szó. Ebben az esetben a harmonizált döntés ellenére egyes tagállamokban kivételesen nem történik meg a harmonizált használat bevezetése. Ez azonban csakis akkor fordulhat elő, ha tagállami vagy regionális szintű piaci kereslet hiánya áll fenn,

1. ábra
Az 5G-hez szükséges frekvenciák elosztásának és a Kódex implementálásának időbeli áttekintése

2. ábra
A Kódexben található, spektrumhasználattal összefüggő, lényegesebb új szabályok áttekintése

12 *Az Európai Parlament és a Tanács (EU) 2017/899 határozata (2017. május 17.) a 470–790 MHz frekvenciasáv Unión belüli használatáról (HL L 138., 2017.5.25., 131.o.).*

akár az érintett sáv egésze vagy egy része szempontjából. Az alternatív felhasználásba beletartozik a harmonizáció időpontjában a tagállamban már meglévő felhasználás is. Az alternatív felhasználás feltételei a következők:

a) a sáv használata iránti piaci kereslet hiányának megállapítása nyilvános konzultáció alapján történik;
b) a szóban forgó alternatív felhasználás nem hiúsítja meg, és nem akadályozza más tagállamokban a sáv rendelkezésre állását, illetve használatát; valamint
c) az érintett tagállam kellően figyelembe veszi a harmonizált sáv hosszú távú rendelkezésre állását és használatát az Unióban, valamint a berendezésekre vonatkozóan a rádióspektrum uniós szinten való használatából eredő méretgazdaságosságot.

4.3. Engedélyezési időtartam

A hosszú távú beruházások előmozdítása érdekében a tagállamok kötelezettsége, hogy kiszámíthatóságot és következetességet biztosítsanak a rádióspektrum-használati jogok megadása, megújítása, módosítása, korlátozása és visszavonása tekintetében. Ennek egyik leglényegesebb eleme, hogy egyedi engedélyezéssel elérhető, vezeték nélküli szélessávú elektronikus hírközlési szolgáltatásokra használható, harmonizált sávok esetében a tagállamok 20 évre kötelesek a szabályozási kiszámíthatóságot biztosítani a jogosultak számára.

A Kódex alapján a jogok legalább 15 évig érvényesek kell, hogy legyenek, lehetővé téve a meghosszabbítást is, melynek legrövidebb időtartama 5 év. Hazánkban a nemzeti vagyonról szóló törvény 2011. évi CXCVI. törvény alapján legfeljebb 15 éves határozott időre lehet a nemzeti vagyont hasznosítani, amely időszak egy alkalommal legfeljebb 5 évvel meghosszabbító. Az uniós minimumszabályok és a hazai maximumszabályok azonosak, azaz a frekvenciaversenyeztetési eljárás során hasznosított frekvenciasávok esetében a jogosultság időtartamának meghatározására nem sok mozgástere marad a hazai szabályozónak a jelenlegi szabályozási környezetben.

4.4. Megújítás lehetősége

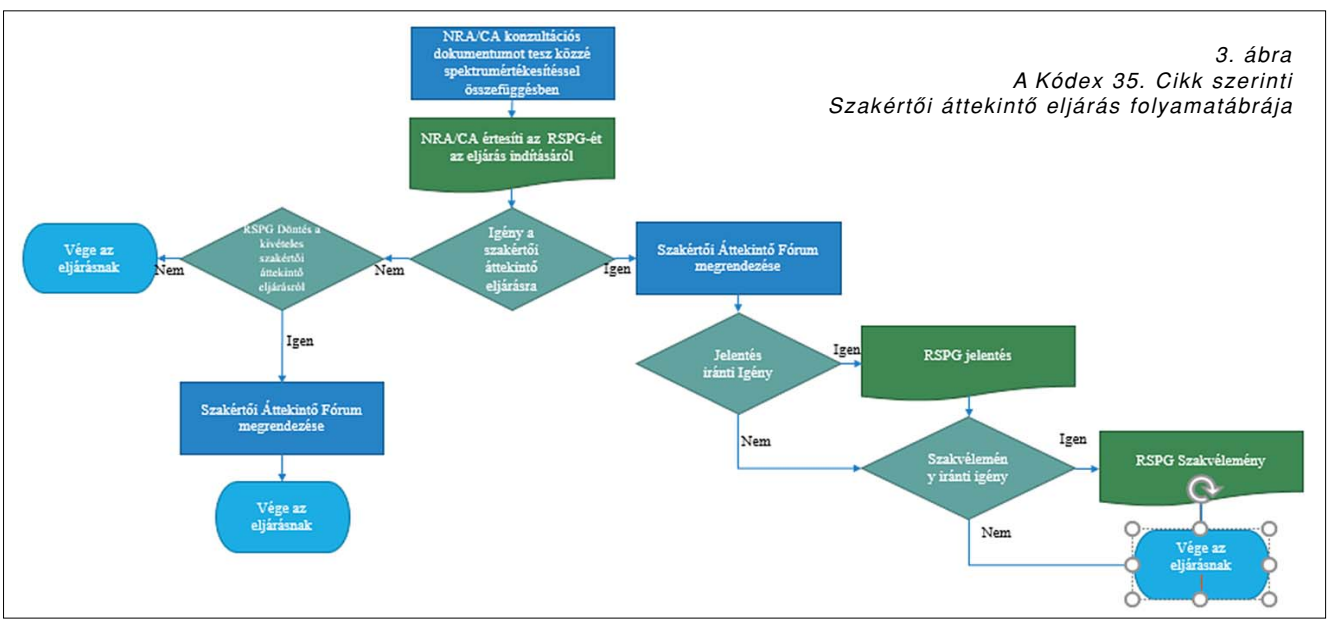
A Kódex szabályai alapján a meghosszabbítás mellett a megújítás jogintézménye is megjelenik. A jelenlegi ágazati szabályok ilyen lehetőséget nem említenek. Az uniós szabályozás alapján mindkét esetben meglevő jog érvényességi ideje egészül ki további időtartammal, de annak feltételei, eljárási szabályai nem teljesen azonosak. Az egybeesések jelentős kihívás elé állítják majd a hazai jogrendbe emelésen dolgozó szakértőket. A megújítás megjelenése mindenesetre további befektetésvédelmi eljárásnak tekinthető.

4.5. Díjazási szabályok

A Kódex szabályai között az igazgatási díjak mellett továbbra is megjelennek a közjavak, mint a rádióspektrum hasznosításáért fizetendő díjak is. Magában a díjstruktúrában tehát nem történt változás. Az Európai Unió Bírósága már kialakult ítélkezési gyakorlata értelmében a tagállamok a Kódexben meghatározottakon túlmenően semmilyen más díjat nem szabhatnak ki a hálózatok üzemeltetéséért és az elektronikus hírközlési szolgáltatások nyújtásáért. A rádióspektrum hasznosításáért fizetendő díjak az optimális felhasználás biztosítása érdekében vethetők ki. A rádióspektrumra vonatkozó díjak szabályozásában új elem a minimumdíjak kiemelése a meglevő díjstruktúrából. A minimumdíjakkal kapcsolatban a tagállamoknak tekintettel kell lenni az alternatív felhasználás lehetőségére.

4.6. Peer review, azaz szakértői áttekintő eljárás

A Peer review Platformot a tagállamokban dolgozó, spektrumértékesítéssel foglalkozó szakértőinek tapasztalatcseréje érdekében alakította ki az RSPG még 2015-ben. A Peer review Platform egyrészt egy webes felület, másrészt workshopok sorozata. A workshop-ok alkalmával a szakértők személyesen is találkoznak egymással, és megosztják tapasztalataikat, terveiket egymás között, egyrészről a már lezajlott értékesítésekről, másrészt beszámolnak terveikről. A webes felület lehetőséget biztó-



3. ábra
A Kódex 35. Cikk szerinti
Szakértői áttekintő eljárás folyamatábrája

sít a már publikált tagállami dokumentumok megosztására, valamint kommunikációs felület (chat), ahol a szakértők információt oszthatnak meg egymással. Különösen értékesítések kapcsán felmerülő kérdések esetén biztosít lehetőséget a többi tagállami szakértő véleményének, tapasztalatainak megismerésére. Központban az értékesítési eljárásokkal kapcsolatos közös gondolkodás fejlesztése, a tanulás és a felhalmozódott ismeretanyag megosztása áll.

A Kódex egyik új hangsúlyos intézkedése a Peer review, azaz a Szakértői áttekintő eljárás (35. Cikk), amely a tagállami spektrumértékesítési eljárások folyamatába beépülő, alapvetően önkéntes eljárás. Az új szabályozásra tekintettel szükség lesz az RSPG-gyakorlat, -szabályozás átalakítására. Eredetileg a Bizottság ezzel tervezte harmonizálni a versenyeztetési eljárásokat, azonban a politikai alkuk eredményeként az eredeti cél is átalakult. Alapvetően a kiválasztási eljáráshoz kapcsolódó intézkedéstervezetről való tapasztalatcsere, illetve a bevált gyakorlatok megosztása az új eljárás lehetséges célja, ezzel is közelítve a tagállami eltérő eljárásokat, amely azonban nem jelenthet adminisztratív terhet. Kivételes esetben, az RSPG által előre meghatározott kritériumok teljesülése esetén RSPG kezdeményezésére is sor kerülhet az eljárásra.

Jelenleg kritériumként a kezdeményező tagállamok minimális számának meghatározásán dolgozik az RSPG Kódexért felelős munkacsoportja. Az RSPG a Kódexből eredő új szabályok, feladatok RSPG-re gyakorolt hatását vizsgáló munkacsoportja a WG EECC. Ez a munkatervi pont szerepel az 2018. januárjában véglegesített RSPG-munkatervben. A munkacsoport javaslata alapján az RSPG hazánkra is jelentős kérdésekben alakít ki közös értelmezést az uniós tagállamok között, illetve ez alapján fogalmaz meg ajánlásokat, javaslatokat az Európai Bizottság részére. A *3. ábra* szemlélteti a Szakértői áttekintő eljárás folyamatát.

4.7. RSPG jószolgálat

Az RSPG jószolgálati munkacsoportja a legrégebben működő munkacsoport. Az érintett tagállamok felkérésére a határövezeti frekvenciakoordinációs problémákkal foglalkozik. A mobil felhasználás 800 MHz-es frekvenciasávban történő bevezetése okozott nehézségeket egyes tagállamokban szomszédos tagállambeli műsorszóró felhasználás miatt. Ezekben a koordinációs egyeztetésekben játszott eredményesen mediátor szerepet az RSPG. A megoldás azonban jelentős erőfeszítéseket igényel és időben hosszasan elnyúlt. Így egy tagállam, nevezetesen Olaszország problémája öt másik tagállamot hátráltatott, azaz dominóhatást gyakorolva késleltette a harmonizált használat összeurópai bevezetését.

Ezen tapasztalaton okulva, a Kódexben már szerepel annak a lehetősége, hogy harmonizált, szélessávra is használható frekvenciasávok esetén, amennyiben valamely tagállam káros zavart okozva hátráltat egy másik tagállamot, és nem sikerül a szabályozás adta egyéb segítségekkel sem megtalálni a megoldást, a Bizottság a vita feloldására, a káros zavarás megszüntetése érdekében az érintett tagállamokat kötő határozatot hozhat. Azonban a Bizottság döntéshozatalának számos feltétele van. Így csak akkor járhat el a Bizottság, ha azt az érintett tagállam kéri. Az érintett tagállam is először a megszokott egyeztetési utakat köteles igénybe venni és csak azok eredménytelensége esetén veheti igénybe ezt a segítséget. A határozathozatal során a Bizottság a lehető legnagyobb mértékben figyelembe kell, hogy vegye az RSPG összehangolt megoldást javasló véleményét, amennyiben az rendelkezésre áll. A határozat címzettjei a megoldatlan káros zavarás problémája által érintett tagállamok lehetnek.

A 700 MHz-es frekvenciasávban a műsorszórás leállítása és vezeték nélküli szélessávú elektronikus hírközlési szolgáltatás bevezetése érdekében szükséges spektrum rendelkezésre bocsájtásának határideje 2020 júniusa. Magyarország földrajzi fekvésénél fogva nincs egyszerű helyzetben, így ugyan másik tagállam miatt nem várható Bizottsági határozathozatal, de nem uniós tagállamok frekvenciafelhasználása miatt, uniós aszszisztenciára még szükség lehet, annak érdekében, hogy az ország teljes területén mihamarabb elérhető legyen az 5G szolgáltatás.

5. Összefoglalás

Összességében megállapíthatjuk, hogy ugyan forradalmi változást nem hozott a Kódex a rádióspektrum-gazdálkodás területén, de az új szabályok, a jelenleg hatályos előírásokhoz képest történt módosítások hosszú távon javíthatnak is a befektetők helyzetén. Azt egyértelműen kijelenthetjük, hogy az 5G mihamarabbi bevezetésében nem játszik kritikus szerepet a Kódex és annak nemzeti jogrendbe építése, viszont hosszú távon kedvezően befolyásolja a vezeték nélküli elektronikus hírközlési szolgáltatásokhoz szükséges rádióspektrum használatát. Ha nem is kizárólag a Kódex eredményeként, de azzal mindenképpen összefüggésben növekszik a tagállamok közötti együttműködés spektrumpolitikáik megalkotása, stratégiai céljaik meghatározása során, különösen a mobil szolgáltatásokra felhasználható frekvenciasávok esetén, elismerve a nemzeti piacaik sajátosságait.

A szerzőről

DR. ULELAY EMILIA a Nemzeti Média- és Hírközlési Hatóság Frekvencia- és Azonosítógazdálkodási Főosztályának főosztályvezető-helyettese. A hírközlési ágazat szabályozásával 1998 óta foglalkozik jogászként. A HIF Jogszabályelőkészítő főosztályán kezdte pályafutását. 2003 óta köteleződött el a spektrumgazdálkodás mellett.
A hazai állami frekvenciagazdálkodási feladatok közül a stratégia- és jogszabály-alkotási munkákban aktív. A nemzetközi szervezetek közül a CEPT ECC (Európai Hírközlési Bizottság) az EU spektrumszabályozás területén működő kommitológiai bizottságában, a Rádióspektrum Bizottságban (Radio Spectrum Committee, RSC), valamint a Bizottság magas szintű tanácsadó csoportjában, a Rádióspektrum Politikai Csoportban (Radio Spectrum Policy Group, RSPG) képviseli a magyar érdekeket. Az RSPG 2018. évi és azt követő időszakára elfogadott munkatervben az EECC (Európai Elektronikus Hírközlési Kódex) munkatervi pont három felelős „előadójának" (társ-rapportőreinek) egyike.

A végfelhasználók jogai az új Európai Elektronikus Hírközlési Kódexben

KOVÁCS ANITA
Telenor Magyarország Zrt.
AnitaKovacs@telenor.hu

Kulcsszavak: elektronikus hírközlési ágazat keretszabályozása, Európai Elektronikus Hírközlési Kódex, kommunikációs szolgáltatások új definíciója

Legkésőbb 2020 végétől az elektronikus hírközlési szolgáltatások magyarországi végfelhasználói, az ezeket nyújtó vállalkozások, valamint a hírközlési ágazatot felügyelő szabályozó hatóságok jogait és kötelezettségeit egy, a mostanihoz képest nem teljesen új, de sok tekintetben jelentős változásokat tartalmazó szabályrendszer alakítja majd.
Ez az új szabályrendszer a 2018 decemberében hatályba lépett Európai Elektronikus Hírközlési Kódexből fakad, ami fenntartja és modernizálni kívánja az iparágra vonatkozó jelenlegi EU-s keretszabályozást. A Kódex fogyasztóvédelmi fejezete, a végfelhasználók jogait körülíró rendelkezések legfontosabb újdonsága az elektronikus hírközlési szolgáltatások definíciójának újragondolása, kiterjesztése az ún. OTT kommunikációs szolgáltatásokra, illetve az ún. maximum harmonizációs megközelítés. Több-kevesebb újdonság található az elektronikus hírközlési szolgáltatások igénybevételéről a végfelhasználókkal kötött szerződésekre vonatkozó tájékoztatási követelményekre, a szolgáltatások tarifáinak és egyéb feltételeinek átláthatóságára, a szolgáltatásminőségre, a szolgáltatóváltást elősegítő előírásokra, a segélyhívási célú kommunikációra vonatkozó előírásokban is. A cikk ezekről a változásokról kíván rövid áttekintést nyújtani.

1. Bevezetés

Közel négy éves európai szintű jogalkotási folyamat eredményeként 2018. december 17-én megjelent az Európai Unió Hivatalos lapjában és hatályba lépett az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról. A következőkben a jogszabályt Hírközlési Kódexként vagy egyszerűen Kódexként fogjuk említeni, ahogy előreláthatóan így hivatkoznak majd rá a vele kapcsolatos szakmai, jogi diskurzusok és tevékenységek során. Az elkövetkezendő hónapokban számtalanszor felbukkan majd a magyarországi elektronikus hírközlési szektor szereplőinek életében a jogszabály, különösen azokéban, akik részt vesznek annak hazai jogrendszerbe történő átültetésében, amelyre két év áll rendelkezésre. Legkésőbb 2020 végétől a Kódexen alapuló szabályok pedig jelentős részben alakítják majd az elektronikus hírközlési szolgáltatatást nyújtó vállalkozások, a felhasználók és a hírközlés iparágat felügyelő szabályozó viszonyrendszerét, jogait és kötelezettségeit az elektronikus hírközlési szolgáltatásokkal összefüggésben.

A Hírközlési Kódex, illetve az ennek majdani magyarországi megfelelője nem eredményez majd a jelenlegihez képest teljesen új szabályozást. Az Európai Unió jogszabály-előkészítő intézményének, az Európai Bizottságnak az ambíciója és mandátuma a 2015–2019-es hivatali időszakban e vonatkozásban arra terjedt ki, hogy értékelje, vajon az elektronikus hírközlésre vonatkozó, eredetileg 2002-ben elfogadott, majd legutóbb 2009-ben felülvizsgált európai keretszabályozás továbbra is megfelelően szolgálja-e fő célkitűzéseinek megvalósulását, netán azonosíthatók-e abban kiküszöbölendő hiányosságok, ellentmondások vagy egyszerűsítési lehetőségek.

Vegyük számba, pontosan mire is terjedt ki és mire nem ez a felülvizsgálat. Magától értetődő módon érintve voltak az eddig érvényben lévő keretszabályozás gerincét alkotó legfontosabb jogforrások, nevezetesen az ún. Keretirányelv [1], az Engedélyezési irányelv [2], Hozzáférési irányelv [3], Egyetemes szolgáltatási irányelv [4], valamint a BEREC rendelet [5], továbbá a Rádióspektrum-határozat [6], a Határozat RSPG létrehozásáról [7], végül az RSPP [8].

A kimaradtak köréből feltétlenül említést érdemel az Elektronikus hírközlési adatvédelmi irányelv [9], melynek felülvizsgálatával a jogalkotók meg akarták várni, amíg az általános adatvédelmi rendelet (közismert nevén a GDPR [10]) megalkotása lezárul. A hírközlési adatvédelmi irányelv kétségtelenül szintén indokolt felülvizsgálatának folyamata nagyrészt a számos fontos vitás kérdés felmerülésének köszönhetően időközben jelentős késedelmet mutat. Így kérdésessé válhat akár az is, hogy legalább a Hírközlési Kódex nemzeti jogba történő átültetésének 2020. december 21-ei határidejére lesze kifejezetten az elektronikus hírközlési szolgáltatások nyújtásával összefüggő személyes adatkezelésre vonatkozó új szabályozás, vagy marad a jelenleg is hatályos „régi” normarendszer. Mivel – ahogy azt később részletesen bemutatjuk –, az elektronikus hírközlési szolgáltatások körét a Kódex kibővíti az ún. over-the-top vagy OTT kommunikációs szolgáltatásokkal, érdekes helyzetet eredményezhet, amennyiben ezzel az alapvetően még távközlésre kitalált követelményekkel a digitális szolgáltatók is – legalább átmeneti ideig – szembetalálják magukat.

Végezetül a teljesség kedvéért álljon még itt, hogy ugyancsak nem foglalkoztak ebben a folyamatban a jogalkotók a roaming-rendelettel [11], a netsemlegességet biztosító rendelettel [12], illetve a nagy sebességű elektronikus hírközlő hálózatok kiépítési költségeinek csökkentését célzó irányelvvel [13], mégpedig azért, mert a hatályba lépésük, illetve alkalmazásuk kezdete óta eltelt idő ezt még nem indokolta.

2. Az elektronikus hírközlési szolgáltatások végfelhasználóit megillető jogokra vonatkozó új szabályok

2.1. Általános célok

Az általános áttekintés után a cikk hátralévő részét egyetlen terület részletesebb bemutatásának szenteljük, nevezetesen annak, hogy miként szabályozza a Kódex az elektronikus hírközlési szolgáltatások végfelhasználóit megillető jogokat. Az az általános célkitűzés, amelynek érdekében az európai jogalkotók indokoltnak látják, hogy meghatározzanak bizonyos felhasználói jogokat, változatlan formában él tovább az új jogszabályban is: az Európai Unió ezen ágazatspecifikus fogyasztóvédelmi szabályok révén kíván gondoskodni a végfelhasználók egységesen magas szintű védelméről, hozzájárulva ezzel az uniós polgárok érdekeinek védelméhez.

Ezek az ágazatspecifikus fogyasztóvédelmi szabályok a következő tárgykörökbe tartozó előírásokat fedik le: az elektronikus hírközlési szolgáltatások igénybevételéről a végfelhasználókkal kötött szerződésekre vonatkozó tájékoztatási követelmények, a szolgáltatások tarifáinak és egyéb feltételeinek átláthatósága, szolgáltatásminőség, a szolgáltatóváltást elősegítő előírások (ideértve a számhordozhatóságot is), segélyhívási célú, illetve vészhelyzeti kommunikáció, továbbítási kötelezettség meghatározott rádió- és televízióműsor-terjesztő szolgáltatások továbbítására (ún. must carry).

Mielőtt belebocsátkoznánk az e tárgykörökbe tartozó rendelkezések, módosítások ismertetésébe, feltétlenül ki kell térni arra a két dologra, ami a Hírközlési Kódex legnagyobb újdonsága a végfelhasználói jogok eddigi szabályozásához képest. Az egyik e szabályok tárgyi hatályában, a másik pedig a harmonizáció szintjében bekövetkező változás. Mindkét kérdés jelentős viták tárgya volt a Kódex előkészítése során.

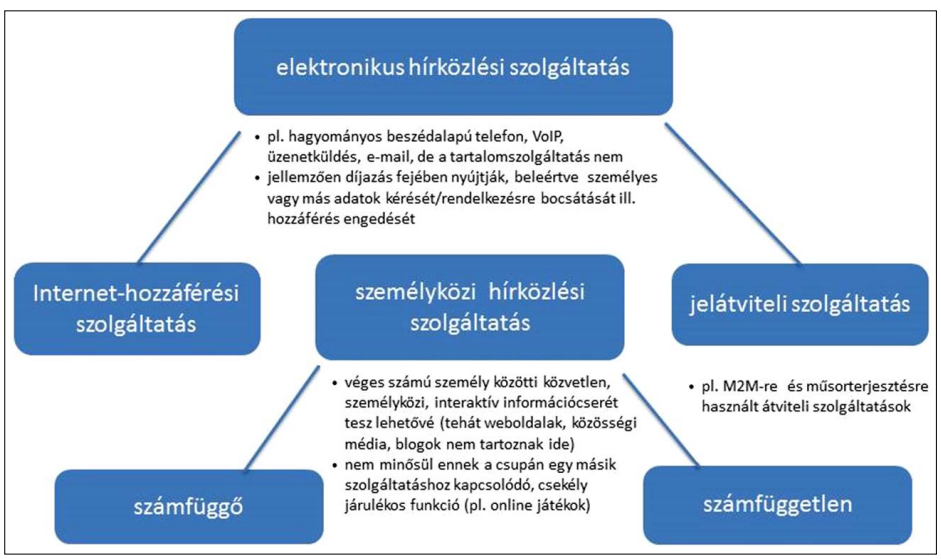
2.2. Az elektronikus hírközlési szolgáltatások új definíciója

Ezidáig az elektronikus hírközlési szolgáltatások nélkülözhetetlen paramétere volt a jelátvitel, kizárólag a teljes egészében vagy részben jeltovábbításból álló szolgáltatások tartoztak a hírközlési szabályozás hatálya alá.

A Kódex megalkotásának idejére azonban már megkerülhetetlenné vált az a tény, hogy a végfelhasználók a hagyományos telefonszolgáltatás és a szöveges üzenetek helyett mindinkább ezekkel funkcionálisan egyenértékű online szolgáltatásokat – például VoIP-szolgáltatásokat (pl. Skype), üzenetküldési szolgáltatásokat (Viber, Whatsapp, Messenger stb.), valamint webalapú e-mail-szolgáltatásokat – használnak kommunikációs célra és a végfelhasználó szempontjából nem releváns, hogy a szolgáltató maga végzi-e a jelátvitelt, vagy a kommunikáció internet-hozzáférési szolgáltatáson keresztül valósul meg (ún. over-the-top jelleggel) [14].

Márpedig amennyiben megfelelően érvényesíteni kívánjuk a szektorális fogyasztóvédelmi szabályozás alapvető célkitűzését, a végfelhasználók hatékony és ugyanolyan szintű védelmét, akkor az megköveteli e védelem hatályának kiterjesztését a funkcionálisan egyenértékű kommunikációt lehetővé tevő szolgáltatásokra. Ezt belátva, a Kódex kiterjesztette az elektronikus hírközlési szolgáltatás fogalmát úgy, hogy abba a teljes egészében vagy nagyrészt jeltovábbításból álló szolgáltatások típusa mellett immár beletartozik az ún. személyközi hírközlési szolgáltatások típusa, valamint az internet-hozzáférési szolgáltatás.

Az internet-hozzáférési szolgáltatás fogalma az (EU) 2015/2120 rendelet 2. cikkének (2) bekezdésében foglalt meghatározásnak megfelelő, tehát ezen értendő az a nyilvánosan elérhető elektronikus hírközlési szolgáltatás, amely internetcsatlakozást és ezáltal az internet lényegében valamennyi végpontjával összekapcsolási lehetőséget biztosít, tekintet nélkül az alkalmazott hálózati technológiára és a használt végberendezésre. A személyközi hírközlési szolgáltatások pedig olyan szolgáltatások, amelyek személyek közötti közvetlen, interaktív információcserét tesznek lehetővé elektronikus hírközlési hálózatokon, nem csupán kiegészítő funkcióként, kizárólag a kommunikáció küldője által meghatározott, véges számú, azaz nem potenciálisan korlátlan számú természetes személy között, akár számozási tervben szereplő hívószámokkal, vagy hívószámokhoz való



kapcsolódás segítségével (számfüggő személyközi hírközlési szolgáltatások), vagy nem ilyen módon (számfüggetlen személyközi hírközlési szolgáltatások).

Nem újdonság az a fontos körülmény, hogy annak érdekében, hogy egy szolgáltatás az elektronikus hírközlési szolgáltatás fogalmába tartozzon, rendes körülmények között díjazás fejében kell nyújtani. A Kódex azonban a digitális gazdaság működési jellemzőivel összhangban egyértelműsíti, hogy a díjazás fogalmába beleértendő az a helyzet, amikor a végfelhasználó a szolgáltatásnyújtó kérelmére személyes vagy más adatokat bocsát aktívan ez utóbbi rendelkezésére, vagy amikor adatokhoz hozzáférést enged (pl. IP-címekhez, tárolt sütik által gyűjtött információkhoz). Továbbá az Európai Unió Bíróságának gyakorlatával összhangban díjazásnak minősül az is, ha a szolgáltatónak harmadik fél, nem pedig a szolgáltatás igénybevevője fizet (pl. olyan hirdetéseken keresztül, amelyek feltételei annak, hogy a végfelhasználó hozzájusson a szolgáltatáshoz) [15].

A végfelhasználók jogaira vonatkozó követelmények nem egyenlő mértékben terjednek ki az egyes szolgáltatástípusokra: összességében megállapítható, hogy a legtöbb előírás a számfüggő személyközi hírközlési szolgáltatásokat, illetve az internet-hozzáférési szolgáltatást érinti, legkevésbé pedig az M2M jelátviteli, illetve a számfüggetlen személyközi hírközlési szolgáltatásokat terheli.

2.3. A harmonizáció szintje

A Hírközlési Kódexet megelőzően hatályban lévő keretszabályozás fogyasztóvédelmi szabályai a minimum harmonizáción alapultak, tehát a tagállamok fenntarthattak és bevezethettek nemzeti jogukban a végfelhasználók védelmével kapcsolatos szigorúbb rendelkezéseket. A keretszabályozás felülvizsgálatakor az Európai Bizottság fontos problémaként azonosította, hogy a végfelhasználók védelmével kapcsolatos szabályok eltérő végrehajtása miatt jelentős belső piaci akadályok keletkeztek, és számos érintett osztotta azt a véleményt, hogy a végfelhasználói jogok teljes harmonizációja jelentősen javítaná a jogbiztonságot, mind a végfelhasználók, mind az elektronikus hírközlési szolgáltatók szempontjából, egyúttal jelentősen csökkentené a piacra lépés akadályait, és a szabályok fragmentációjából eredő, szükségtelen megfelelési terhet [16]. A teljes harmonizáció megvalósítása legnagyobb akadályának az bizonyult, hogy több tagállam azzal érvelt, így csökken majd a végfelhasználók számára általuk biztosított védelem jelenlegi szintje, ezért a kérdés az új szabályozással kapcsolatos viták és tárgyalások végéig nyitva maradt.

Végül az EU-ban jellemző kompromisszumos megoldás született: az ún. teljes, de kalibrált harmonizáció. Ez azt jelenti, hogy fő szabályként ténylegesen úgy rendelkezik a Kódex, hogy a tagállamok nem tarthatnak fenn és nem vezethetnek be nemzeti jogukban a végfelhasználók védelmével kapcsolatos eltérő rendelkezéseket, ideértve az eltérő szintű védelmet biztosító szigorúbb vagy kevésbé szigorú rendelkezéseket. Azonban mégis van erre lehetőségük, amennyiben a Kódex így rendelkezik és számos helyen található ilyen kivételszabály. Másrészt megadja az ettől való eltérés lehetőségét a Kódex egy átmeneti időszakra is, mert úgy rendelkezik, hogy 2021. december 21-ig a tagállamok továbbra is alkalmazhatnak eltérő, szigorúbb nemzeti fogyasztóvédelmi rendelkezéseket, amennyiben ezek a rendelkezések már 2018. december 20-án hatályban voltak, és a belső piacot érintő, ezekből eredő bármilyen korlátozás arányos a fogyasztóvédelem céljával. A tagállamok emellett természetesen fenntarthatnak vagy bevezethetnek nemzeti normákat a Kódex által kifejezetten nem szabályozott kérdések tekintetében, különösen pedig a hírközlési szolgáltatások folyamatos fejlődésével összefüggésbe hozható újonnan felmerülő kérdések kezelése érdekében.

A cikk hátralévő részében röviden, áttekintő jelleggel bemutatjuk a végfelhasználói jogok szabályozásának egyes tárgyköreit érintő módosításokat, mégpedig azokat kiemelve, amelyek lényegesebb újdonságot jelentenek a már eddig is igen magas szintű és a keretszabályozás irányelvei által konkrétan megkövetelt nél jellemzően szigorúbb hatályos magyar előírásokhoz képest.

2.4. Alapelvi jellegű rendelkezések

Mindeddig lényegében meghiúsult, azonban továbbra is fontos EU-s cél marad az elektronikus hírközlés határokon átnyúló szolgáltatásokra épülő piacának létrehozása. Az ezt akadályozó egyik potenciális tényező a végfelhasználók indokolatlan megkülönböztetése. Ezért a Kódex kifejezetten rendelkezik arról, hogy a szolgáltatók nem írhatnak elő eltérő követelményeket a végfelhasználók állampolgárságával, lakhelyével vagy székhelyével összefüggő okok alapján, kivéve abban az esetben, ha ez az eltérő bánásmód objektív módon alátámasztható.

A Kódex több ponton nevesít kifejezetten a fogyatékossággal élő végfelhasználókkal szemben teljesítendő fogyasztóvédelmi követelményeket.

2.5. Személyi hatály

A Kódex következetesebbnek tűnik abban, hogy a védelmet a fogyasztónak minősülő végfelhasználóknak adja meg. Azonban ez az elv továbbra sem érvényesül majd maradéktalanul, ugyanis több, elsődlegesen fogyasztóvédelmi jellegű előírást – nevezetesen a szerződések adataira, a szerződések maximális időtartamára és a szolgáltatáscsomagokra vonatkozókat – a mikro- és kisvállalkozások, sőt újdonságként a nonprofit szervezetek esetében is érvényesíteni kell. A jogalkotók álláspontja szerint az említett kategóriákba tartozó vállalkozások és szervezetek tárgyalási pozíciója hasonló a fogyasztókéhoz, és ezért a fogyasztókkal azonos szintű védelmet kell élvezniük, kivéve abban az esetben, ha kifejezetten lemondanak ezen jogukról. Egyéb rendelkezéseket, így például a számhordozhatóságot, továbbra is minden végfelhasználó esetében tiszteletben kell tartani [17].

A kötelezett szolgáltatói oldalt illetően pedig figyelemreméltó, hogy a számfüggetlen személyközi hírközlési szolgáltatásokat nyújtó mikrovállalkozásoknak nem kell alkalmazniuk a végfelhasználók jogairól szóló rendelkezéseket, kivéve, ha egyéb elektronikus hírközlési szolgáltatásokat is nyújtanak.

2.6. Szerződésekre vonatkozó tájékoztatási követelmények

A továbbra is rendkívül részletes szabályozás addícionális új eleme, hogy a szolgáltatóknak a fogyasztók rendelkezésére kell bocsátaniuk az alapvető szerződési feltételek tömör, meghatározott minta szerint készítendő összefoglalóját is.

2.7. A szolgáltatások átláthatósága

A tarifákra és a Kódex mellékletében meghatározott egyéb feltételekre vonatkozó közzétételi kötelezettség az internet-hozzáférési szolgáltatást vagy a nyilvánosan elérhető személyközi hírközlési szolgáltatást feltételekhez kötő szolgáltatókra fog kiterjedni, nem csupán világos, átfogó, hanem géppel olvasható módon, a fogyatékossággal élő végfelhasználók számára pedig akadálymentes formátumban.

2.8. Szolgáltatások minősége

A nemzeti szabályozó hatóságok egyéb illetékes hatóságokkal koordinálva azt is előírhatják a nyilvánosan elérhető személyközi hírközlési szolgáltatásokat nyújtó szolgáltatók számára, hogy tájékoztassák a fogyasztókat, ha az általuk nyújtott szolgáltatások minősége valamilyen külső tényezőtől, például a jelátvitel feletti ellenőrzéstől vagy hálózati kapcsolattól függ. A nemzeti szabályozó hatóságok – más illetékes hatóságokkal koordinálva, a BEREC által kiadott iránymutatás legmesszemenőbb figyelembevételével – nemcsak a mérendő szolgáltatásminőségi paramétereket, hanem az alkalmazandó mérési módszereket is meghatározhatják majd az internet-hozzáférési szolgáltatások és a nyilvánosan elérhető személyközi hírközlési szolgáltatások minőségét illetően.

2.9. A szolgáltatóváltást elősegítő rendelkezések

A fogyasztó, illetve a számfüggetlen személyközi hírközlési szolgáltatásoktól és a gépek közötti szolgáltatások nyújtására használt átviteli szolgáltatásoktól (M2M) eltérő, nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtói közötti határozott idejű szerződések időtartama nem haladhatja meg a 24 hónapot. A tagállamok továbbra is elfogadhatnak vagy fenntarthatnak olyan rendelkezéseket, amelyek értelmében ez az időtartam ennél rövidebb is lehet. Ugyanakkor ez a megszorítás nem vonatkozik az olyan részletfizetési szerződések időtartamára, amelyek esetében a fogyasztó egy külön szerződésben vállalja, hogy kizárólag a fizikai összeköttetés létrehozását részletekben fizeti, különösen az ún. rendkívül nagy kapacitású hálózatokkal való összeköttetés esetén.

A Kódex a magyarhoz hasonló szigorú és részletes szabályokat tartalmaz a szerződések módosítására és megszüntetésére, továbbá rendelkezik a szolgáltatóváltás alapvető szabályairól az internet-hozzáférési szolgáltatás vonatkozásában és pontosítja a számhordozhatósággal kapcsolatos előírásokat. Ami viszont teljes újdonság, hogy kifejezetten az elektronikus hírközlési szolgáltatók csomagajánlatait célzó követelményeket is bevezet a szolgáltatóváltás elősegítése érdekében, mert a jogalkotó úgy ítélte meg, hogy jóllehet a szolgáltatáscsomagok sokszor előnyösek a fogyasztók szempontjából, megnehezíthetik, illetve költségessé tehetik a szolgáltatóváltást, és a végfelhasználók szerződéses foglyul ejtését idézhetik elő [18]. Ezért a Kódex úgy rendelkezik, hogy amennyiben a szolgáltatáscsomag, vagy szolgáltatásokból és végberendezésből álló csomag tartalmaz legalább egy internet-hozzáférési szolgáltatást, vagy egy nyilvánosan elérhető, számfüggő személyközi hírközlési szolgáltatást, a Kódex szerződés adatait összefoglaló dokumentumra, az átláthatóságra, a szerződés időtartamára és felmondására, valamint a szolgáltatóváltásra vonatkozó rendelkezéseit a csomag minden elemére alkalmazni kell, ideértve például azokat a digitális szolgáltatásokat, műsorszolgáltatásokat, végberendezéseket, amelyek nem tartoznak közvetlenül e rendelkezések hatálya alá.

2.10. Segélyhívási célú illetve vészhelyzeti kommunikáció

A segélyhívó szolgálatok segélyhívási célú kommunikáció útján való elérésére vonatkozó szabályozás alapvetően technológiai változásokkal indokolt frissítése mellett a Kódexbe került a fordított helyzet, vagyis annak szabályozása is, amikor a lakosságot szükséges riasztani azonnali vagy kialakulóban levő jelentős veszélyhelyzetekben, katasztrófákban. A szabályozást különösen az Európai Parlament szorgalmazta, melynek tagjai úgy tapasztalták, hogy a tagállamonként eltérő minőségű szabályozás aggályos lehet jelentős veszélyhelyzetek, így esetleges terrortámadások esetében.

Az e területre vonatkozó tagállami jogszabályok közelítése érdekében a Kódex legkésőbb 2022. június 21-től előírja, hogy amennyiben a tagállam lakossági riasztórendszert működtet, a mobil számfüggő személyközi hírközlési szolgáltatások nyújtóinak díjmentesen továbbítaniuk kell a lakossági riasztásokat minden érintett végfelhasználó számára, tehát azoknak, akik a riasztási időszakban az illetékes hatóságok meghatározása szerint az azonnali vagy kialakulóban levő jelentős veszélyhelyzetek és katasztrófák által potenciálisan érintett földrajzi területeken tartózkodnak. A tagállamok úgy is rendelkezhetnek, hogy a lakossági riasztások egyéb nyilvánosan elérhető elektronikus hírközlési szolgáltatások útján, vagy pedig internet-hozzáférési szolgáltatásra épülő mobilalkalmazás révén kerüljenek továbbításra, feltéve, hogy a lakossági riasztórendszer hatékonysága egyenértékű a lefedettség és a végfelhasználók elérésére vonatkozó képesség tekintetében, az érintett területen csupán ideiglenesen tartózkodókat is beleértve. A Kódex végrehajtásának felülvizsgálata során a Bizottság pedig majd azt is felmérheti, hogy az uniós joggal összhangban megvalósítható-e az egész Unióra kiterjedő, közös lakossági riasztórendszer létrehozása.

3. Zárszó: vissza- és előretekintés

Cikkünk bevezetőjéből kiderült, hogy az elektronikus hírközlési szektor európai keretszabályozásának legutóbbi átfogó felülvizsgálata és a mostani, a Kódexet eredményező módosítás között majdnem 10 év telt el. Meglehe-

tősen valószínű azonban, hogy a Kódex felülvizsgálatáig nem fog ennyi idő eltelni, legalábbis ami a végfelhasználók jogaira vonatkozó szabályokat illeti. A jogalkotók ugyanis – mintha elismernék azt, hogy az új, módosított ágazatspecifikus fogyasztóvédelmi szabályrendszer nem biztos, hogy tartósan kiállja majd az idő próbáját –, beiktattak egy erre a tárgykörre vonatkozó különleges felülvizsgálati eljárást.

Megbízták a BEREC-et, hogy kísérje figyelemmel a jövőbeli technológiai és piaci fejleményeket a tagállamokban, és első alkalommal 2021. december 21-ig – tehát már egy évvel a nemzeti jogba történő átültetés határidejét követően –, majd ezt követően háromévente, illetve legalább két tagállam indokolt kérésére tegye közzé rendszeresen véleményét, amely többek között arra vonatkozó értékelést tartalmaz, hogy e fejlemények milyen hatással vannak a Kódex rendelkezéseinek gyakorlati alkalmazására a végfelhasználók tekintetében. Különösen a szolgáltatóváltás lehetőségeit, az ennek esetleges hiánya által okozott piaci torzulást és a végfelhasználóknak okozott kárt, illetve azt szükséges elemezni, hogy a számfüggetlen személyközi hírközlési szolgáltatások fokozottabb igénybevétele és interoperabilitásuk hiánya veszélyezteti-e érzékelhető módon a sürgősségi segélyszolgálatok elérését. Az Európai Bizottságnak – a lehető legteljesebb mértékben figyelembe véve a BEREC véleményét – jelentést kell közzétennie és ha ezen irányelv célkitűzéseinek biztosítása érdekében szükségesnek ítéli, jogalkotási javaslatot kell benyújtania a módosítása céljából.

A Kódex tehát megszületetett, az implementáció rajtra kész, és úgy tűnik, a végrehajtásával egy időben maga a szabályozás is alakul majd.

A szerzőről

DR. KOVÁCS ANITA jogász, 2013-tól a Telenor Magyarország Zrt. vezető szabályozási szakértője, 2015–2016-ban a Telenor Csoport brüsszeli irodájának munkatársa. Korábban 1999-től egészen 2012-ig a Gazdasági Versenyhivatal Infokommunikációs Ágazati Irodájának vizsgálója, majd vezetője, ennek köszönhetően több éves tapasztalattal rendelkezik az elektronikus hírközlési szektort érintő versenyfelügyelet, illetve piacszabályozás területén. 2011–2013 között az Antenna Hungária Zrt. jogi, szabályozási osztályának vezetője.

Hivatkozások

[1] Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások közös keretszabályozásáról (HL L 108., 2002.4.24., 33.o.).
[2] Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatok és az elektronikus hírközlési szolgáltatások engedélyezéséről (HL L 108., 2002.4.24., 21.o.).
[3] Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az elektronikus hírközlő hálózatokhoz és kapcsolódó eszközökhöz való hozzáférésről, valamint azok összekapcsolásáról (HL L 108., 2002.4.24., 7.o.).
[4] Az Európai Parlament és a Tanács 2002/21/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról (HL L 108., 2002.4.24., 51.o.).
[5] Az Európai Parlament és a Tanács 1211/2009/EK rendelete (2009. november 25.) az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) és Hivatalának létrehozásáról (HL L 337., 2009.12.18., 1.o.).
[6] Az Európai Parlament és Tanács 676/2002/EK határozata (2002. március 7.) az Európai Közösség rádióspektrum-politikájának keretszabályozásáról (HL L 108., 2002.4.24. 1.o.).
[7] a Bizottság 2002. július 26-i 2002/622/EK határozata (2002. július 26.) a rádiófrekvencia-politikával foglalkozó csoport létrehozásáról (HL L 198., 2002.7.27., 49.o.).
[8] Az Európai Parlament és Tanács 243/2012/EU határozata (2012. március 14.) egy többéves rádióspektrum-politikai program létrehozásáról (HL L 81., 2012.3.21., 7.o.).
[9] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről) (HL L 201., 2002.7.31., 37.o.).
[10] Az Európai Parlament és Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről) (HL L 119., 2016.5.4., 1.o.).
[11] Az Európai Parlament és a Tanács 531/2012/EU rendelete (2012. június 13.) az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming) (HL L 172., 2012.6.30., 10.o.).
[12] Az Európai Parlament és Tanács (EU) 2015/2120 rendelete (2015. november 25.) a nyílt internet-hozzáférés megteremtéséhez szükséges intézkedések meghozataláról, továbbá az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv és az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming) szóló 531/2012/EU rendelet módosításáról (HL L 310., 2015.11.26., 1.o.).
[13] Az Európai Parlament és a Tanács 2014/61/EU irányelve (2014. május 15.) a nagy sebességű elektronikus hírközlő hálózatok kiépítési költségeinek csökkentésére irányuló intézkedésekről (HL L 155., 2014.5.23., 1.o.).
[14] (EU) 2018/1972 irányelv (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról, 15. preambulum bekezdés.
[15] (EU) 2018/1972 irányelv (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról, 16. preambulum bekezdés.
[16] (EU) 2018/1972 irányelv (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról, 257. preambulum bekezdés.
[17] (EU) 2018/1972 irányelv (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról, 259. preambulum bekezdés.
[18] (EU) 2018/1972 irányelv (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról, 283. preambulum bekezdés.

Summaries • of the papers published in this special issue

This Special Issue is compiled from the papers of the 21th HTE Infokom 2018, the Infocommunications Networks and Application Conference, organized by the Scientic Association for Infocommunications (HTE).

Machine learning use cases in 5G context

Keywords: 5G networks, IoT, edge computing, distributed cloud, neural networks, augmented reality

The paper describes how artificial intelligence helps in operational support systems in network automation and an object detection and position estimation solution use case where artificial intelligence plays a key role. It is described how these systems fit to the 5G landscape, giving also the background why we are talking about this now. Distributed Cloud, an edge computing solution is introduced, explaining what techniques 5G networks can offer to host low latency and compute demanding use cases.

Industry 4.0 solutions – Factory infrastructure monitoring and supervision

Keywords: Industry 4.0, IoT, infrastructure supervision

Factory subsystems, such as production, factory infocommunications system, and facility or base infrastructure, constitute a pretty complex production ecosystem. In this complex ecosystem, it can easily happen that a failure in a basic component blocks the whole production process, and thus the normal operation of the factory. In this paper, we introduce, and illustrate via a plotting table based demonstration, our Industry 4.0-ready, unified factory infrastructure monitoring and supervision system.

Shift from analog PMR to DPMR in industrial settings: Some notable experiences of the transition process

Keywords: dPMR, DMR, speech intelligibility

Due to advancements in radio technology, digital private mobile radio (dPMR) has been gradually replacing traditional/analog voice and data radio transmission in the past 10 years. Prior to the digital revolution, manufacturers and integrators of the analog systems had done their best to satisfy the needs of their users and improve the communication capacities of the traditional mobile radio. By presenting the planning and installation phases and sharing the experiences made during the operation of two networks of different size and complexity in Hungary, the paper demonstrates the virtues and merits of the digital shift, without omitting to mention the not so apparent challenges and drawbacks of such transition.

Strategic role of tower infrastructures in the telecom-market

Keywords: towerco, MNO, tower, infrastructure

Nowadays the strategic importance of own tower infrastructure is gradually decreasing for MNOs, while willingness for sharing the networks is on the rise. For cost-efficiency purposes more and more MNOs decide to sell their tower portfolio to towercos that are specialized in managing tower infrastructures. With upcoming 5G networks the significance of towercos might further increase.

Cybersecurity in the age of the fourth industrial revolution

Keywords: Industry 4.0, IoT, NISD, Cybersecurity Act, GDPR, cyber-physical system

The core building blocks of the fourth industrial revolution are undoubtedly the networked digital devices that have appeared in billions in the past years. Their secure operation is therefore an essential requirement for both our economy and our society. However, cybersecurity raises issues for Industry 4.0, given that there is much less experience with IT focused defense for complex industrial systems or cyber-physical systems than with traditional threats coming from the physical space. This paper reviews the European and national strategies and legislation aimed at strengthening cyber security and points out what regulatory tools are available to support and control the actors of the fourth industrial revolution.

Blockchain and its specific security issues

Keywords: blockchain, Bitcoin, cryptocurrency

The paper provides an introduction to the world of blockchain as a decentralised system, using the example of Bitcoin, the first blockchain-based system. We emphasize the difference between blokchain, which is the internet of values, as a platform, on the one hand, and the cryptocurrencies, on the other hand. Then the different consensus mechanisms are dealt with. Finally, we address some security issues, resulting from the inherent vulnerability of blockchain's centralised environmental elements, as well as from making use of the vulnerability due to protocol errors of blockchain.

Present and future of school networks

Keywords: Digital Education Strategy of Hungary (DES), school network, network of the future's school

The digitalisation of the education system has become unavoidable in order to prepare young people to meet the requirements of a changing labor market. Therefore, as part of the Digital Success Program (DSP), the Hungarian government prepared a strategic plan aiming at the digital transformation of the Hungarian education system. Along with the current developments, we should begin to think about how a school should look like in the future: where, and what should children learn in 10 years' time?

Impact of the European Electronic Communications Code on radio spectrum management

Keywords: European Electronic Communications Code, radio spectrum management, 5G, Peer review

With the publication of the European Electronic Communications Code in December 2018, the 24 months available to Member States have begun to transpose it into their national legal frameworks for the sector. There have also been a number of changes in the field of radio spectrum management, of which this paper intends to review the most important new regulatory elements in the article, examining its possible impact, especially with regard to the introduction of 5G.

End-user rights in the new Code

Keywords: new definition of communication services, regulatory framework of electronic communications

From the end of 2020, at the latest, the Hungarian end-users of electronic communications services, the service providers, and the regulatory authorities supervising the sector will face a regulatory regime which is significantly different from the current one although not completely new. The most important novelty of the Code in its consumer protection chapter containing the end-user rights provisions are the redesign of the definition of electronic communications services, its extension to cover the so called OTT communications services and the maximum harmonization approach.