

## KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK MAGYARORSZÁGON<sup>1</sup>

### *Absztrakt*

*Ma már a fejlett nyugati társadalmak mindennapjaiban nincs olyan terület, ahol ne lenne meghatározó tényező a számítógép-hálózat, valamint a hálózatok által összekötött megannyi információs infrastruktúra és az ezekre épülő valamilyen szolgáltatás. Mindezek azonban komoly veszélyforrást is jelentenek, hiszen — amennyiben elfogadjuk azt az állítást, miszerint ezek a rendszerek mindennapjaink részévé váltak —, akkor ezek teljes, vagy részleges hiánya, illetve működésképtelensége is igen komoly veszélyeket idézhet elő. Jelen írás célja, hogy kiemelve néhány hazai információs infrastruktúrát bemutassa, hogy hazánk is jelentős mértékben függ ezektől a rendszerektől.*

*Nowadays there are not such fields in our everyday life where we are not depending on one or more information infrastructures. However, these systems mean increasingly risks. Goal of this paper is to bring forward some Hungarian information infrastructure which the country depend on.*

**Kulcsszavak:** *infrastruktúra, kritikus infrastruktúra, kritikus információs infrastruktúra ~ infrastructure, critical infrastructure, critical information infrastructure*

### BEVEZETÉS

Ahogy nő az információtechnológia dominanciája a mindennapokban, úgy erősödnek azok a szakértői figyelmeztetések, amelyek azoknak a veszélyeknek a fokozódására próbálják meg felhívni a figyelmet, amelyek e dominanciából eredeztethetőek.

A veszélyek oka elsősorban az, hogy ahogy nő a számítógépek száma úgy nő annak a veszélye, hogy a számítógépeinket megtámadják, illetve a megtámadott gépeket — akár azok tulajdonosainak tudta nélkül — további támadásokra felhasználják.

Számítógépek természetesen nem csak otthonainkban vannak. Azokat az infrastruktúrákat, amelyek a mindennapi életünket kiszolgálják, segítik, vagy támogatják, szintén számítógépek, illetve számítógépes hálózatok működtetik és irányítják.

Mindezeknek megfelelően jelen írás célja, hogy bemutassa melyek azok az infrastruktúrák, amelyek a legfontosabbak — egyben a legsebezhetőbbek — az információs társadalom számára. Bemutatja egy változatban, hogyan osztályozzák, csoportosítják ezeket, a rendszereket. Az írás kitér a legfontosabb hazai infrastruktúrákra, ismerteti ezek rövid működését, rendszerirányítását.

---

<sup>1</sup> A cikk a Robothadviselés 7. tudományos konferencián elhangzott előadás szerkesztett változata. Az írás nagymértékben támaszkodik Kovács László: *Kritikus információs infrastruktúrák* című egyetemi jegyzetére (ZMNE, Budapest, 2007).

## INFRASTRUKTÚRÁK

Az információs társadalom kiépítése, majd zavartalan működése számos nélkülözhetetlen rendszert és eszközt — *infrastruktúrát* — feltételez, amelyek a társadalom és a gazdasági élet funkcióit támogatják, vagy ezeken keresztül valósulnak meg a különböző — a társadalom működése szempontjából elengedhetetlen — funkciók, illetve feladatok.

Természetesen ezzel kapcsolatosan felmerül a kérdés, hogy mit is értünk egyáltalán infrastruktúra alatt.

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése „*a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.*” [1]

A Magyar Larousse Enciklopédia meghatározása szerint az infrastruktúra „*a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.) Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák).*” [2]

Egy másik meghatározás szerint az infrastruktúra nem más, mint „*egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.*” [3]

1997-ben egy, az akkori amerikai elnök, Bill Clinton utasítására létrehozott bizottság a következőképpen definiálta az infrastruktúra fogalmát (természetesen az Egyesült Államok vonatkozásában): „*Az infrastruktúrák olyan egymástól függő hálózatok és rendszerek összessége, amelyek meghatározott ipari létesítményeket, intézményeket (beleértve a szakembereket és eljárásokat), illetve elosztó képességeket tartalmaznak. Mindezek biztosítják a termékek megbízható áramlását az Egyesült Államok védelmi és gazdasági biztonságának fenntartása, valamint a minden szinten zavartalan kormányzati munka és a társadalom egésze érdekében.*” [4]

Amennyiben az információs társadalom szempontjából vizsgáljuk az infrastruktúrák kérdését, akkor az infrastruktúra fogalmán belül általános feladatú és információs rendeltetésű infrastruktúrát különböztethetünk meg.

Az **általános feladatú infrastruktúra** fogalma alatt olyan állandóhelyű vagy mobil építmények, eszközök, rendszerek, hálózatok, az általuk nyújtott szolgáltatások, és működési feltételek összességét kell érteni, amelyek valamilyen társadalmi, gazdasági vagy akár katonai funkciók és rendszerek feladatorientált, zavartalan és hatékony működését teszik lehetővé. [3] Ilyen társadalmi funkciók lehetnek (természetesen a teljesség igénye nélkül, hiszen a társadalom különböző, szerteágazó területei számos egyéb funkcióval is bírhatnak):

- közigazgatási;
- szállítási;
- ellátási;
- hírközlési;
- vezetési;
- védelmi (ország védelem, rendvédelem, katasztrófavédelem, polgári védelem);
- oktatási;
- egészségügyi;
- tájékoztatási.

Az **információs rendeltetésű infrastruktúrák** olyan állandóhelyű vagy mobil létesítményeket, eszközöket, rendszereket, hálózatokat, illetve az általuk nyújtott szolgáltatásokat jelentik, melyek az információs társadalom működéséhez szükséges információk megszerzését, előállítását, tárolását, szállítását és felhasználását teszik lehetővé.

Ebből a kettős felosztásból is láthatjuk, hogy azok nagyon sokszor egymást átfedő területeket is érintenek, illetve például az információs rendeltetésű infrastruktúrák — vagy

azok egyes rész-elemei — sok esetben megtalálhatóak az általános rendeltetésű infrastruktúrákban.

Tovább vizsgálva az információs rendeltetésű infrastruktúrákat, röviden **információs infrastruktúrákat**, megállapíthatjuk, hogy azok „*az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrárendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját.*” [5]

Az információs infrastruktúrákon belül különböző rendeltetésű és típusú infrastruktúrahalmazokat különböztethetünk meg. Rendeltetésük (feladatuk) szerint az információs infrastruktúrákat az alábbi két nagy csoportra lehet osztani:

- funkcionális (alap) információs infrastruktúrákra és
- támogató információs infrastruktúrákra.

A **funkcionális információs infrastruktúrákat** feladatorientált információs szolgáltató infrastruktúráknak is lehet nevezni. Rendeltetésük, hogy fizikailag lehetővé tegyék a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végezzenek. Az információs társadalom információs infrastruktúráin belül ezek az elsődlegesek. Biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását. A funkcionális információs infrastruktúrák rendszerint nagykiterjedésű, bonyolult szervezésű hálózatok vagy rendszerek formájában működnek. [3]

A **támogató információs infrastruktúrák** a kutató, fejlesztő és ellátó információs infrastruktúrák gyűjtő megnevezése (más néven háttér információs infrastruktúráknak is nevezhetők). [5] Rendeltetésük, hogy létrehozzák, és folyamatosan biztosítsák az alapvető információs szolgáltatásokat végző funkcionális információs infrastruktúrák zavartalan működéséhez és fejlődéséhez szükséges szellemi és anyagi alapokat, valamint támogató háttereket.

Az információs termelési korszak és az információs társadalom kibontakozásával kialakuló globális gazdaságot a globális információs környezet veszi körül. Ennek a globális környezetnek a műszaki alapját az a globális információs infrastruktúra képezi, amely nem más, mint azoknak a vezetékes és vezeték nélküli távközlési rendszereknek, valamint számítógép-hálózatoknak összessége, amelyek a globális információcserét biztosítják.

E hálózatok digitális jeltovábbító közegei az optikai kábelek és rádiócsatornák, melyek a föld felszínén, a föld alatt, a tenger felszíne alatt vagy a föld körüli, közeli kozmikus térben — űrben — továbbítják az információkat. Ebben a globális információs közműben egyre nagyobb szerepet tölt be az internet. A rohamos ütemben bővülő globális elektronikus kereskedelem és elektronikus pénzpiac egyre nagyobb mértékben veszi igénybe az internetet. A globális információs környezetben — az információs közművek hálózatán keresztül — a világ minden érintett globális, regionális és nemzeti szerve, intézménye és működési rendszere részt vesz.

## KRITIKUS INFRASTRUKTÚRÁK

Amennyiben az infrastruktúrákat nemzetbiztonsági szempontból vizsgáljuk, és feltérképezzük azokat a kihívásokat és veszélyeket, amelyekkel napjainkban szembe kell néznünk, akkor **kritikus és sebezhető infrastruktúrákat** különböztethetünk meg. Ezeknek az infrastruktúráknak a működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe. Ezért alapvető fontosságú, hogy feltárjuk, és pontosan behatároljuk e kritikus infrastruktúrákat, mivel egy információs támadásnak — azok információs rendszerein keresztül — potenciális célpontjai lehetnek. [3]

*„A kritikus infrastruktúrák veszélyeztetettségének feltérképezése, mérése, értékelése, s a szükséges védelmi intézkedések meghozatala előbb azt feltételezi, hogy a feltérképezéstől az intézkedésig egyetértés legyen abban, mi is az a kritikus infrastruktúra. Míg az infrastruktúra fogalma kellő körültekintés árán kielégítő pontossággal meghatározható, a kritikusság ismérvei sokrétűek, szerteágazóak, tudomány- és iparáganként változnak. Egy infrastruktúra tehát nagyon sok szempontból lehet kritikus, kritikussá minősítéséhez viszont az is elég, ha csak egyetlen egy kritérium szerint az. A kritikus infrastruktúra fogalmának meghatározása ennek megfelelően nem egységes.” [6]*

Mindezek alapján tehát a már a kritikus infrastruktúrák feltérképezése is meglehetősen nehéz és bonyolult feladat, mert *„ami kritikus (infrastruktúra) helyileg, az nem biztos, hogy kritikus az állam számára is. Ráadásul, erről gyakran még pontos információ sincs, hiszen jellemzően területi, vagy helyi szinten nem rendelkeznek szakszerű, tudományosan megalapozott kockázatértékeléssel.” [7]*

Születtek azonban olyan módszerek, amelyek alkalmasak lehetnek a kritikusság mérésére az infrastruktúrák vonatkozásában is. Az egyik ilyen szerint három tényezőt kell figyelembe venni a meghatározáshoz. E három tényező a következő [8]:

- Hatókör: amellyel a kritikus infrastruktúra vagy annak részének elvesztését, elérhetetlenségét földrajzi kiterjedéssel méri. Ez lehet nemzetközi, nemzeti, regionális, területi vagy helyi.
- Nagyságrend: amely a veszteség vagy behatás mértéke a következőképp mérhető: Nincs hatás, minimális, mérsékelt vagy jelentős. A nagyságrend megállapításához a következőket is figyelembe lehet venni:
  - Népeségre gyakorolt hatása (az érintett lakosság száma, áldozatok, betegségek, súlyos sérülések, kitelepítések)
  - Gazdasági hatás (GDP-re gyakorolt hatása, jelentős gazdasági veszteség, és/vagy termelés, szolgáltatás fokozatos romlása)
  - Környezetvédelmi hatás (a lakosságra és lakókörnyezetére gyakorolt hatás)
  - Interdependencia (a kritikus infrastruktúrák egyéb elemei között)
  - Politikai hatás (az államba vetett bizalom)
- Időbeli hatás: amely megmutatja, hogy az adott infrastruktúra vagy egyes elemének vesztesége mennyi ideig fejt ki komoly hatását (azonnal, 24—48 óra, egy hét, hosszabb időtartam).

Természetesen egy-egy infrastruktúrának nem minden eleme tekinthető kritikusnak, még abban az esetben sem, ha kritikus infrastruktúráról beszélünk. Ezért szükség lehet azonosítani és meghatározni azokat az elemeket, amelyek a legkritikusabbak, azaz amelyek támadásával, és amelyek kiesésével, részleges, időleges, vagy teljes működésképtelenségével a legjelentősebb mértékben okozhatók komoly humán (emberi élet) vagy anyagi (gazdasági) kár. Az infrastruktúrák méretének és összetettségének mérése lehetőséget teremthet beazonosítani ezeket a kritikus elemeket.

A kritikus infrastruktúrák meghatározása során a rendszerek prioritálása is komoly segítséget nyújthat. Egyfajta ilyen prioritási rend kialakítása lehet a következő [8]:

1. Önmagukban kritikus létesítmények
2. Sérülésük több infrastruktúra működését is érinti
3. Interdependencia
4. Földrajzi elhelyezkedés
5. Tulajdonviszonyok

Számos országban (nemzetközi szervezetben, szövetségben) megtörtént az infrastruktúrák számbavétele, valamint csoportosítása. Az Európai Unió ilyen besorolása a következő [9]:

- energia (olaj és gáztermékek, finomítók, tárolás a csőhálózattal, villamosenergia-előállítás, és továbbítás);

- információs és kommunikációs technológiák (információs rendszerek és hálózatok védelme, műszerautomatizálás és irányító rendszerek, internet, vezetékes telekommunikáció biztosítása, mobil telekommunikáció biztosítása, rádió kommunikáció és navigáció, műholdas kommunikáció, műsorszórás);
- víz (ivóvízellátás biztosítása, vízminőség ellenőrzése, vízmennyiség biztosítása és szinten tartása);
- élelmiszer (élelmiszer ellátás biztosítása, élelmiszer biztonság felügyelete);
- egészségügy (járóbeteg és kórházi ellátás, gyógyszer és oltóanyag ellátás, laboratóriumok);
- pénzügyek (nem állami pénzügyi rendszer és szolgáltatások, kormányzati pénzügyi feladatok);
- közbiztonság (közbiztonság fenntartása, biztonság, igazságügyi rendszer)
- polgári adminisztráció (kormányzati funkciók; fegyveres erők; polgári adminisztráció szolgáltatásai; készenléti szervek; postaszolgáltatások);
- szállítás (közúti, vasúti, légi közlekedés, belföldi vízi szállítás, tengeri hajózás);
- vegyi és nukleáris ipar (vegyi és nukleáris anyagok, összetevők gyártása, feldolgozása, tárolása, veszélyes anyagok szállító csővezetékei);
- űr és kutatás (űr, kutatás).

## KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

Napjainkban a **kritikus infrastruktúrák nem egyeznek meg a kritikus információs infrastruktúrákkal**. A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló zöld könyv szerint „*kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, internet, műholdak stb.)*”. [9]

Mint a megfogalmazásból látszik, a dokumentum is különbséget tesz e két fajta infrastruktúra kategória között. Korábban egy ország kritikus infrastruktúrái fizikailag és logikailag is önállóak voltak, egymástól csekély mértékben függtek. Az információtechnológia fejlődése következtében azonban napjainkban e rendszerek már egyre inkább automatizáltak és egymással szoros kapcsolatban állnak. [10]

Mint ahogy arra már utaltunk, szinte minden kritikus infrastruktúrát különböző szintű és rendeltetésű infokommunikációs rendszereken keresztül vezérelnek, irányítanak és ellenőriznek. Ennek megfelelően, amennyiben példaként ki akarunk emelni egy-egy rendszert, akkor az ország nyilvános mobil távközlő hálózata, mint önmagában is kritikus infrastruktúra, és egyben kritikus információs infrastruktúra is megnevezhető, vagy akár például az energiaellátó rendszert irányító, vezérlő számítógép-hálózatok is ezek közé sorolhatók. [11]

Mindezek alapján tehát fontossági sorrend-, valamint a teljesség igénye nélkül egy ország kritikus információs infrastruktúrái közé a következők tartozhatnak:

- energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- kommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás számítógép-hálózatai;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai;
- kormányzati és önkormányzati számítógép-hálózatok.

Az elmúlt időszakban a különböző infrastruktúrák nagyon sokszor különösen jó célpontokat jelentettek a különböző támadásoknak. Ugyanakkor, amíg a támadások csak a fizikai dimenzióban fenyegettek, addig az országhatárok bizonyos fokú védelmet jelentettek. Az infokommunikációs rendszerek globálissá válásával azonban az információs dimenzióból

érkező fenyegetéseknek nem szabnak semmiféle korlátot az országok határai, hiszen egy ország gyakorlatilag bármely információs infrastruktúrája elérhető anélkül, hogy annak fizikai közelébe (államhatárokat átlépve) kellene jutni. Ezt a veszélyforrást tovább erősíti az a tény is, hogy ma „már korlátozott erőforrások is elegendőek az infokommunikációs rendszerekre alapozott kritikus infrastruktúráink elleni támadások megtervezésére és kivitelezésére. A különböző egyéni aktivisták, jogosulatlan felhasználók és terroristák aszimmetrikus fenyegetései részben kibővítették, részben, pedig felváltották a jól ismert háborús fenyegetettségeket.” [12]

E tekintetben kijelenthetjük, hogy a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik. [11]

## KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK MAGYARORSZÁGON

Magyarország is elkötelezte magát az információs társadalom építése mellett. Ennek megfelelően elkezdődött e folyamat humán és infrastrukturális feltételeinek kialakítása. Az infrastruktúra kiépítése terén hazánk komoly eredményeket ért el. Jelentős fejlődés tapasztalható a különböző infokommunikációs rendszerek kiépítése és fejlesztése során. Ugyanakkor — a többi Európai Unió országához hasonlóan — hazánkban is meg kellett történnie azoknak a veszélyeknek a feltárása, amelyek egyrészt az információs társadalom alappilléreit, azaz az információs infrastruktúrákat, másrészt a 21. század veszélyeiből következően egész társadalmunkat fenyegetik.

A Magyar Köztársaság nemzeti biztonsági stratégiája (2073/2004. (IV. 15.) Korm. Határozat) a II.1.6. pontban tárgyalja *Az információs társadalom kihívásai* címmel az előbb említett veszélyeket: „A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára.” [13]

Mindezekon túl a magyar kormány meghatározta azokat az infrastruktúrákat, amelyekre elsősorban — a terrorizmus elleni harcban — a civil lakosság védelme érdekében különös gondot kell fordítani. Ezek a következők: [14]

- energiaellátás;
- közművesítés;
- közlekedés;
- szállítás;
- távközlés;
- elektronikus adatforgalom;
- informatikai hálózat;
- bankrendszer;
- szolgáltatások;
- média;
- ivóvíz;
- élelmiszer alapellátás;
- egészségügyi biztosítás.

Ezekből is jól látszik, hogy számos olyan infrastruktúra van, amelyek működése alapvető fontosságú hazánk mindennapi életének biztosítása területén.

Terjedelmi korlátok miatt azonban ezek közül az infrastruktúrák közül csak kettőt mutat be jelen írás: elsőként a hazai — kritikus — infrastruktúrák közül az energiaellátás szektorból a **villamosenergia-rendszert, illetve annak irányítását**, majd ezt követően az információs és telekommunikációs szektorokból a **hazai internet kialakulását**.

## Villamosenergia-rendszer Magyarországon

A villamos energia egyik sajátos jellemzője, hogy ez – eltérően a legtöbb energiától – nem tárolható, azaz ebből minden pillanatban éppen annyit kell termelni, mint amennyi a pillanatnyi fogyasztás. Ennek megfelelően az igényként felmerülő fogyasztás és a termelés egyensúlyát mindenkor fenn kell tartani.

Az ország fogyasztóinak villamosenergia-ellátása a villamosenergia-rendszer feladata. Ez a rendszer a villamos művekből (termelő, szállító, elosztó berendezések) és a hozzájuk csatlakozó fogyasztókból áll. Az erőművek termelik meg a fogyasztók által igényelt villamosenergiát, amely a 220-400 kV-os hálózat segítségével jut el az áramszolgáltatók betáplálási pontjaihoz, ahonnan az elosztás 120 kV-os vezetéseken történik a középvezetési (20 kV, 10 kV) táppontokig.

Az ellátás biztonságát növeli, hogy a 220-400 kV-os alaphálózat, a 120 kV-os főelosztó hálózat és a fogyasztók közvetlen ellátását biztosító közép- és kisfeszültségű hálózat túlnyomó része hurkolt. Ennek megfelelően az állomásokot összekötő vezeték hálózatot alkotnak, így egy elem elvesztése nem okozhat nagyobb kiterjedésű ellátás kiesést.

A biztonságot fokozza, hogy az egyes országok hálózatai úgynevezett rendszeregyesülésként egymással összekapcsolva üzemelnek. Ez nem csak a topológiai biztonságot növeli, hanem az erőművekben keletkezett üzemzavarok esetén a kiesett teljesítmény pótlásában is részt vesznek az együttműködő energiarendszerek. Az országok közötti kapcsolat az energia-szolgáltatás fizikájából adódóan rendkívül szoros, bármely rendszerben is lép fel hiány, a vele szinkron működő energiarendszerek mindegyike automatikusan részt vesz annak pótlásában. Ez az együttműködés Nyugat- és Közép Európa minden országára kiterjed és kb. 300.000 MW teljesítményű energiarendszer összehangolását jelenti (összehasonlításként a magyar energiarendszer éves csúcsteljesítménye nagyságrendileg 6000-6500 MW).

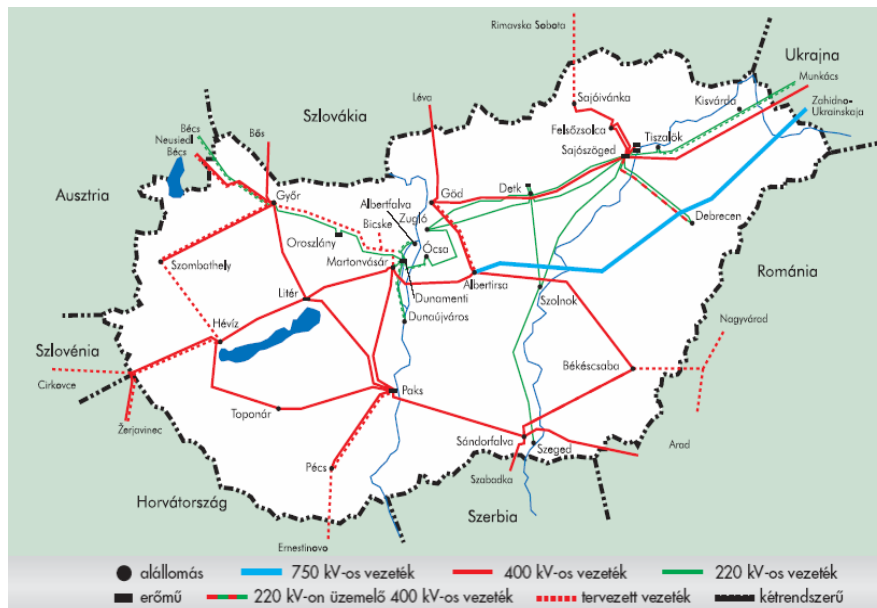
Az energiarendszer szórt struktúrája, többszörösen hurkolt topológiája nagy biztonságú ellátást biztosít. Ellátási zavarok csak kis területre lokalizáltak, a fogyasztók kis csoportjánál és rövid ideig lépnek vagy léphetnek fel. A gyakorlat azt mutatja, hogy nagyon kevés azoknak az üzemzavaroknak a száma, amelyeknél a fogyasztói kiesés a jelentésre már kötelezett 50 MWh-t eléri, vagy meghaladja. [15]

A magyarországi villamosítás története a XIX. század második feléig nyúlik vissza. Két évvel a világ első közcélú villamos művének New York-i üzembe helyezése után az Osztrák-Magyar Monarchiában, Temesvárott létesült általános célú villamos mű 1884-ben. A mai Magyarországon a mátészalkai villamosítás 1888-ban, Párizsával egyidejűleg indult el. Ettől az időtől számítjuk a magyar villamosenergia-ipar működésének kezdetét is. [16]

Ma a hazai villamos erőműveink teljesítőképessége elméletileg több mint 8200 MW. Vannak azonban olyan áramtermelő egységek, amelyek hosszú ideje állnak, de a kapacitásmérlegben még számolnak velük, ugyanakkor ezek indítása azonban bizonytalan lehet. A csúcscsökkentés időszakában – a hazai fogyasztás kielégítésére – egyelőre elegendő 6300-6400 MW erőművi teljesítmény.

Éves szintén Magyarország bruttó villamosenergia-fogyasztása 41-42 milliárd KWh. Ennek döntő hányadát négy erőmű adja. A Paksi Atomerőmű termelése mintegy 14 milliárd KWh. A Mátrai Erőmű lignittal üzemel, szénhidrogénnel – alapvetően földgázzal – működik

a Dunamenti Erőmű és a Tiszai Erőmű. Ugyancsak gázüzemű a csepeli erőmű, és gázzal üzemelnek a budapesti (a kelenföldi, az újpesti és a kispesti) fűtőerőművek is. Szénrel működő erőművünk már csak egy van, az oroszlányi erőmű, amely barnaszénrel működik.



**1. ábra:**  
Magyarország villamos energia hálózata [17]

A hazai villamosenergia-fogyasztás nem egyenletes. Éjszaka általában keveset fogyasztunk, reggel hét óra körül nagyon gyors a fogyasztás felfutása, azután az évszaktól, időjárástól függően alakul a délutáni-esti csúcs, és este tizenegy óra után megint lecsökken a fogyasztás. A maximum és minimum között gyakran 1000-1200 MW teljesítménykülönbség is van. Ez óriási kihívás elé állítja az egész villamosenergia-rendszert az erőművektől a rendszerirányítóiig.

### A villamosenergia-rendszer irányítása Magyarországon

Mint ahogy láthattuk, a váltakozóáramú villamosenergia-ellátás alapvető tulajdonsága, hogy az energia termelése, szállítása és fogyasztása egy időpillanatban történik, azaz ez az energia ipari méretekben nem tárolható. A termelés és fogyasztás pillanatnyi egyensúlyáról a rendszerirányítónak kell gondoskodni.

A villamosenergia-ellátás alkotóelemeinek működését hierarchikusan felépített üzemirányítói rendszer hangolja össze. A középfeszültségű hálózat irányítását az Üzemirányító Központok (ÜIK), az áramszolgáltatói 120 kV-os hálózat és az erre csatlakozó kisebb teljesítményű erőművek irányítását a Körzeti Diszpécser Szolgálatok (KDSZ) végzik, az alaphálózat és az erőművek üzemfelügyelete a MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR ZRt.) feladata. [15]

A MAVIR létrehozását megelőzően az Országos Villamos Teherelosztó 1949. novembere óta látta el a rendszerirányítás műszaki feladatait. 2006. január 1-jétől pedig az integrált átviteli rendszerirányító (Transmission System Operator – TSO) létrejöttével az Országos Villamostávvezeték Rt. (OVIT Rt.) Üzemeltetési Igazgatósága és a Magyar Villamos Művek Rt. (MVM Rt.) Hálózati Igazgatósága átkerült a rendszerirányítóhoz.

A MAVIR ma a következő fő feladatokat látja el [18]:



- gondoskodik a magyar villamosenergia-rendszer megbízható, hatékony és biztonságos irányításáról, a szükséges tartalékokról az erőművekben és a hálózaton;
- felügyeli és gyarapítja a hálózati vagyont, elvégzi a megfelelő, üzembiztos ellátáshoz szükséges felújításokat, karbantartásokat és fejlesztéseket;
- biztosítja a villamosenergia-piac zavartalan működését, további bővítését, az egyenlő hozzáférést a rendszerhasználók számára;
- összegzi a villamosenergia-ellátás szereplőitől kapott adatokat;
- tájékoztatja a piac szereplőit;
- összehangolja a magyar villamosenergia-rendszer működését a szomszédos hálózatokkal;
- koordinálja a nemzetközi szakmai együttműködéseket;
- a jövőbe tekintve elkészíti a hálózatfejlesztési stratégiát és javaslatot tesz az erőműpark fejlesztésére.

A MAVIR felelős tehát azért, hogy az ország villamosenergia-rendszerében mindig rendelkezésre álljon a fogyasztók maradéktalan ellátásához szükséges energia, teljesítmény, és ez megfelelő minőségben és biztonsággal el is jusson a fogyasztókhoz.

A rendelkezésre álló és a fogyasztók által igényelt teljesítmény egyensúlyának folyamatos zavartalansága biztosításához a Rendszerirányítónak nagy mennyiségű információt kell feldolgoznia.

Az MAVIR információit három nagy csoportra lehet osztani [15]:

- kívülről, az irányított rendszerből érkező információk. Ezek az energiarendszer erőműveiből, alállomásaiból az irányítási hierarchia alsóbb szintjén álló Közeti Diszpécser Szolgáltatoktól, illetve a magyar energiarendszerrel párhuzamosan üzemelő külföldi energiarendszerek üzemirányítóitól érkeznek;
- belső, az üzemirányítónál előállított információk. Ezek az irányított rendszer elemeinek jellemzőit tároló adatbázisok (hálózati elemek terhelhetősége, erőművi gépegységekre vonatkozó adatok, stb.) illetve naponta változó, az energiarendszer üzemének tervezett paramétereit tartalmazó adatok (pl. szállítási menetredek, erőművek termelési menetredek, stb.);
- kimenő információk. A beérkezett adatok feldolgozása után a rendszerirányítótól kimenő információk lehetnek on-line parancsok az erőművek teljesítményének szabályozására vagy távparancsok, készülék ki és bekapcsolására ill. lehetnek napi frissülésű menetredek vagy elszámolási adatok. A kimenő információk közé sorolhatók a statisztikai feldolgozások, de ezek az üzemirányítás biztonságát közvetlenül nem befolyásolják.

A rendszerirányító tevékenységét az on-line érkező adatok feldolgozását végző számítógépes rendszer támogatja. Ez a rendszer látja el a SCADA (Supervisory Control and Data Acquisition - rendszerfelügyelet és adatgyűjtés), valamint az EMS (Energy Management System - hálózatszámítási és optimalizációs) feladatokat.

A SCADA alrendszer alapfunkciói: [15]

- adatlekérdezés és adatcsere, amely során mintegy 100.000 valós idejű adatot gyűjt a villamos energia rendszerből;
- alarm feldolgozás, amely a villamosenergia-rendszer normálistól eltérő állapotára utaló információk kezelését jelenti. Az alarmüzenetek különböző alarmlistákra irányíthatók, ami áttekinthetőbbé teszi az információkat, segít az üzemirányítók közötti feladatmegosztásban;
- megjelenítés, amelynek eszköze munkahelyenként 3 db képernyő, valamint egy kivetítő. Ezek a különböző funkciókhoz tartozó képek igény szerint nagyíthatók,

kicsinyíthatók, egymás mellé rendezhetők, így biztosítva a személyzet számára az egyéni, legáttekinthetőbb információ-megjelenítést;

- parancsküldés, amely a diszpécser vagy egyes automatikus funkciók által definiált parancsok küldését, végzi. A hálózati alállomásokban a parancsokat a telemechanikai rendszer (RTU) fogadja és hajtja végre, az erőművekben pedig a teljesítmény szabályozó rendszer;
- központi wattos teljesítményszabályozási funkciók, amelyek feladata:
  - csereteljesítmény és frekvenciaszabályozás;
  - gazdaságos teherelosztás;
  - tartalékfigyelés;
  - termelési költség számítás;
- automatikus feszültség-meddőszabályozás, amely határérték-túllépések megszüntetésére és a hálózati veszteség minimalizálására szolgál.

Az üzemirányítási tevékenység folyamatos, zavarmentes működésének feltétele az információáramlás és feldolgozás biztonsága.

A végponti adatgyűjtés biztonságát szolgálja az optikai kettős adatátviteli gyűrű a fejgépek és a mezőgépek között. Ebben kettős fénykábel köti össze a berendezéseket, amely hurkot alkotva visszatér a fejgéphez. A gyűrű bármely pontban megszakítható, a fejgép és a mezőgépek közötti adatátviteli kapcsolat megmarad. A fejgépekből induló felső szintű adatátviteli vonalak egymástól függetlenek, az átvitt információ is független egymástól. Bármely vonal hibája esetén a többi vonal zavartalanul tovább működik.

Az RTU-k működési paraméterei távközlési úton elérhetők, ami lehetővé teszi a távhibakeresést és távhangolást.

Az adatkapcsolatok biztonságát, folyamatos rendelkezésre állását egyrészt az RTU – Üzemirányító közötti átviteli utak tartalékolása, másrészt kerülő utak (RTU - KDSZ - Üzemirányító) kiépítése biztosítja.

A folyamatirányító számítógépben külön funkció végzi a különböző útvonalakon, eltérő időben érkező adatok időhelyes összehasonlítását. Tartós eltérés esetén a rendszer hibaüzenetet küld.

Az operatív üzemirányítás biztonságát szolgálja, hogy a rendszer standard elemekből épül fel, a szervereket és munkaállomásokat Ethernet hálózat fogja össze. A rendszer megbízhatósága alapvetően függ az alkotóelemek megbízhatóságától, de a megbízhatóságot jelentősen növeli a redundáns kiépítés is. Ez a kettős megvalósítás vonatkozik a hálózatra és a tápellátásra egyaránt. A két rész-rendszer külön helyiségben helyezkedik el, ami jelentősen csökkenti a tűz vagy mechanikai sérülés kockázatát. A technikai eszközök megbízhatóságán túl ugyanilyen fontosságú a rendszer védelme a szándékos vagy véletlen károkozással szemben. Ezt hivatottak biztosítani a felhasználói jelszavas hozzáférés, a beavatkozások idejének és helyének rögzítése, az egyes felhasználók igényeihez és tevékenységéhez szabott hozzáférési jogosultságok.

Külön meg kell említeni az alaprendszertől független, csökkentett funkcionalitású, de a villamosenergia-rendszer kézi üzemirányításához elégséges információt biztosító tartalék mérőrendszert. Ezek a mérések az alállomásokból és az erőművekből független távadókból, külön átviteli utakon érkeznek és a MAVIR-nál is önálló feldolgozó rendszer jeleníti meg az adatokat a diszpécsernek számára. [15]

A folyamatirányító számítógép-rendszerbe történő illetéktelen behatolás lehetősége gyakorlatilag kizárt, mivel a rendszer külső hozzáférése fizikailag blokkolható. A belső, kezelői beavatkozások szakterületekre korlátozottak, jelszóval védettek és naplózottak.

Az üzemirányításban dolgozók, valamint az üzem-előkészítést, értékelést végző munkatársak kiterjedt számítógép-hálózatra támaszkodhatnak tevékenységük során, amely magában foglalja az ügyviteli feladatok ellátásához, a villamos-energia elszámoláshoz

szükséges gépeket, a tervezéshez használt adatbázisokat, valamint biztosítja az internet és e-mail elérhetőséget.

Ez a rendszer könnyen lehet illetéktelen behatolás célpontja, amelynek célja a számítógépes rendszerben tárolt adatállományokhoz vagy programokhoz való hozzáférési lehetőség megszerzése, vagy rosszindulatú programok, programrészek bejuttatása, programok módosítása a rendszer működésének megzavarása céljából. Az illetéktelen behatolás adatok sérülését, módosítását, üzleti titok kiszivárgását okozhatja.

Az illetéktelen behatolás ellen a rendszert tűzfal védi. Az esetlegesen bejutó rosszindulatú programok okozta károk megelőzésére szolgál a hálózat elemeinek rendszeres vírusellenőrzése. Az eddigi üzemeltetési tapasztalatok szerint komoly, a rendszer működését veszélyeztető külső behatolás, vírusfertőzés nem történt. [15]

## Internet Magyarországon

### Információs Infrastruktúra Fejlesztési program

Az IIF (Információs Infrastruktúra Fejlesztési) program 1985-ben indult, a SZTAKI (Számítástechnikai Automatizálási Kutató Intézet) akkori főigazgatója, Vámos Tibor akadémikus ötlete alapján. Az IIF a magyarországi kutatás-felsőoktatás-közgyűjtemények számítógép-hálózati hátterének megvalósítását tűzte ki alapvető céljaként. Ez abban az időben meglehetősen merész terv volt, hiszen egyebek között minden hálózati termék szigorú embargó alá esett, azaz a fejlett nyugati technológiákat nem lehetett a keleti blokk (Szovjetunió és szövetségesei) számára eladni. Az embargóval sújtott termékek és technológiákat az úgynevezett COCOM<sup>2</sup> listák tartalmazták.

Mivel 1988-tól az USA engedélyezte Európa számára is az internet technológiákat, így megkezdődhetett a kísérleti internet kapcsolatok felépítése, a név — domain name — szolgáltatás biztosítása és az internet címzések használata az elektronikus levelezésben. A MATÁV<sup>3</sup> korszerűbb, import csomagkapcsoló központokat szerezhetett be, melyekkel az adathálózat minőségét, teljesítményét és a szolgáltatások körét is bővíthették. 1992-re a csomópontokba Unix-os szerverek (host computers) kerültek. Ezekhez alapértelmezés szerint tartozik a TCP/IP protokoll és a névszolgáltató szoftverrendszer. Elindult a HBONE (országos, bérelt vonalas, IP-protokollt alkalmazó gerinchálózat) kialakítása. Fontos cél volt, hogy a HBONE és a nagy nemzetközi hálózatok megbízható, nagy kapacitású vonalakkal is összekapcsolásra kerüljenek. [19]

A HBONE különcélú (távközlő) hálózat. A HBONE a robusztus MAG-ból, valamint a MAG routereihez (közvetlenül vagy közvetve) kapcsolódó regionális központi routerekből áll, beleértve az összekötő adatvonalakat is. A HBONE gerinc fő vidéki és budapesti vonalai valamint nemzetközi kapcsolatai gigabites sávszélességűek. A vidéki és nemzetközi gigabites kapcsolatok a legkorszerűbb DWDM<sup>4</sup> technológiára épülnek, melyet a HBONE alkalmazott legelsőként Magyarországon.

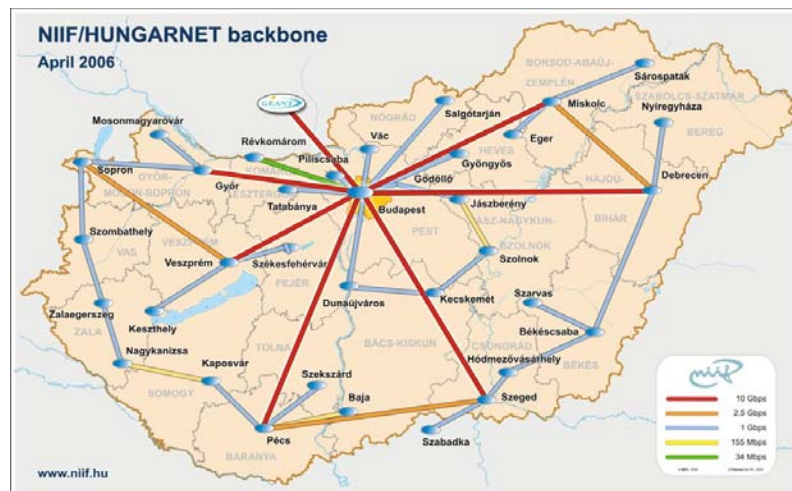
---

<sup>2</sup> COCOM: Coordinating Committee for Multilateral Export Controls, azaz magyarul: Többoldalú Exportellenőrzési Koordináló Bizottság. Az akkori NATO tagállamok (Spanyolország és Izland kivételével) és Japán részvételével működő bizottság, székhelye Párizs volt. A bizottságot 1950-ben hozták létre. Ellenőrzésével megakadályozták egyes termékek, főként katonai felszerelések, fejlett technikájú műszaki berendezések, pl. számítástechnikai, híradástechnikai, navigációs stb. exportját a (volt) szocialista országokba. A bizottság ellenőrzése alá vont termékeket az ún. COCOM listák tartalmazták. [20]

<sup>3</sup> Magyar Távközlési Rt., napjainkban a vállalat neve Magyar Telekom.

<sup>4</sup> DWDM: Dense Wavelength Division Multiplexing — nagysűrűségű hullámhossz multiplexálás. Olyan hullámhossz multiplexáláson alapuló átviteli technológia, mely lehetővé teszi, hogy 8-tól akár 40-ig terjedő különböző frekvencián továbbítsunk információt az optikai kábelben keresztül. A DWDM technológia alkalmas arra, hogy SDH rendszerek átvitelét is ellássa, vagy azokat helyettesítse. [21]

Kezdetben a HBONE csak három budapesti tudományos intézetben lévő routerből és az összekötő nagysebességű mikrohullámú kapcsolatokból, illetve a MATÁV Budapesten, a Városház utcai központjában lévő csomagkapcsoló központokból állt. Ma már a HBONE a budapesti magból és a több mint 20 helyen elhelyezett csomópontokból álló hálózata szolgálja ki a hazai felsőoktatást, kutatás-fejlesztést, könyvtárakat és közgyűjteményeket, egy átjárón keresztül a Miniszterelnöki Hivatalhoz kapcsolódó kormányzati szerveket valamint számos egyéb közintézményt is. [19] [22]



2. ábra:

A HBONE Gerinchálózati topológia

(csak a nagysávszélességű, hazai távolsági kapcsolatok kerültek feltüntetésre) [22]

Az IIF Program a hazai kutatói hálózat alapjainak megteremtése után a 90-es évek elejétől már valamennyi érintett minisztérium és az OTKA (Országos Tudományos Kutatási Alap) támogató részvételével NIIF (Nemzeti Információs Infrastruktúra Fejlesztési) Programként folytatódott. [23]

A Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program a magyarországi kutatói hálózat fejlesztésének és működtetésének programja. A Program a teljes magyarországi kutatói, felsőoktatási és közgyűjteményi közösség számára biztosítja:

- az integrált országos számítógép-hálózati infrastruktúrát;
- a kommunikációs, információs és kooperációs szolgáltatásokat;
- az élvonalbeli alkalmazási környezetet;
- tartalom-generálási, illetve tartalom-elérési háttérrel.

A Program központi költségvetési támogatásra támaszkodik. A fejlesztési és működtetési feladatokat az NIIF Intézet (NIIFI) fogja össze, a Program Tanács irányítása és a Műszaki Tanács szakmai közreműködése mellett. A Program szorosan együttműködik a felhasználói közösséget tömörítő Hungarnet Egyesülettel.<sup>5</sup>

Az NIIF Program — a nemzetközi gyakorlatnak megfelelően — egyúttal élvonalbeli szerepet tölt be a legújabb hálózati technológiák magyarországi fejlesztésében és alkalmazásában is. Ennek megfelelően a program meghatározó szerepet játszik az informatika országos fejlődésében. Korszerű, versenyképes infrastruktúrát és szolgáltatásokat biztosít a

<sup>5</sup> A HUNGARNET Egyesület feladata a Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF) alkalmazói körébe tartozó felső-, és középfokú oktatási intézmények, akadémiai és más kutatóintézetek, közgyűjtemények (könyvtárak, levéltárak, múzeumok) társadalmi szervezeteként képviselni ezen intézmények információs infrastruktúrájának és országos számítógépes szolgáltatásainak összehangolt fejlesztését hazai és nemzetközi szervezetekben. Az Nemzeti Információs Infrastruktúra Fejlesztési Iroda (NIIFI) által létrehozott és üzemeltetett magyar kutatói, felsőoktatási és közgyűjteményi hálózatot (NIIF Hálózat) illetve az üzemeltető szervezetet (NIIFI) gyakran nevezik HUNGARNET-nek, különösen nemzetközi fórumokon. Pontosabb azonban az NIIF Hálózat ill. NIIF Iroda elnevezések használata. [24]

felsőoktatás és a kutatás számára, de egyúttal követendő példával is szolgál az országszerte folyó informatikai fejlesztésekhez. [25]

## **A Sulinet-hálózat [26]**

A Sulinet központi fejlesztési program 1996 szeptemberében indult azzal a céllal, hogy korlátlan és ingyenes internet-kapcsolattal, az ehhez kapcsolódó internetes tartalomszolgáltatással, multimédiás számítógépes laborokkal lássa el a hazai és határon túli magyar közoktatási intézményeket.

Napjainkban közel két és fél ezer oktatási intézmény csatlakozik a Sulinet hálózatához, ez azt jelenti, hogy a középfokú oktatási intézmények 99 százaléka, illetve az általános iskolák 20 százaléka, illetve néhány határon túli magyar iskola rendelkezik ingyenes és korlátlan internet-kapcsolattal, és internet-laborral, ami átlagban egy helyi szerverből és hét kliens gépből áll. A 2003-ban induló Sulinet Expressz Programnak köszönhetően további 600 oktatási intézmény kapcsolódhatott a hálózathoz.

A Sulinet hálózathoz tartozó intézmények zömében 128 kb/s digitális, illetve ADSL I, valamint ADSL II.-kapcsolattal, vagy ahol erre nem volt lehetőség analóg (ez általában 56 kb/s-os, különösen indokolt esetben 128 kb/s-os) vonallal kapcsolódik a hálózathoz.

A Sulinet hálózat hierarchikus felépítésű: az intézmények a regionális központokhoz csatlakoznak, a regionális központok, pedig a Sulinet országos központjához. Ez a megoldás egy könnyen átlátható, egyszerű, hatékony struktúrát eredményezett.

Minden intézményben a kapcsolat típusához (ADSL, ISDN, bérelt vonal) igazodó végponti eszköz és router található. Az iskolai számítógépek a router-hez kapcsolódó HUB-on keresztül érik el az internetet.

Az iskolai vonalak a regionális központok nagyteljesítményű routereihez kapcsolódnak. Regionális központból tizenegy van az országban (Debrecen, Győr, Miskolc, Pécs, Szeged, Székesfehérvár, Szolnok, Zalaegerszeg, valamint Budapesten három). Minden központban található egy regionális szerver, amelynek legfontosabb feladata az iskolák web-elérésének gyorsítása (proxy, cache szolgáltatás).

A régiók 15 Mb/s-os optikai kábellel kapcsolódnak a Sulinet technikai központjához, aminek feladata a régiók közötti, valamint a Sulinet és a „külvilág” közötti kommunikáció biztosítása. A központ 68 Mb/s-os kapcsolattal rendelkezik a világ felé és 100 Mb/s-os vonallal csatlakozik a hazai hálózathoz.

Az Oktatási és Kulturális Minisztérium által működtetett tartalomszolgáltató központ 2 Mb/s-os sávszélességgel kapcsolódik a Sulinethez.

A központban található a Sulinet webszerver (<http://www.sulinet.hu>), ftp-szerver (<ftp://ftp.sulinet.hu>) és levelezőlista-kezelő szerver (<http://lista.sulinet.hu>).

A webszerver a tartalomszolgáltatás legfontosabb eleme. Ezen találhatóak a tanuláshoz, tanításhoz, iskolai adminisztrációhoz, iskolai hálózat karbantartásához kapcsolódó friss hírek, anyagok.

Az ftp-szerver az iskolai hálózat üzemeltetéséhez kötődő legfontosabb programokat tartalmazza.

A levelezőlista-kezelő szerver több mint 10 levelezőlistát szolgál ki. Ezen listákon az oktatás résztvevői kicserélhetik véleményeiket, tapasztalataikat. Ezek közül a két legnagyobb létszámú lista a Sulinet hírlevél (kb. 6000 tag), ami heti rendszerességgel ad tájékoztatást a Sulinet Program újdonságairól és a TechInfo (kb. 700 tag), amin iskolai rendszergazdák oldják meg felmerülő problémáikat, információkkal, tapasztalataikkal segítik egymást. [26]

## **Elektronikus Kormányzati Gerinchálózat [27] [28]**

A Kormány 2003 decemberében fogadta el az Elektronikus Kormányzat Stratégia és Programtervet<sup>6</sup> (E-kormányzat stratégia). A Stratégiában meghatározott e-kormányzati programok és feladatok túlnyomó többsége 2006 végére teljesült.

Az E-kormányzat stratégia megvalósítása érdekében a Kormányzati Informatikai és Társadalmi Kapcsolatok Hivatala (KITKH), majd az Elektronikus kormányzat-központ (EKK) összkormányzati koordinációs tevékenységét a Kormányzati Informatikai Egyeztető Tárcaközi Bizottság (KIETB) segítette. A KIETB az 1991-ben létrehozott Informatikai Tárcaközi Bizottság (ITB) jogutódja. Tagjai a fejezeti jogkörű költségvetési szerveknek az informatika ágazati stratégiájának kidolgozásáért és végrehajtásáért felelős vezetői. A KIETB működését a 1054/2004 (VI. 3.) Korm. határozatban került szabályozásra.

Az elektronikus kormányzás feladatainak fontos részét képezi az EU által az eEurope 2005 akciótervben meghatározott 20 alapvető szolgáltatás megvalósításának koordinálása. E területen az EKK tevékenységét segítette a szolgáltató állam létrehozásához kapcsolódó reformfolyamatok felgyorsítása érdekében a közigazgatási szolgáltatások korszerűsítésével kapcsolatos feladatokat összehangoló Koordinációs Bizottság irányítása alatt működő, a 1126/2003. (XII. 12.) Korm. határozattal létrehozott E-Kormányzat Operatív Bizottság (EKOB).

Mind a KIETB, mind az EKOB eredményesen látta el feladatait. A kibővült, valamint megváltozott feladatok figyelembe vételével, a koordinálás egyszerűsítése és átláthatóbbá tétele érdekében előkészítés alatt áll a két korábbi bizottság feladatait átvevő, új Közigazgatási Informatikai Bizottság létrehozása.

Az elektronikus közigazgatás megvalósításának alapját a Központi Elektronikus Szolgáltató Rendszer (Központi Rendszer) biztosítja, amely a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) rendelkezése alapján együttesen magába foglalja az Elektronikus Kormányzati Gerinchálózatot (EKG), a kormányzati portált, a kormányzati ügyféltájékoztató központot, az ott megjelenő szolgáltatásokat és ügyintézési lehetőségeket, valamint azok fenntartóit és üzemeltetőit, továbbá biztosítja az ügyfelek számára az elektronikus ügyfélkapu létesítésének lehetőségét.

Az elektronikus kormányzás alapinfrastruktúráját a 1122/2001 (XI. 22.) Korm. határozatban megfogalmazottaknak megfelelően létrehozott Elektronikus Kormányzati Gerinchálózat (EKG) képezi.

Az EKG egy olyan informatikai hálózat, amelynek feladata, hogy a kormányzati és közigazgatási adatbázisokat, hálózatokat és informatikai rendszereket összekapcsolja a vonatkozó kormányrendeletben meghatározott kormányzati körnek, valamint a különböző kormányzati szolgáltatások elérhetőségét biztosítsa a civil szféra számára.

Az EKG infrastruktúrájának megerősítésével válik lehetővé a kormányzati rendszerek elektronizálása és új, hatékony, távolról is elérhető szolgáltatási rendszerek bevezetése, egy szóval az e-kormányzat kialakítása. Ezek a szolgáltatások jelentősen közelítik egymáshoz az igazgatási munkát és a civil szférát, erőteljesen lecsökkentve az ügyintézéshez szükséges időt, nyílttá, átláthatóvá teszik a közszféra munkáját.

Az EKG célja és rendeltetése [29]:

1. Nagy sebességű, nagy üzembiztoságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú hálózati infrastruktúra biztosítása a civil szféra számára az állami intézmények által nyújtott szolgáltatások eléréséhez (Front-Office feladatok);
2. Az új infrastruktúrára épülő szolgáltatások és egyes eddig elszigetelt (pl. ágazati) hálózatok elérhetővé tétele a jogosult felhasználók számára (Back-Office feladatok);

---

<sup>6</sup> 1126/2003. (XII. 12.) Korm. határozat

3. A kormányzati szervek közötti kommunikáció, az adatátvitel költségeinek csökkentése, minőségi szintjének emelése;
4. Kormányzati szintű, több felhasználó által használt alkalmazások hatékony működtetése;
5. Olyan infrastrukturális háttér biztosítása, amely alkalmas az elektronikus ügyvitel és ügyintézés feltételeinek megteremtésére, a jövőbeli elektronikus közigazgatás koncepciójának, vagyis az állampolgár és a kormányzat újszerű kapcsolatának kiszolgálására;
6. A kétirányú kormányzati kapcsolatok biztosítása a brüsszeli adminisztráció rendszereihez (csak az EKG-n keresztül lehetséges);
7. A minisztériumok és a központi intézmények részére biztosítson védett, — security, — szolgáltatások nyújtását és elérését.

Az EKG fő célkitűzése, hogy a jelenlegi széttagolt, gyakran nem megfelelő kapacitású és biztonságú hálózatokat egy olyan nagy sávszélességű, üzembiztos, országos elérhetőséget biztosító és egységes gerinchálózat váltsa fel, amelyen különös figyelmet kap a hálózaton elérhető szolgáltatások üzembiztonsága. A gerinchálón minden intézmény kapcsolatrendszere önálló magánhálózatként kerül kialakításra a közös infrastruktúrán, ezzel is tovább növelve a biztonságot. Az EKG által megteremtett infrastrukturális alapokon működik a Miniszterelnöki Hivatal felügyeletében a Kormányzati Portál, amely különböző minisztériumok honlapjait tartalmazza.

A 2005. április 1-jétől igénybe vehető Ügyfélkapu biztosítja, hogy az ügyfél egyedileg azonosított módon biztonságosan léphessen kapcsolatba a központi rendszer útján az elektronikus ügyintézés, illetve elektronikus szolgáltatást nyújtó szervekkel.

A 2005. augusztus 1-jétől működő Kormányzati Ügyféltájékoztató Központ (KÜK), a 189-es hívószámon, valamint sms-ben, faxon és e-mailben (189@ugyfelvonal.hu) elérhető ügyfélvonal az állampolgárok számára 24 órán keresztül folyamatosan nyújt tájékoztatást közigazgatással összefüggő általános kérdésekben, valamint a központi rendszeren keresztül elektronikusan elérhető szolgáltatásokról.

## **Kereskedelmi internet**

Ma már több mint 200 szolgáltató biztosít internet hozzáférést Magyarországon. Ezek közül számos saját kiépített országos hálózattal rendelkezik.

Ilyen országos hálózat például a Pan-Tel<sup>7</sup> optikai gerinchálózata. A PanTel mintegy 4000 kilométer hosszú, világszínvonalú optikai szálas hálózata Magyarország egyik alternatív távközlési infrastruktúrája. A PanTel hálózata biztosítja minden megyeszékhely, valamint számos más város optikai vezetéken történő elérését. [30]

A cég SDH (Synchron Digital Hierarchy) technológia használatával gyűrűs struktúrájú hálózatot épített ki. Ily módon egy gerinchálózati csatlakozási pont (POP — Point Of Presence) egy másik gerinchálózati csatlakozási ponttal mindig két független optikai nyomvonalon van összekötve. A két POP között, ha az egyik nyomvonalon megszakadna az összeköttetés, a másik nyomvonalon keresztül a kommunikáció tovább folytatódhat. Így két POP között igen nagy rendelkezésre állású összeköttetések hozhatók létre. A PanTel hálózata több gyűrűre van felosztva. Az egyes gyűrűk közötti forgalmat redundáns kiépítésű Crossconnectek biztosítják.

<sup>7</sup> A PanTel Kft. közép-európai vezetékes távközlési szolgáltató, mely az alternatív vállalatként hang-, adat- és internetszolgáltatásokat ajánl elsősorban üzleti ügyfelek, távközlési szolgáltatók és internetszolgáltatók részére. [31]



**3. ábra:**

A PanTel optikai gerinchálózata, POP-jai, és határátlépő pontjai [30]

A PanTel hálózata nemcsak az országon belül, hanem az országhatárokon túl is igénybe vehető. Optikai szálas kapcsolat működik Ausztriával, Romániával, Szlovákiával, Szlovéniával, Horvátországgal, Szerbiával és Bulgáriával. Az osztrák vasutakkal 2001-ben aláírt szerződése alapján a vállalat 400 km hosszúságú optikai szállal rendelkezik Ausztriában, 1400 km-nyi optikai szálát bérel Romániában, és kb. 620 km-nyi optikai szálát használ Bulgáriában. A PanTel nagy sáv szélességű, közvetlen összeköttetést üzemeltet a nagyobb külföldi szolgáltatói összekapcsolódási pontok felé (pl. Frankfurt, Bécs, Prága). Közép-európai távközlési szolgáltatóként valamint a kedvező földrajzi elhelyezkedésnek köszönhetően, a PanTel átjáró szerepet tölt be Nyugat- és Kelet-Európa között, mintegy hidat képezve a régiók országai között. A nemzetközi gerinchálózaton keresztül a már ismert szolgáltatásokat nyújtja a cég ügyfelei részére, a helyi elérési szakaszt az adott ország telekommunikációs engedéllyel rendelkező partnerein keresztül biztosítják. [30]

Hasonlóan a PanTel-hez szintén országos hálózattal rendelkezik az Antenna Hungaria ZRt. is, amely leányvállalatán az Antenna Távközlési ZRt.-n keresztül biztosít hazai és nemzetközi internet hozzáférést.

Az Antenna Távközlési ZRt. távközlési szolgáltatásait a nagy sebességű, az egész országot lefedő digitális mikrohullámú Országos Transzport Hálózatán, valamint vezetékes budapesti optikai hálózatán keresztül biztosítja. Az országos digitális mikrohullámú gerinchálózat 51 állomásból áll. Az SDH rendszerű, gyűrűs kialakítású hálózat lehetővé teszi, hogy a vállalat a digitális átvitel minden előnyét kihasználja.

A cég hozzáférési hálózatában átviteli közegként használható rézvezető, optikai kábel, VSAT és mikrohullámú összeköttetés. Az Antenna Távközlési ZRt. infrastruktúrájából, magaslati telephelyeiből, tornyaiból adódóan Magyarország területén döntően mikrohullámú elérési hálózat kiépítését tudja megvalósítani, mely gyors telepíthetősége mellett magas rendelkezésre állást is biztosít. Mindezek mellett Budapest területén mikrohullámú és optikai kábeles megoldásokat is nyújt.





4. ábra:

Az Antenna Távközlési ZRt. gerinchálózata [32]

A mikrohullámú elérési hálózat jellemzően pont-pont és pont-multipont struktúrájú lehet. A pont–pont jellegű összeköttetés az adott két pont között teremt kapcsolatot. Pont–multipont esetben a sok végpont egy bázisállomáson keresztül kapcsolódik a hálózathoz.

A vezetékes elérési hálózatot optikai kábeles, és kisebb sebességek esetén rézkábeles megoldással tudják megvalósítani.

A meglévő budapesti optikai gyűrűs hálózat (SDH alapú STM-1, STM-4 és STM-16-os rendszerek) lehetővé teszi, hogy a végpontokig történő kábelek kihúzásával a gerinchálózaton keresztül a jeleket gyorsan és megbízhatóan a csomópontokba szállítsa.

Az Antenna Hungária ZRt. egy másik leányvállalata, a HungaroDigiTel Kft. révén a professzionális távközlés egy különleges technológiáját, a VSAT<sup>8</sup> műholdas digitális távközlési technológiát is tudja alkalmazni az összeköttetések kiépítésénél. E technológia előnye a földi adatátvitellel szemben a rugalmas hálózat felépítési és módosítási lehetősége, a gyorsabb telepíthetőség, a megbízhatóbb működés és az áthidalta távolságtól független üzemeltetési költség. Ezen kívül alkalmazása egyszerűbb és előnyösebb más technológiákhoz képest, előnyös az elégtelen távközlési infrastruktúrájú területeken, a szétszórta elhelyezkedő felhasználók biztonságos együttműködéséhez, az alkalomhoz és eseti helyszínekhez fűződő időszakos távközlési igények kielégítésére, valamint — vevőberendezésként — a kiterjedt földrajzi területeken és széles felhasználói körben történő információterjesztéshez esetén.

Az Antenna Távközlési ZRt. szolgáltatásai végponttól-végpontig menedzselték. A Hálózat Felügyeleti Központ ügyelete napi 24 órában fogadja a telefonon, e-mailen illetve faxon érkező hibabejelentéseket. A Hálózat Felügyeleti Központ független klíma és energetikai rendszerrel, fixen telepített dízel berendezéssel rendelkezik.

Biztonsági okokból egy tartalék központtal is rendelkeznek, fizikailag más telephelyen elhelyezve. Az ügyeletes operátorok munkáját szakterületekre specializálódott rendszermérnökök segítik. [32]

A különböző hazai internetszolgáltatók nemzetközi irányú kapcsolatainak koordinálását a BIX (Budapest Internet Exchange) szervezet végzi. A BIX alapvető célja, hogy a különböző szolgáltatók közötti magyarországi és regionális internet forgalom ne terhelje az internet

<sup>8</sup> VSAT: Very Small Aperture Terminal. Kétutas műholdas kommunikációra alkalmas földi terminál. Az alkalmazott parabola antenna mérete általában 0,75 és 1,2 m között van. Adatátviteli sebessége a keskenysávtól (pl.: bankkártya terminálok ATM-ek) egészen a 4 Mbit/sec-ig (pl.: műholdas internet hozzáférés, VoIP, video átjátszás) tart.

szolgáltatók nemzetközi irányú kapcsolatait,<sup>9</sup> valamint, hogy platformot biztosítson a szolgáltatói hálózatok IP alapú összekapcsolásához.

A BIX egy földrajzilag is elosztott hálózati rendszer, amely BIX szolgáltatási pontokból és az azokat összekötő adatátviteli kapcsolatokból áll. A BIX szolgáltatók üzemeltetik a BIX szolgáltatási pontokat és fenntartják az azok közötti adatátviteli kapcsolatokat. A BIX szolgáltatási pontokon csatlakozhatnak saját hálózatukkal a BIX felhasználói, a BIX tagok. BIX szolgáltatási pont csak az lehet, amely legalább egy 1 Gb/s (full duplex) sebességű elsődleges és egy legalább 1Gb/s (full duplex) kapacitású tartalék közvetlen 2. szintű kapcsolattal rendelkezik a budapesti BIX szolgáltatási ponthoz, illetve a tartalék kapcsolat esetében tetszőleges másik BIX szolgáltatási ponthoz. [33]

A legtöbb hazai internet szolgáltató tagja az Internet Szolgáltatók Tanácsának (ITSZ). Az ITSZ magyarországi internet szolgáltatók szakmai koordinációs és érdekvédelmi képviselője, amely külön figyelmet fordít a .hu TLD adminisztráció szabályozására. Ennek keretében — az egyesületi formában működő szervezet — alapvetően koordinációs és tájékoztatósi, valamint tudományos-technikai célokat szolgál belföldön és külföldön egyaránt. [34]

Az ITSZ különböző statisztikákat vezet — többek között a hazai hostokról, DNS-ekről, domain namekről —, amelyek érdekes információkkal szolgálhatnak a hazai internet jelenlegi helyzetéről.

## ÖSSZEFOGLALÁS

A két hazai kritikus információs infrastruktúra bemutatásával is jól nyomon követhető, hogy hazánk is komoly eredményeket ért el az elmúlt években az információs társadalom alapjait meghatározó rendszerek kialakítása és kiépítése terén.

Mindez azonban azzal is jár, hogy komolyan számolni kell azokkal a veszélyekkel, amelyek e rendszereket és közvetetten a gazdaságot, a közigazgatást, illetve a mindennapi élet egyéb más fontos területeit veszélyeztetik.

Ahhoz, hogy a veszélyekkel szemben megfelelő védelmet tudjunk kialakítani, először számba kell venni, és fel kell mérni, hogy milyen infrastruktúrákkal rendelkezünk, ezek hol és milyen mértékben fedik át egymást, milyen mértékben hatnak egymásra. Ez a feltáró munka meglehetősen komplex, hiszen a bemutatottakból is kiderül, hogy a különböző tulajdonosi viszonyok, a különböző technológiák, és nem utolsósorban a különböző funkciók min-mind nehezítik az éleslátást. Ugyanakkor e munka elvégzése nélkül nehezen képzelhető el hatékony és hatásos védelem kialakítása.

---

<sup>9</sup> Nemzetközi irányú egy kapcsolat, ha azon Magyarországról az internet valamely root name szervere elérhető

## Felhasznált irodalom

1. Magyar értelmező kéziszótár, MTA, Budapest, 2002.
2. Magyar Larousse Enciklopédikus szótár. Akadémiai Kiadó, Budapest, 1992.
3. Haig Zsolt–Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN 963 327 391 9
4. Critical Foundations Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, Washington, 1997. október
5. Várhegyi István–Makkay Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000.
6. Précseyi Zoltán–Solymosi József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. Hadmérnök, 2007. március.  
[http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007\\_1\\_precsenyi.html](http://zrinyi.zmne.hu/hadmernok/archivum/2007/1/2007_1_precsenyi.html) ISSN 1788-1919
7. Bukovics István–Vavrik Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés. Hadmérnök, 2006. december.  
[http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006\\_3\\_bukovics.html](http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006_3_bukovics.html) ISSN 1788-1919
8. Muha Lajos: A Magyar Köztársaság információs infrastruktúráinak védelme. Doktori (PhD) értekezés, ZMNE, Budapest, 2007.
9. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.
10. Munk Sándor: Információs szintér, információs környezet, információs infrastruktúra. Nemzetvédelmi Egyetemi Közlemények 2002. 2. sz. ZMNE, Budapest, ISSN 1417-7323
11. Haig Zsolt: Az információs társadalmat fenyegető információlapú veszélyforrások. Hadtudomány 2007/3. ISSN: 1215-4121
12. Gerencsér András: Rövid összefoglalás kritikus információs infrastruktúrák védelméről.  
[http://www.isaca.hu/addons/news\\_1626\\_CIIP\\_GerencserAndras.pdf](http://www.isaca.hu/addons/news_1626_CIIP_GerencserAndras.pdf)
13. 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról
14. 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól
15. Kapás Mihály: A villamosenergia-ellátás biztonsága, A rendszerirányító feladatai és az operatív üzemirányítás technikai eszközei, Veszélyhelyzetek megelőzése és kezelése. Szakértői melléklet in: Haig Zsolt – Kovács László – Makkay Imre – Seebauer Imre – Vass Sándor–Ványa László: Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002.
16. <http://www.mvm.hu/engine.aspx?page=cegtortenet>
17. A magyar villamosenergia-rendszer (VER) adatai 2006, MAVIR 2006
18. <http://www.mavir.hu>
19. <http://www.aldasuai.sulinet.hu/tantargy/sztech/internet.doc>
20. <http://lazarus.elte.hu/~climbela/cocom.htm>

21. <http://www.nhit-it3.hu/>
22. <http://www.iif.hu/index.php?headline=infra&menu=menu-kapcs.html&text=infra1.html>
23. <http://www.niif.hu/hu/story>
24. <http://www.iif.hu/index.php?headline=hungarnet&text=hungarnet.html&nomenu=1>
25. <http://www.niif.hu/hu/intro>
26. <http://www.okm.gov.hu/main.php?folderID=537&articleID=743&ctag=articlelist&iid=1>
27. <http://www.meh.hu/szervezet/hivatalok/ekk/ekormanyzat/stratismerteto.html>
28. <http://www.meh.hu/szervezet/hivatalok/ekk/ekk/alapdok20070323.html>
29. <http://www.meh.hu/szervezet/hivatalok/ekk/keszr/ekg/ekg20050920.html>
30. [http://www.pantel.hu/a\\_pantelrol/halozat/gerinchalozatunk/](http://www.pantel.hu/a_pantelrol/halozat/gerinchalozatunk/)
31. [http://www.pantel.hu/a\\_pantelrol/a\\_cegrol/](http://www.pantel.hu/a_pantelrol/a_cegrol/)
32. <http://www.atrt.hu>
33. <http://www.bix.hu/index.php3?lang=hu&page=charter>
34. <http://www.iszt.hu/iszt/alapszabaly.html>

*Jelen írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.*