Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette
Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből II.

Szemelvények a katonai műszaki tudományok eredményeiből II.

Hallgatói kötet

Szerkesztette

Hausner Gábor

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2021

Szerzők

Ambrus Éva
Bodnár László
Csanádi Győző
Deák Veronika
Dévai Dóra
Domán László
Goda Zoltán
Huszár Péter
Huszár Viktor
Katona Gábor
Kralovánszky Kristóf
Kretz András
Kutassy Emese
Lakatos Bence Roland
Matusz Márk Péter
Olajosné Lakatos Boglárka
Priváczkiné Hajdu Zsuzsanna
Salamon Endre
Takács Krisztina
Terék Tamás
Tímár Attila

Szakmai lektorok

Bíró Tibor
Haig Zsolt
Padányi József
Palik Mátyás
Pohl Árpád
Restás Ágoston

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Koltay András rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Oláh Andrea
Korrektor: Bíró Csilla, Bujdosó Hajnalka
Tördelőszerkesztő: Fehér Angéla

ISBN 978-963-531-441-6 (PDF) | ISBN 978-963-531-442-3 (ePub)

Tartalom

Kralovánszky Kristóf

Állami célú adatátviteli rendszerek, hálózatok részleges integrálhatóságának egyes kérdései

Bevezetés

Definíció szerint a kibertér létezésének alapfeltétele az infokommunikációs eszközök hálózatba kapcsoltsága, így kijelenthető, hogy a kibertér infokommunikációs hálózatok nélkül nem értelmezhető, és amennyiben infokommunikációs hálózatokon van adatforgalom (üzemben van), akkor az a hálózat (és minden használatban lévő végpontja) szükségszerűen része a kibertérnek.[1]

Az információs társadalomban az állam technikai működtetése infokommunikációs technológiákra alapul, amelyek eltérő helyszínek közötti kommunikációját adatátviteli hálózatok teszik lehetővé.[2] Az állam, mint különleges szereplő, saját, többségében zárt infokommunikációs rendszereket működtet, amelyek (helyesen) elkülönülnek a polgári rendszerektől, részben adatvédelmi okokból, részben pedig a működési biztonság megteremtése céljából.

Az állam saját szereplői (ágazatai és alágazatai) számos esetben egymással párhuzamos adatátviteli rendszereket üzemeltetnek, amelyek infrastruktúrái részben (többször teljes egészében) elvileg összevonhatók lennének. Ezzel egy időben, napi szinten jelenik meg az adatok és információk megosztásának szükségessége is, vagyis e hálózatok között – meghatározott szabályok szerint – átjárást és folyamatos adatáramlást kell(ene) biztosítani.

Az exponenciálisan növekvő komplex állami adatmennyiség mozgatása és folyamatos elérhetőségének biztosítása rendkívül komoly kihívás elé állítja ezen zárt célú rendszerek üzemeltetőit. Az ennek kapcsán keletkező átviteltechnikai és rendelkezésre állási lehetséges problémák – akár jelentős – működtetési és egyéb használati korlátozásokhoz vezethetnek. A kutatás elsődleges célja e fenti adatátviteli hálózatok szervezetek közötti megosztási lehetőségeinek elemzése – ugyanakkor nem konkrét műszaki megoldást, hanem műszakilag megvalósítható logikai koncepciót kíván vizsgálni és felépíteni.

A szerző szándékosan nem kíván konkrét műveleti példákat bemutatni, amelyek alátámasztják, hogy miért indokolt a jelenlegi rendszerektől sokszor jelentősen eltérő módon alakítani az itt részletezett adatátviteli rendszereket. Nem cél szembeállítani hazai jó és rossz példákat, mert szervezeti vagy személyes felelősséget ilyen formában taglalni – jelen keretek között – nem jó, illetve a valódi okok és problémák tartalmukban részben minősítettek lehetnek.

---

[1] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

[2] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.

A csoportosítások és határértékek (küszöbértékek) jellemzően a szerző saját szakmai tapasztalatain alapulnak, és számos esetben nem létezik nyílt forrású irodalmuk – ahol lehetséges, ott természetesen a releváns források jelölve vannak. E cikk a teljes téma lényegesen tágabb és részenként is alátámasztott kutatásának az alapjául (is) szolgál, így számos hipotézist is tartalmaz.[3]

Hálózatok csoportosítása

Az infokommunikációs hálózatok egyik lehetséges csoportosítása az állam működését támogató (biztosító) hálózatok és az azon kívüli hálózatok (például lakossági) szerinti szétválasztás. E csoportosítás alapján az állam működését támogató hálózatok szükségszerűen elsőbbséget élveznek, amelyeken belül további differenciálás lehetséges célok/üzemeltetők szerint.[4] Nagyon fontos további megkülönböztetés (az előbbiekkel párhuzamosan) az adatátviteli mennyiség, a vonali sebesség és az átviteli technológia szerinti csoportosítás is. Mindez táblázatban összefoglalva, mátrixként értelmezve, az alábbiak szerint foglalható össze.

18. táblázat: *Adatátviteli paraméterek*

Üzemeltetés tartalma	Adatátviteli mennyiség (naponta)	Vonali sebesség (szinkron)	Átviteli technológia
honvédelmi rendvédelmi katasztrófavédelmi államigazgatási (központi kormányzat, illetve önkormányzatok) nemzetbiztonsági egészségügyi egyéb speciális (vasút, villamosenergia-ellátás, kritikus infrastruktúrák)	< 100 MB 100 MB – 1 GB < 1 GB 1–5 GB 5–20 GB 20–100 GB > 100 GB	< 50 Kbps 50–500 Kbps 0,5–5 Mbps 5–50 Mbps 50–500 Mbps 0,5–1 Gbps 1–10 Gbps > 10 Gbps	optikai réz dedikált- mikrohullámú egyedi, rádiós (nem mikrohullámú és nem wifi) mobil (2G, 3G, 4G, 5G) műholdas

Forrás: a szerző szerkesztése

Minden állami alágazatnak (üzemeltetési tartalom szerint megkülönböztetve) – különösen végrehajtói szinten – megvannak a maga sajátos kommunikációs igényei, ezért jelen

[3] Több hipotézist a szerző szakmai tapasztalatai már most is alátámasztanak, a következő időszak kutatásai pedig további tudományos alapokat biztosíthatnak.

[4] A csoportosítási lista nem teljes, illetve főbb részei között akár jelentős átfedések lehetnek, különösen speciális feladatok végrehajtása során (például katasztrófavédelem–rendvédelem egy természeti/ipari katasztrófa esetén). Természetesen fontos a nyílt, zárt, különcélú stb. szerinti megkülönböztetés is, de jelen rész szempontjából ennek kisebb a jelentősége.

vizsgálat szempontjából az adatátviteli hálózatok klasszikus helyi hálózati (*Local Area Network* – LAN) szegmensei nem relevánsak.[5]

Országos adatátviteli rendszert tekintve, koncepcionálisan az alábbi fő részeket célszerű megkülönböztetni:[6]

- központi gerinchálózati (10 Gbps feletti vonali sebességgel);
- regionális gerinchálózat (5–10 Gbps közötti vonali sebességgel);
- regionális elosztóhálózat (1–5 Gbps közötti vonali sebességgel).

A fentiek természetesen átlagos értékek és egy kiemelt végpont akár önmagában is generálhat regionális szintű forgalmat (amely lehet jellemzően akár egyirányú, akár kétirányú).

Hibatűrő helyi hálózatokkal kapcsolatos kutatások és konkrét megoldások – maival is összehasonlítható felhasználási méretekben – több mint két évtizede léteznek, de óriási különbség van a helyi hálózatok és a nagy kiterjedésű hálózatok (*Wide Area Network* – WAN) között, amelynek elsődleges oka a fizikai távolságokból adódó kábelhosszak (kapcsolati távolságok) több nagyságrendi különbsége.[7] Ezért lehet, hogy hibatűrő LAN-ok kialakítására számos koncepció létezik,[8] de hibatűrő WAN-ok esetében elsődlegesen meghatározó szempontjai a rendszer felhasználási módjai és üzemi sajátosságai, amelyek gyökeresen eltérő topológiájú modelleket eredményezhetnek.[9]

Jelen írás hipotézise szerint egy komplex kormányzati hálózatban alapfeltétel, hogy egy regionális elosztóhálózati aktív hálózati elem elágazási pontjainak legalább 2,5 (két és fél),[10] egymástól független irányba kell kapcsolódni, ami a gyakorlatban azt jelenti,

---

[5] Értelmezésében nem tekinthető LAN-szegmensnek egy taktikai harcászati adatátviteli rendszer azon része, ahol például egy drón vagy harcjármű pont–multipont típusú kommunikációt végez, különösen akkor, ha a multipont rész egyik eleme „felfelé" irányban továbbítja a megkapott adatot. LAN-szegmensnek tekintett ugyanakkor a drón vagy harcjármű pont–pont jellegű kommunikációja. Vezető nélküli eszköz (például drón) esetén az irányítási adatfolyam és az adatszerzési adatfolyam különbözőnek tekintendő.

[6] Vonatkoztassunk el egyelőre a különböző, jelenleg különállóként működő országos zárt célú hálózattól (mint például a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózat – MH KCEHH).

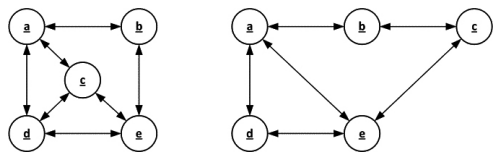
[7] LAN esetében az átlagos kábelhossz egy aktív eszköz (jelismétlőket nem beleszámítva) és egy végberendezés között 50–100 méteres nagyságrend. Ugyanez WAN esetében 5–50 km nagyságrend.

[8] Paul LeMahieu – Vasken Bohossian – Jehoshua Bruck: *Fault-tolerant switched local area networks*. Proceedings of the First Merged International Parallel Processing Symposium and Symposium on Parallel and Distributed Processing. IEEE Xplore, Orlando, 1998. 747–751.

[9] Muriel Médard – Steven S. Lumetta: Network reliability and fault tolerance. In John G. Proakis (ed.): *Wiley Encyclopedia of Telecommunications.* Hoboken, New Jersey, John Wiley & Sons, 2003. 36.

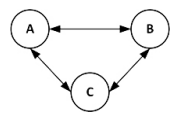
[10] Gyakorlati tervezési és üzemeltetési okokból nem elégséges az egy tartalékirány, mert az irányok átviteli képessége változó lehet és a tartalékirányok nem „üres", vagyis meleg tartalékok, hanem üzemben lévő átviteli hálózatok, amelyek már eleve valamilyen forgalmi terheléssel rendelkeznek. Így egy nagyobb forgalmú vonal átterhelése túlterhelődést és ennek következtében részleges dominóeffektust okozhat. Ezt hivatott kikerülni a kettő és három közötti kapcsolódási pontok rendszere – más megfogalmazásban az egy és kettő közötti tartalékirányok rendszere. Annak pontos meghatározását, hogy hol szükséges a két tartalékirány, szintén a tervezéshez kapcsolódó komplex gráfok fogják segíteni.

hogy az elemek kisebb részének legalább kettő,[11] míg a fennmaradó résznek legalább három független irányba (1. ábra) kell kapcsolódniuk. Regionális gerinchálózatnál ennek az értéknek közelíteni kell a háromhoz – főként azért, hogy kieső központi gerinchálózati elemeket időlegesen ki tudjon váltani.



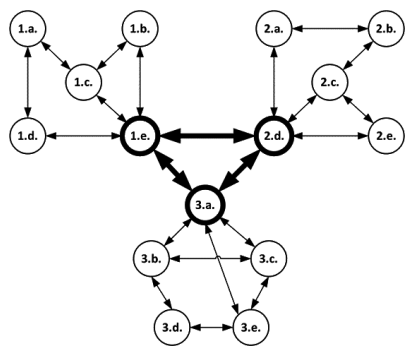
1. ábra: Területi, regionális hálózatok irányai
Forrás: a szerző szerkesztése

Központi gerinchálózatnál szintén legalább 2 független iránynak (2. ábra) lennie kell (a 3. ábrán a központi gerinchálózatot az 1.e.–2.d.–3.a. pontok közötti vonalak modellezik).



2. ábra: Központi gerinchálózat iránya
Forrás: a szerző szerkesztése

A központi gerinchálózat és a regionális hálózatok kapcsolatát a 37. ábra mutatja.[12] Az 1.e., 2.d. és a 3.a. pontok közötti gerinchálózati kapcsolatok a regionális hálózatok szempontjából nem tekintendők saját független irányoknak.



3. ábra: Hálózati szintek kapcsolódásai
Forrás: a szerző szerkesztése

[11] Ezek jellemzően a kisebb forgalmú, kisebb szomszédos forgalmú és magasabb telepítési költségű végpontok.
[12] A néhány végpontból álló sematikus ábrák messze nem képesek a komplex hálózati topológiák hibatűrési irány- és kapcsolatrendszerét bemutatni, így elsősorban az elvi (logikai) megértést szolgálják.

Általánosságban elmondható, hogy a gerinchálózati szinteken az átviteli főtechnológia vezetékes (és jellemzően, illetve a lehetőségek szerint optikai), de a konkrét helyzettől, az üzemeltetés várható időtartamától és egyéb paraméterektől (üzemi áthidalás, ideiglenes terheléselosztás) függően lehet vezeték nélküli is (mikrohullámú vagy lézeralapú).

Mobil adatátvitelre szintén fontos a meglévő infrastruktúrák használata és szükség szerinti kiegészítése, amelyre a TETRA–hálózat (TETRA: TErrestrial Trunked RAdio – földfelszíni trönkölt rádió) alkalmassá tehető akár 30 Mbps sebességig, így gépjárműbe szerelve rendkívül gyors adatátvitel érhető el. Ez részben meglévő infrastruktúrák alkalmazásával a TETRA biztonságát ötvözi az üzemelő digitális műsorszóró technológiákkal (*Digital Audio Broadcast / Digital Video Broadcast* – DAB/DVB) és tesz lehetővé műveleti szintű követelményeket is meghaladó mértékű adatátvitelt. [13]

Végponti oldalon a hatályos jogi szabályozás alapján[14] is meghatározhatók azok az elemek, amelyeknél legalább két független külső adathálózati kapcsolattal kell rendelkezni. Jelen modellezés szempontjából ilyen esetben a két irány nem egy élő + egy tartalékot jelent, hanem egy élő + egy meleg tartalékot + egy hideg tartalékot. A meleg tartalék jelentse azt, hogy akár pillanatnyi terhelésmegosztással is egy 95/5%-os megosztás huzamosabb időre (akár néhány órára is) 5/95%-ra módosulhat, anélkül, hogy az a régió többi elemére bármilyen korlátozást vagy további jelentős átirányítást jelentene. A hideg tartalék használatba vétele pedig értelem szerint már beavatkozást jelenthet a környező vonalak forgalmi szervezésébe.[15]

Maga a gyakorlati tervezés is számos, rendkívül komplex gráfmodell elkészítését igényli, amelyek önmagukban is igen terjedelmesek, ám a helyesen kiválasztott modellek extrapolálhatók. Elkészíthető tehát a rendszermodell egy régióra/megyére, amely utána alkalmassá tehető egy országos méretű rendszer vizsgálatára. Az adott ország állami berendezkedése a szintek autonómiáján módosíthat ugyan, de logikai értelemben a rendszer működőképes marad. Nagyobb országok esetében (például Németország) szintén adaptálható lenne a koncepció azzal, hogy ott a tartományi szint felel meg egy kisebb ország szintjének és erre kerül a szövetségi mint plusz szint.[16]

Magyarországon egy ilyen országos hálózat kiépítése alágazatonként nagyságrendileg 10 000 km hálózatot igényelne,[17] amelyet kiegészítenek még a mobil mikrohullámú

[13] Faster than the standard – higher data rates with TETRA. *News from Rohde & Schwarz,* 182. (2004), 2. 21–23.

[14] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

[15] Hálózatmenedzsment szempontból a hideg tartalék elindulása automatikus, de azonnali riasztást generál és legalább aktív felügyeletet, de inkább beavatkozást igényel a hálózati operátoroktól.

[16] E tanulmány természetesen nem egy Európa minden országára alkalmazható modellt kíván adni, hanem egy lehetséges, jól skálázható és rugalmasan adaptálható keretrendszer lehetőségét mutatja be.

[17] Bancsics Ferenc: *Az NTG helye a Gigabit társadalom fejlesztésében.* HTE INfokom, 2018.

irányok, és amelyeket a későbbi részek mutatnak be.[18] Amennyiben a rendszer része az államigazgatási (TETRA rádió típusú és GSM-UMTS-LTE [19] rádiótelefon típusú) mobil kommunikáció, akkor annak vezetékes (regionális gerinchálózati és regionális elosztóhálózati) szegmense részben a fentieken felüli hálózatot igényel – illetve logikai szervezés szempontjából egy-egy bázisállomás tekinthető egy önálló alágazat elemi végpontjának. Mindezek külön-külön történő létrehozása a honvédelmi, rendvédelmi, katasztrófavédelmi és államigazgatási szervek számára nyilvánvalóan irracionális, hiszen a komplex rendszerek egyenkénti bekerülési költsége – üzemeltetés nélkül – 600–1000 milliárd forintos nagyságrendet képvisel.[20]

Meg kell tehát keresni azokat a megoldásokat, amelyek segítségével megosztott használatú adatátviteli hálózat hozható létre. Ezt a célt szolgálja Magyarországon részben a Nemzeti Távközlési Gerinchálózat (NTG), amely elsősorban a szűken értelmezett államigazgatás és a belbiztonsági szervek adatátviteli igényeit szolgálja ki, így például a Magyar Honvédség saját belső céljaira, kiterjedt módon jellemzően nem áll rendelkezésre.

Minősített adatok átviteli biztonsága

Szükséges röviden a Honvédség, a Rendőrség és a nemzetbiztonsági szolgálatok adatátviteli sajátosságait áttekinteni. Magától értetődő okokból e szervezeteknek létszükséglet, hogy garantáltan megbízható, a legmagasabban minősített adatok átvitelére is biztonsággal megfelelő hálózatuk legyen (ahogy ez törvényi előírás egy sor más állami szervezetnek is).[21] E biztonság megteremtése több pilléren nyugszik, amelyek közül kettő a hálózati hardveres biztonság vonali tekintetben és ugyanez végponti eszköz tekintetben. Fontos különbséget tenni a vonali elkülönítés és a nyomvonali elkülönítés fogalmai között. Az előbbi a fizikai adatátviteli szál (optika) vagy kábel (réz) elkülönítését jelenti, vagyis azt, hogy azon az elemi vezetéken más szervezet adatátvitele fizikailag se tudjon megjelenni.[22] A nyomvonali elkülönítés pedig nem zárja ki, hogy egy kötegelt vezetékcsoporton egymás mellett fusson egy honvédségi és egy más államigazgatási forgalmat kiszolgáló (elemi) vezeték. Az elemi vezetékek közötti fizikai biztonságot (árnyékolás, megfelelő optikai köpeny) természetesen biztosítani kell – ami a telepítési költségeket jelentősen

[18] A Nemzeti Távközlési Gerinchálózat 2018-as valós és tervezett végleges mérete közötti extrapolációval, amennyiben az NTG felhasználója csak egy szervezet lenne (például Rendőrség).

[19] GSM *(Global System for Mobile Communications)* – 2G-hálózatok; UMTS *(Universal Mobile Telecommunication System)* – 3G-hálózatok; LTE *(Long Term Evolution)* – 4G-hálózatok. A legújabb technológiájú 5G-hálózatok egyelőre az állami szegmensben nem jellemzőek, széles körű, csak állami felhasználásuk további jelentős biztonsági kutatásokat és gazdasági elemzéseket igényel.

[20] A szerző iparági és kiberbiztonsági szakemberekkel történt egyeztetéseket követően készült, konszenzuson alapuló becslése.

[21] A honi jogszabályi kötelmeken felül nemzetközi szerződések és szövetségi rendszerek szabályzatai (pl. NATO, EUROPOL stb.) is megfogalmazzák ezeket.

[22] Átgondolandó, hogy optikai kábelezésnél a multimode technológia használata mennyiben jelenthet kockázatot a szétválasztásban, azonban jelen írás terjedelmi korlátai e vizsgálatot nem teszik lehetővé.

növeli bár, de bevett és jól működő megoldások állnak rendelkezésre. Megjegyzendő, hogy míg a megfelelő fizikai védelemmel ellátott optikai szálak önmagukban kevésbé kitettek lehallgathatóságnak,[23] addig a végponti részeken, ahol az optikai jel fotodiódás és lézerdiódás váltása történik, rendkívül magas az elektromágneses interferenciának való kitettség (és ezzel a támadhatóság).[24]

Nyilvánvaló, hogy a minősített adatok megfelelő kezelését meg kell teremteni, de ez – a végponti adatátviteli eszközök elhelyezésének vonatkozásában – megoldható a moduláris kiépítésen belül, ahol a nyílt rendszerek fizikailag elkülönítve jelennek meg, míg a minősített adatkezelő rendszerek külön zárható fülkében kapnak helyet. Egy olyan végponton, ahol kizárólag minősített adatátviteli eszközöket helyeznek el, ez a szétválasztás nem szükséges, ugyanakkor a fizikai biztonság az eszközök elhelyezési helyisége körül valósul meg – vagyis maga a helyiség lesz zárt körlet, annak minden előírásával.

Megvalósításában ez lehet egy minikonténer, amelyet megfelelő betonalapra helyeznek el, majd fallal és tetővel vesznek körbe, illeszkedve a helyi építészeti sajátosságokhoz. A konténer belső része szintén moduláris és a hálózati eszközökön kívül biztosítja a szünetmentes tápellátást, valamint a hűtést/fűtést. A megvalósításokhoz egy sor jogszabályi módosítás szükséges, mert a jelenlegi rendelkezések (például 90/2010. [III. 26.] Korm. rendelet) az ilyen megoldásokat jelenleg nem, vagy csak részlegesen támogatják. Léteznek (és racionális keretek között elérhetők) azonban olyan technikai és fizikai megoldások, amelyek biztosítják a jogalkotó szándéka szerinti védelmet.

A vonalak elkülönítését és azzal egyidejű kötegelését rendkívül jól szemlélteti egy nagyvárosi metrótérkép – amely természetesen analógia csupán –, ahol a különböző színű vonalak a különböző szolgálatokat (funkciókat) jelentik, ugyanakkor számos részen megfigyelhető az egy nyomvonalon haladás a többcélú létesítményeknél.[25]

Optikai szálak esetén a kötegelés nem okoz jelentős logisztikai problémát, hiszen egy elemi szál önmagában is képes több száz kilométeres távolságban 100 Gbps nagyságrendű adatátvitelre, vagyis egy 96 elemi szálból álló optikai köteg,[26] amely átmérőben, földkábelként nem haladja meg a néhány cm-t. Ha információbiztonsági megfontolásból kötegelt kábelezés szintjén is elválasztjuk a nyílt, titkos és szigorúan titkos adatátviteli hálózatokat, és nyomvonalanként három kötegelt optikai kábellel (3 x 96 szál) számolunk, akkor a teljes átmérő (beleértve a kötegek rozsdamentes acél és alumínium védőköpenyét

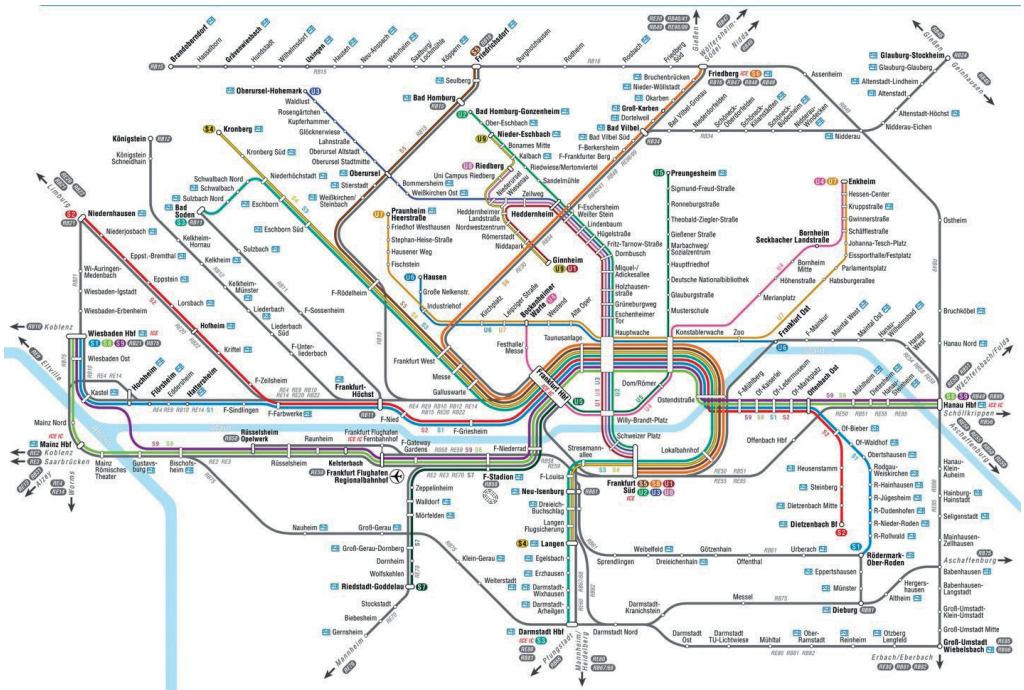
[23] A lehallgathatóság ellen védeni kell magát a fizikai hálózatot. Az adatátviteli biztonság kockázataival részletesebben egy korábbi írásunkban foglalkoztunk: Kralovánszky Kristóf: Elektronikus határvédelmi rendszerek jellemző sebezhetőségei és védelmük lehetőségei. *Hadmérnök,* 14. (2019), 1. 271–282.

[24] Keith D. Masterson – David R. Novotny – Galen H. Koepke: *Electromagnetic shielding characteristics of optical-fiber connectors*. NIST Publications, Boulder, Colorado, 1997.

[25] A térkép nem szolgál példaként a hálózati elágazási pontok számára (és redundanciájára) – különösen nem az egy vonalon egymást szekvenciálisan követő állomások esetében. A térképet ugyanakkor mikrohullámú kapcsolatokkal kiegészítve és egy külső gyűrűt alkalmazva – ahol a sugárirányú vonalakat e külső gyűrű összeköti – már vizuálisan is jóval közelebb kerülünk a redundancia egy magasabb fokához. Különösen érvényes ez akkor, ha nem egy, hanem több (koncentrikus) gyűrűt alkalmazunk.

[26] Ez ma már messze nem számít extrémitásnak sem technológiájában, sem költségeiben egy 48 vagy 72 szálas hasonló kábellel összehasonlítva.

is) még mindig nem haladja meg az 5–8 cm-t.[27] Ugyanez természetesen távvezeték-oszlopok tetején is megvalósítható, ahogy az NTG gerinchálózatának legnagyobb része ma is működik.[28]



4. ábra: Frankfurt am Main és elővárosainak sematikus gyorsvasúti hálózattérképe
Forrás: Rhein-Main-Verkehrsverbund[29]

[27] CentraCore Optical Ground Wire (OPGW). *Aflglobal.com.*

[28] Kralovánszky Kristóf: A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle,* 7. (2019), 3.
Felmerülhet a kérdés, hogy amennyiben háromszor 96 szál áll rendelkezésre, akkor miért kell egyesíteni hálózatokat? Az ok a végponti berendezések optimalizálásában keresendő. Nagyságrendileg 15 000 végponttal számolva (rendvédelem, honvédelem, katasztrófavédelem, önkormányzatok, egészségügyi intézmények stb.) Magyarország esetében és végpontonként átlagosan 15 routerrel számolva, 225 000 végponti eszközről lenne szó, amelyek központ oldala további 50 000-es nagyságrendű eszközt igényelne, így a teljes hálózatban közel 300 000 routert kellene üzemeltetni, ami nyilvánvalóan lehetetlen. Ezért az elkülönítések – ameddig lehetségesek – router port szinten valósulnak meg, ami a szükséges routerek számát akár 60–75%-kal is csökkentheti.

[29] Netzpläne helfen bei der Orientierung. *Rhein-Main-Verkehrsverbund.*

A rendszer irányítása[30]

E tanulmány egyik hipotézise szerint az országos rendszer régiókra osztandó, amelyből legalább egy régió az ország adminisztratív központja önmagában.[31] A régiók központjait magasabb szinten kell kezelni, vagyis azokat egy országos központ fogja össze. Az országos központnak régiókon belüli irányítási jogköre alapértelmezetten nincs.

A központokat (regionális és országos) a területi jelzővel, mint előtaggal, nevezzük Működés Összehangoló Központnak (MÖK).[32] Minden MÖK-ben van legalább egy fő azokból a szervezetekből, amelyek az adott regionális rendszer főbb felhasználói (honvédség, rendőrség, katasztrófavédelem, mentők stb.). Ezek a képviselők tartják a kapcsolatot saját szervezetük regionális ügyeleteivel és jogosultak operatív döntések meghozatalára. A MÖK működését a képviselt szervezetek egy választott tisztje[33] irányítja, akit egy évre jelölnek ki, és minden évben más szervezet adja.[34] Az országos MÖK a regionális szervezeteivel megegyezően működik azzal, hogy ott az előbbi operátoroknak legalább egyéves területi tapasztalattal kell rendelkezni.

A régiók saját belső működését és sajátosságait – amelyek ágazatonként akár napi szinten is változhatnak – a területileg illetékes MÖK ismeri és ennek alapján képes operatív döntéseket hozni.

Egy MÖK fizikai elhelyezése megvalósulhat önálló épületben vagy többcélú objektumban (például nagyobb honvédségi laktanyák). Az ilyen típusú elhelyezést indokolhatja (és támogathatja) az adott központ fizikai védelmi igénye is, amely egy katonai objektumon belül meg tud valósulni. Ugyanígy laktanyákon belül diszlokálhatnak részben azok a mobil eszközök és egyéb technikák, amelyek a külső településekhez szükségesek (önjáró rádiórelé, mobil antenna).[35] Maga a laktanya továbbá szolgálhat stacioner / mobil váltópontként is, ahová a külsőleg települt ideiglenes végpontok csatlakozhatnak. Természetesen nem feltétel, hogy honvédségi objektumban valósuljon meg a (közös) diszlokáció, hiszen Magyarországon is számos olyan rendőrségi objektum létezik a megyékben,

---

[30] A Nemzeti Infokommunikációs Szolgáltató Zrt. szervezete, feladata, felépítése és szolgáltatói viszonyrendszere jól ismert a szerző előtt. A jelen tanulmányban leírt komplex rendszer számos funkcionális párhuzamosságokat mutat a NISZ Zrt. jelenlegi működésével, de koncepciójában és üzemeltetésében jelentősen eltér attól.

[31] Magyarország esetében ez értelemszerűen Budapest. Nagyobb országokban a tartományi központok is rendelkezhetnek „fővárosi szereppel", azonban egy tartomány nem szükségszerűen tekinthető régiónak. Az állam sajátos felépítése miatt az előbbi alapvetéstől lehetnek eltérések. Ilyen például Svájc, ahol a kantonok rendkívül erős önrendelkezési jogokkal bírnak, ám egy kanton nem tekinthető régiónak, sokkal inkább igaz, hogy egy régió több kantont tartalmaz. Svájc központi régiója (Zentralschweiz) hat kantont foglal magában: Lucerne, Uri, Schwyz, Obwalden, Nidwalden, Zug. Maga a régió pedig csupán 4483 km^2, vagyis nagyságrendileg Fejér megye méretével megegyező. Honi viszonylatban Fejér megye nem lenne önálló régiónak nevezhető.

[32] A MÖK-ök klasszikus értelemben is *Command and Control* (C2) központoknak tekintendők.

[33] Századosi/őrnagyi rendfokozatban vagy azzal megegyező szintű köztisztviselői/közalkalmazotti fokozatban és akinek legalább 2 éves MÖK operátori tapasztalata van.

[34] Az éves MÖK vezetői váltások országosan egymástól eltérő időpontban történnek.

[35] Részletesebben a „Speciális igények" részben.

ahol ez logisztikailag nem okozna problémát. De ugyanez igaz lehet más, például katasztrófavédelmi objektumokra is.

Tételezzük fel, hogy egy veszélyes anyagot szállító vasúti szerelvény balesetet szenved az egyik fővároson kívüli régióban, de lakott területen belül. Ennek okán ötszázas nagyságrendben szorulnak orvosi ellátásra a város lakói, a katasztrófavédelemnek folyamatosan, több ponton kárelhárítási, illetve monitorozási feladata van, a honvédség segít az érintett területek kiürítésében, az Országos Mentőszolgálat végzi a betegek szállítását, két környező kórház a betegek befogadását, míg a rendőrségnek területvédelmi feladatai vannak. A felhasználók számának kis területen történő jelentős növekedése megköveteli a mobil hang- és adatátvitel biztosításának kiterjesztését, amelyet az összes közreműködő felé folyamatosan biztosítani kell, és amelyet a normál TETRA-cellák már nem tudnak kiszolgálni.

Ebben az esetben a regionális MÖK feladatai:

- intézkedik új mobil TETRA-cella felállításáról és hálózatba kapcsolásáról;
- elvégzi a TETRA-felhasználók ideiglenes csoportokba történő átsorolását;
- biztosítja a beavatkozó erők számára a plusz kommunikációs eszközöket;
- kialakítja a képátviteli és videókonferencia ideiglenes útvonalakat az országos gerinchálózat felé;
- elvégzi az adatátviteli tartalmak és vonalak priorálását, hogy a helyszíni erők hang- és adatforgalmai feltétlen elsőbbséget élvezzenek;
- folyamatos egyeztetést végez az országos MÖK-kel;
- elvégzi a védekezésbe későbbiekben bekapcsolandó szervezetek (például kórházak, egyéb egészségügyi intézmények, központi állami szervek) kommunikációs vonalainak előkészítését és biztosítását;
- kialakítja a kitelepített lakosság államigazgatási infokommunikációs kiszolgálását ellátó adatbázisok és állományok elérhetőségét (például az eredeti lakóhely szerint illetékes háziorvosi adatbázisok) a kitelepítési hely szerint illetékes MÖK-kel.

Nemzetközi interoperabilitás

Meg kell teremteni a határokon átívelő földrajzi régiókkal is az interoperabilitást, ami különösen fontos lehet rendvédelmi, katasztrófavédelmi, vagy kutató-mentő feladatok ellátása során.[36] Ennek kapcsán olyan hálózati szegmentálással kell rendelkezni, ahol egy zárt adatátviteli részre ideiglenes hozzáférés biztosítható a szomszédos/szövetséges országok[37] társszerveinek.

[36] Nemzetközi kutató-mentő feladatok esetén lehetséges, hogy egy külföldről Magyarországra érkező egység (akár század szintű is) bekapcsolandó egy komplex végrehajtásba. Ugyanígy lehetséges honi egység(ek) külföldre telepítése, hasonló feladat ellátására. Ilyen lehet például egy kiterjedt erdőtűz, amelynek során a hazai normál tűz- és katasztrófavédelmi képességnek meg kell maradnia.

[37] A szövetség lehet katonai (NATO), igazgatási (Schengeni Egyezmény) vagy egyéb államközi szerződésen alapuló.

Egy határ közelében zajló mentési/katasztrófavédelmi feladat során meg kell oldani, hogy a kijelölt egységek tudjanak egymással adatot megosztani, illetve tudjanak egymással hang alapon is kommunikálni. A kommunikáció szervezésében ez a gyakorlatban rendkívül összetett és nagy tapasztalatot igénylő feladat lehet.

Lehetséges példaként a magyar–osztrák határ környezetében egy ipari/természeti katasztrófa elhárítása során, az Osztrák Szövetségi Hadsereg, a Magyar Honvédség, egy osztrák tartomány rendőrsége, egy magyar megye rendőrsége, a Készenléti Rendőrség meghatározott alegységei, az Országos Mentőszolgálat és az Osztrák Vöröskereszt között kell megoldani úgy az operatív kommunikációt, hogy az állapotról valós időben rendelkezzen információval mindkét ország országos rendőrfőkapitánysága és belügyminisztériuma is. Ehhez kapcsolódhat a két ország légiforgalmi irányítása, amennyiben a művelet a bécsi repülőtér leszálló útvonalában történik, és a végrehajtásban forgószárnyas légi járművek is részt vesznek.

A feladat azonban – *ad-hoc* jelleggel – messze nem lehetetlen, de az érintett osztrák és magyar MÖK (illetve a központok rendszere) nélkül gyakorlatilag elképzelhetetlen.

További feltétel a honi és a regionális együttműködés folyamatos gyakoroltatása, nem csupán a központok, hanem a kapcsolódó szervezetek oldaláról is. Ez azzal (is) jár, hogy a MÖK-személyzetek létszámát úgy kell kialakítani, hogy a folyamatos oktatások és gyakorlatok mellett is elégséges működési létszámmal (és tartalékkal) rendelkezzenek.

Ugyanígy fontos kapcsolatok lehetnek a meglévő tudásközpontok bekapcsolásai, amelyek rendkívül szerteágazó és hasznos tapasztalatokkal rendelkezhetnek. Ilyenek például a NATO kiválósági központjai, ahol nem csupán a szűkebb értelemben vett szaktudás (például Egészségügyi Kiválósági Központ – MILMED COE)[38] hozzáférhető, hanem olyan többnemzeti vagy szervezeti együttműködési tapasztalat is, amely a teljes feladat sikeres végrehajtását támogatja. A kiválósági központoknak pedig ez az egyik deklarált célja, hogy a tagállamok által megismert tudást koncentrálja és megossza. Az együttműködés pedig tovább szélesíti a kiválósági központok saját tapasztalatát.[39]

Speciális igények

A korábbiakban bemutatott katasztrófavédelmi példák is jól szemléltetik, hogy elengedhetetlen a földrajzi helyszíntől független, stabil, 8–12 órán belül telepíthető, nagy adatátviteli képességű (legalább 200 Mbps) vonal és végpont kiépíthetősége. Ennek egyik biztonságos módja mikrohullámú egységekkel valósítható meg, amelyek a legközelebbi arra alkalmas két vezetékes pontra továbbítják az adatforgalmat, majd onnan a regionális MÖK intézkedéseivel az országos hálózatban is elérhetővé teszik. A teljes rendszert üzemeltető szervezet tehát rendelkezne mindazon technikával (például a fentiekben leírt laktanyákban diszlokálva), amelyek segítségével:

[38] MILMED COE: NATO Centre of Excellence for Military Medicine, Budapest.

[39] Kralovánszky Kristóf: NATO Kiválósági Központok és a transzformáció. *Hadtudományi Szemle,* 9. (2016), 4. 141–153.

- a települési ponton helyi hálózat, addicionális TETRA-cella és vezetési pont kialakítható;[40]
- a települési pont és a stacioner végpont között legkésőbb 8 órán belül az első pont–pont kapcsolat kialakítható (amelyen minimálisan 30–50 Mbps átviteli sebesség garantálható – attól függően, hogy az adatátviteli rész a TETRA-rendszerhez kapcsolódik-e, vagy más kapcsolati technológiával alakítják ki);
- a második pont–pont kapcsolat a második stacioner végponttal legkésőbb 16 órán belül kialakítható, legalább 200 Mbps átviteli sebességgel.[41]

Az országos rendszer regionális részében megfelelő lehet, ha minden végpontra olyan kommunikációs modult telepítünk, amely képes legalább két független (két vezetékes, vagy egy vezetékes és egy mikrohullámú) irány kiszolgálására. A modul az adott végpont és a környezetében lévő két másik, vele nagyságrendileg megegyező végpont adatátviteli igényét legyen képes kiszolgálni (amennyiben a végpontok egyenkénti önálló adatátviteli igénye az 500 Mbps sebességet nem haladja meg).

Ilyen végponti kommunikációs modul telepíthető az összes rendőrőrsre, kapitányságra, katasztrófavédelmi kirendeltségre, valamint mentőállomásra és kisebb önkormányzatra.[42]

Ezzel a fix végpontok – a teljes hálózat szempontjából – elágazási pontokká válnak. Ezek a végpontok azok a stacioner pontok, amelyekre a mikrohullámú vagy egyéb, vezeték nélküli irányok bekapcsolhatók – így a fix végpontok vezetékes / vezeték nélküli átjárókként is képesek üzemelni. A folyamatos üzemű végpontok pedig a fent leírtakon keresztül olyan hálózati tartalékkal (vonali és forgalmi egyaránt) rendelkeznek, amelyek garanciát jelentenek a mobil telepítések zökkenőmentes adatátvitelére.

Ideiglenes végpontok kialakítása esetén általában kettős követelmény a mobil hang- és a mobil adatátvitel biztosítása. Előbbit ideiglenes TETRA-cellák kialakításával lehet megvalósítani, míg utóbbit részben a már említett DAB/DVB hibrid technológiával a TETRA-rendszer integrációjával, 30 Mbps sebességig. Konstans 15 Mbps ideiglenes mobil végponti adatátviteli sebességet meghaladó adatátviteli igény esetén más, biztonságos vezeték nélküli hálózat kialakítása szükséges.

---

[40] Ez a vezetési pont lehet a több készenléti szolgálat által régóta vágyott, hosszú tengelytávú teherautó vagy autóbuszalvázra telepített felépítmény, amely az első 6–8 órában saját maga ki tudja alakítani a pont–pont kapcsolatot a stacioner adatátviteli ponttal.

[41] A második vonal kiépítését követően, a feladat várható elhárítási idejétől függően, az első vonal átviteli sebességét szintén 200 Mbps-re kell növelni.

[42] A 2–3000 fős magyarországi települések önkormányzataihoz jelenleg jellemzően publikus internet adatkapcsolat áll csak rendelkezésre, holott egy minősített helyzetben, ahol védelmi feladatokat kell regionális szinten megvalósítani, kulcskérdés a megfelelő minőségű (stabilitású és sebességű) államigazgatási adatkapcsolat. Ugyanez elmondható a honi közfinanszírozott egészségügyi ellátásban működő kis és közepes orvosi rendelők adatátviteli rendszeréről is, ahol a publikus internet túlterhelődése esetén jelentős fennakadások keletkezhetnek.

Valós redundancia

Amennyiben egy komplex rendszerre bízza az állam a saját infokommunikációs adatátvitelét, alapfeltétel a redundancia. Országos állami adatátviteli rendszerrel szemben támasztott fundamentális követelmény a rendkívül magas funkcionális rendelkezésre állás: 99,75% / nap (naponta 3,6 perc megengedett kiesés), amely adott esetben óránkénti 99,75%-os követelményt is jelenthet. Ilyen arányokat kizárólag meleg tartalékokkal lehetséges megoldani, ahogy azt a hálózati topológiák résznél is bemutattuk.

Számos szolgáltató kiváló marketingfogásokkal igyekszik egy adatátviteli vonalat – komoly felár ellenében – „redundánssá" tenni. Egy valós példán alapuló[43] egészségügyi szolgáltató naponta 160–200 GB új adatmennyiséget hoz létre radiológiai vizsgálatok formájában. Az adatmennyiség 50%-át távleletezéssel értékeli ki, vagyis 80–100 GB adatot minden nap feltölt a távleletező orvosoknak. Egy vizsgálat átlagosan 1 GB méretű. A távközlési szolgáltató ajánlata 4G-tartalék volt a 200 Mbps szinkron vonali sebességű adatátviteli kapcsolat mellé. Nyilvánvaló, hogy a 4G-tartalék ideális körülmények között (tökéletes kapcsolat a cellán belül, átlag alatti cellaterhelés) lehet megoldás, ám az esetek döntő részében (különösen nappal) alkalmatlan akár 30 perces optikai vonali kiesés áthidalására, mivel a cellák terheltsége jellemzően magas, a 4G-modem külső antennája is jellemzően egy vasbeton szerkezetű beltérben helyezkedik el, amely nyílászáróval nem rendelkezik, így sokszor a 4G valós átlagos átviteli sebesség a 150–200 Kbps mértéket sem érte el. Ilyen értelemben tehát (ebben a konkrét esetben) nem beszélhetünk valósan funkcionális vonali redundanciáról.[44]

A példa is jól mutatja, hogy a vonali sebesség mellett legalább annyira fontos a vonal heti, napi, óránkénti, illetve akár ötperces intervallumokban mért átlagos kihasználtsága (adatátviteli igénye) is, hiszen ebből számíthatók a lehetséges (kumulált) tartalékvonalak és kapacitások.

Különleges üzem, reziliencia

Az országos közös rendszer működése normál üzeműnek nevezhető, ha a főbb vonalakon az átlagosnak megfelelő terhelés jelentkezik, és a normál karbantartások miatt üzemen kívüli kapcsolatokon kívül az elfogadott mértéket nem meghaladó mértékű meghibásodás tapasztalható. Különleges üzemű a rendszernek az az állapota, amikor bármilyen okból, operátori vagy vezetői döntés (utasítás) alapján jelentős vonali átterheléseket kell végezni, illetve bizonyos forgalmakat időben és/vagy adatmennyiségben korlátozni kell. Különleges üzem lehet országos és/vagy regionális.

Az átterhelések méretéről, mértékéről az adott helyzetnek megfelelő szinten az illetékes MÖK dönt – adott esetben az országos MÖK jóváhagyásával.

---

[43] A szerző saját tapasztalata. Sem az egészségügyi intézmény, sem a távközlési szolgáltató megnevezése a példa szempontjából nem releváns.

[44] Az 1–2 Mbps érték sem lett volna operatív szempontból elfogadható – ebben az esetben a minimális szint 5–8 Mbps között van.

A különleges üzem egy sajátos fajtája a szigetszerű üzem, amely egy, az országos hálózatról részlegesen vagy teljesen leszakadt hálózati szegmens önálló üzemelését jelenti. Az ilyen különleges üzem több szinten értelmezhető.

Az egyik esetben helyi szintről van szó, ahol a hálózat részleges kiesései csak egy adott minimális terület korlátozottságát vagy kiesését eredményezik, és nem járnak a hálózat fennmaradó részének jelentős megakadásával. Ekkor is törekedni kell az olyan hálózati kialakításra, hogy csökkentett sávszélességgel, de alapvető államigazgatási feladatok ellátására képes maradjon (központi nyilvántartások lekérdezése, alapszintű költségvetési, számviteli és iktatási feladatok ellátása). Erre a legkézenfekvőbb megoldás egy legalább 3G-szintű stabil, mobil adatátviteli tartalék kialakítása – amely szintén állami adatátviteli hálózatként üzemel.

A második esetben egy hálózati rész (rész-régió) kapcsolata megszakad az országos gerinchálózattal, ilyenkor már azonban nem megoldás az egyenkénti 3G-tartalék alkalmazása, vagyis a régió központjával kell tudni kapcsolatot teremteni és onnan üzemeltetni infokommunikációs alkalmazásokat és ott elérni adatbázisokat.

A harmadik pedig az országos szint: Magyarország példájánál maradva legalább három olyan főközpontnak (hálózatüzemeltetési központ – *Network Operations Center*) kell lennie, amelyek közül ha az egyik időlegesen kiesik, a másik kettő teljes mértékben ki tudja szolgálni a teljes országos infrastruktúrát úgy, hogy a kiesett központ visszatérésekor a szükséges szinkronizációk se okozzanak fennakadást a kétközpontú (és az országos) működésben.

Ez a típusú többrétű és rétegeken belül is elosztott működési modell a rendszer rezilienciájának kulcsa. Amíg tehát a redundancia három fő rétege a vonali üzem, vagyis a klaszteren belüli, klaszterek közötti és gerinchálózati adatátvitel hibatűrése, addig a tartalmi üzem hibatűrése az elosztott adattároláson keresztül valósul meg, melyről egy korábbi írásban részletesen esik szó.[45]

Kiberbiztonság[46]

A teljes rendszer kiberbiztonsága az egyik legfőbb kérdés. Amikor egy államot működtető komplex adatátviteli hálózatról van szó, akkor a bizalmasság, sértetlenség és rendelkezésre állás hármasságában kompromisszumot kötni nem lehetséges. Szinte biztosan megjelenő ellenérv a központosítással szemben az abban rejlő hatalmas lehetséges sérülékenység, hiszen egy központi rendszer kiiktatása az állam funkcionális működésének teljes leállásához vezethet.

[45] Kralovánszky Kristóf: Elosztott adattárolás egyes kérdései. *Hadmérnök,* 13. (2018), 4. 297–305.; Charles Lamb: The guiding principles for cloud-scale, geo-distributed databases. *Database Journal,* September 24, 2015.

[46] Jelen tanulmány elsődleges célja nem egy ilyen komplex rendszer kiberbiztonságának tételes levezetése (terjedelmi okokból kulcspontokat van csak lehetőség megemlíteni), hanem a komplex felépítés bemutatása.

A rendszer központisága ugyanakkor csak virtuális, mert a centralizáltság nem a topológiában vagy az egyetlen központi elosztóban valósul meg, hanem a felhasználás sokoldalúságában.

Az alkalmazandó, mesterséges intelligencián alapuló állandó forgalmi elemzések, a többrétegű humán felügyelet, a fizikai elkülönítettség, az alkalmazási síkonként és tartalmi funkciókként megjelenő belső redundanciák mind-mind arra hivatottak, hogy a rendszer egy esetleg sikeres támadása csak a támadás pontjában okozzon minimális fennakadást és az a fennmaradó részekre ne legyen hatással – vagyis a rendelkezésre állás és a sértetlenség a nem érintett részeken biztosított maradjon.

A bizalmasság és a sértetlenség másik része ugyanígy, rendkívül szerteágazó és multifaktoros azonosítási rendszereken (hardver és szoftver modulokra vonatkozóan egyaránt) keresztül valósul meg, amelyben az ellátási lánc biztonsága, vagyis a beépített/felhasznált hardverek követése is kulcsszerepet kap, az alapvetően tiltó szabályrendszeren keresztül. Itt is jelentős szerephez jutnak a mesterséges intelligencián alapuló, valós idejű elemzések, amelyeket a folyamatosan és több szinten kialakított szakértő humán felügyelet egészít ki és tesz teljessé.

Összefoglalás, következtetések

A kormányzati és állami adatátviteli rendszerek egyre szerteágazóbb felhasználása szükségszerűen eredményezheti a különböző ágazatok elkülönült hálózatainak megjelenését, ezzel több párhuzamos átviteli kapacitás létrejöttét. A rendszerek felügyelete önmagában is egyre komolyabb kihívást jelent az üzemeltetők számára, amely nem elsősorban a technikai rendelkezésre állást, hanem az adat- és információbiztonságot állítja fókuszba.

Valódi funkcionális probléma a kiépült önálló hálózatok rugalmatlanságában van és lesz, mert a legritkább esetben képesek egy vészhelyzeti eseményhez gyorsan adaptálódni. Ugyanekkora gazdasági problémát is magukban hordoznak, hiszen a hálózatok fenntartója (és kiépítője) az állam – ha többszörös áttéteken keresztül is –, amely ezeken keresztül fölösleges párhuzamos kapacitásokat finanszíroz.

A hatékonyság, a rugalmasság és a folyamatosan skálázható hibatűrő rendelkezésre állás integrált irányítás mellett valósítható meg, ami egyúttal a gazdaságosabb működést is biztosítani tudja. Mivel a vezetékes gerinchálózati rész Magyarország legnagyobb részén – bizonyos szükséges kiegészítésekkel – rendelkezésre áll, a vázolt komplex adatátviteli rendszer elvi bevezethetősége nem szükségszerűen irracionális. A teljes koncepció ugyanakkor nem Magyarország-specifikus, vagyis az adott ország sajátosságaival módosítva bevezethető bármilyen 5–15 milliós lakosságú, közepes vagy magas fejlettségű országban.

Egy országos rendszer kiépítése és a tanulmányban foglalt komplexitású üzemeltetése optimista becslések alapján 24–30 hónap, egy legalább 12–18 hónapos tervezést követően. Maga az optikai hálózat azonban sokkal hosszabb ideig fogja a rendszert kiszolgálni, a végberendezések pedig tervezetten cserélhetők. Egészséges állapotban a teljes hálózaton

lesznek első, második és harmadik generációs elemek és modulok[47] – ezek azonban homogén rendszerként kiválóan üzemeltethetők maradnak.

A rendszer által biztosított stabilitás és rugalmasság érezhetően megnöveli a honvédelmi, rendvédelmi, katasztrófavédelmi és egyéb szolgálatok képességeit, különösen a normál feladatellátástól eltérő időszakokban, így járulva hozzá a lehetségesen bekövetkező károk minimalizálásához és akadályozva meg emberi életek értelmetlen elvesztését. Ezzel egyidőben jelentős honi háttéripar és képzési rendszer kiépülését és folyamatos működését teremti meg, valamint eredményét tekintve az ország kiberbiztonságát és ezzel szuverenitásának biztosíthatóságát jóval magasabb szintre emeli.

Felhasznált irodalom

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. Online: http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.350656

Bancsics Ferenc: *Az NTG helye a Gigabit társadalom fejlesztésében.* HTE INfokom 2018. Online: www.hte.hu/documents/4176585/4584083/Bancsics_Ferenc.pdf

CentraCore Optical Ground Wire (OPGW). *Aflglobal.com.* Online: www.aflglobal.com/Products/Fiber-Optic-Cable/Aerial/OPGW/CentraCore-Optical-Ground-Wire-(OPGW).aspx

Faster than the standard – higher data rates with TETRA. *News from Rohde & Schwarz,* 182. (2004), 2. 21–23. Online: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_news_from_rs/182/n182_accessnet.pdf

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kralovánszky Kristóf: A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle,* 7. (2019), 3. Online: https://doi.org/10.32561/nsz.2019.3.4

Kralovánszky Kristóf: Elektronikus határvédelmi rendszerek jellemző sebezhetőségei és védelmük lehetőségei. *Hadmérnök,* 14. (2019), 1. 271–282. Online: http://hadmernok.hu/191_22_kralovanszky.pdf

Kralovánszky Kristóf: Elosztott adattárolás egyes kérdései. *Hadmérnök,* 13. (2018), 4. 297–305. Online: http://hadmernok.hu/184_23_kralovanszky.pdf

Kralovánszky Kristóf: NATO Kiválósági Központok és a transzformáció. *Hadtudományi Szemle,* 9. (2016), 4. 141–153. Online: http://epa.oszk.hu/02400/02463/00033/pdf/EPA02463_hadtudomanyi_szemle_2016_04_141-153.pdf

Lamb, Charles: The guiding principles for cloud-scale, geo-distributed databases. *Database Journal,* September 24, 2015. Online: www.databasejournal.com/sqletc/the-guiding-principles-for-cloud-scale-geo-distributed-databases.html

LeMahieu, Paul – Bohossian, Vasken – Bruck, Jehoshua: *Fault-tolerant switched local area networks.* Proceedings of the First Merged International Parallel Processing Symposium and Symposium on Parallel and Distributed Processing. IEEE Xplore, Orlando, 1998. 747–751. Online: 10.1109/IPPS.1998.670011

[47] A hálózat életkora szempontjából vizsgálva.

Masterson, Keith D. – Novotny, David R. – Koepke, Galen H.: *Electromagnetic shielding characteristics of optical-fiber connectors.* NIST Publications, Boulder, Colorado, 1997. Online: https://doi.org/10.6028/NIST.TN.1383

Médard, Muriel – Lumetta, Steven S.: Network reliability and fault tolerance. In Proakis, John G. (ed.): *Wiley Encyclopedia of Telecommunications.* Hoboken, New Jersey, John Wiley & Sons, 2003. Online: 10.1002/0471219282.eot281

Netzpläne helfen bei der Orientierung. *Rhein-Main-Verkehrsverbund.* Online: www.rmv.de/c/fileadmin/documents/PDFs/_RMV_DE/Linien_und_Netze/Streckennetz/Liniennetzplaene/RMV-Schnellbahnplan.pdf

A Katonai Műszaki Doktori Iskolában folyó képzés és kutatás a műszaki tudományterülethez tartozó tudományágaknak a teljes védelmi szektorban történő alkalmazására irányul. A hallgatók tudományos tevékenységüket gyakran több tudományterület és tudományág határterületén művelik, és a kutatásaik során azok interdiszciplináris kérdéseire, szinergiáira fókuszálnak.

Mindezt az ebben a kötetben található írások is igazolják. A szerzők olyan tudományos problémákat feszegetnek, mint például a blokkláncok és a mesterséges intelligencia alkalmazhatósága a kiberhadviselésben, a Mi–24 helikopterek elektronikai hadviselési képességeinek fejlesztése vagy az állami célú adatátviteli rendszerek integrálhatóságának kérdései. A környezetbiztonság és a vízgazdálkodás, valamint a vízbiztonság területéhez köthetően is több írással találkozhatunk a kötetben.