Online ökoszisztémák

Tanulmány a Nemzeti Média- és Hírközlési Hatóság számára

Szerzők:

Dr. Orosz Péter
Dr. Skopkó Tamás
Dr. Marosits Tamás

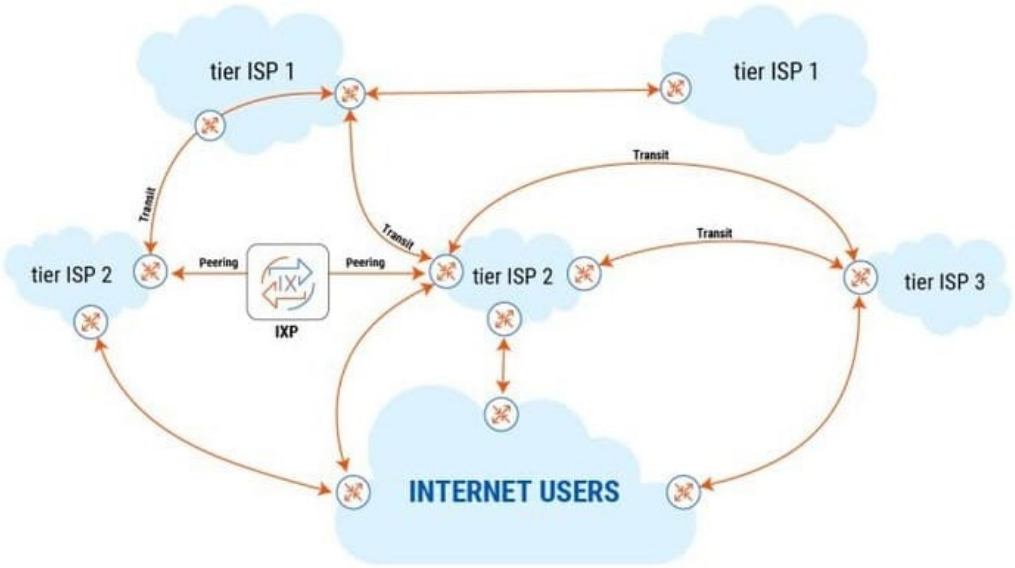
BME SmartCom Lab

Budapest, 2023. október

Tartalomjegyzék

1 Vezetői összefoglaló

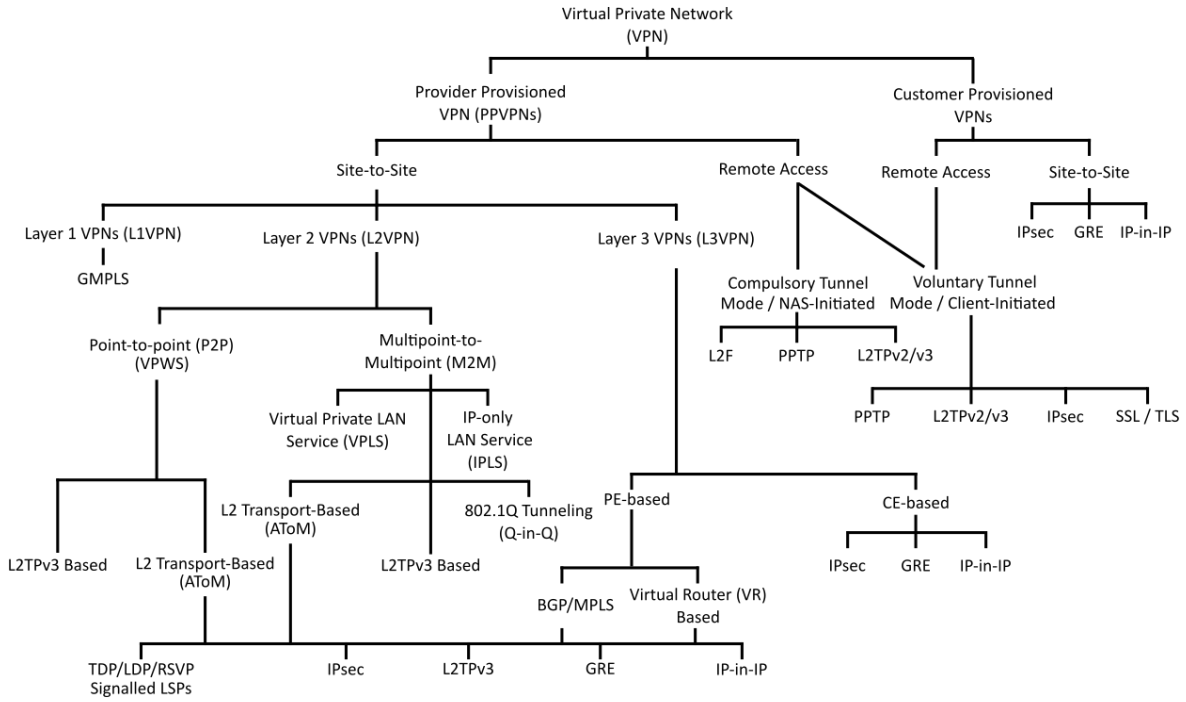
Tanulmányunkban bemutatjuk az Internet szolgáltatásait és a szolgáltatások létrejöttéhez, közvetítéséhez szükséges architektúrális elemeket, amelyek hálózattá teszik a vezetékeket és a kapcsolóeszközöket.
A Bevezetés után a 3. fejezet az Internet architektúráját mutatja be, elsősorban az egyes internetszolgáltatók (Internet Service Provider, ISP) hálózatainak széleire koncentrálva. Az ISP-k hálózatai kapcsolják össze a szolgáltató-hálózatokat (Content and Application Service Provider, CAP-eket) és a fogyasztókat (1. ábra). Mivel nem minden ISP globális, ezért sok esetben csak akkor tudjuk a szolgáltatást és a fogyasztót összekapcsolni, ha más szolgáltatók hálózatait is igénybe vesszük. A hálózatok viszonyától függően az összekapcsolódás lehet egyenrangú vagy hierarchikus.



1. ábra Az Internet globális képe az IP tranzittal és a társviszonnyal

A szolgáltatói hálózat másik oldalára a felhasználók kapcsolódnak. A hozzáférési hálózatok az Internet speciális részei, hiszen a vezetékes esetben dedikált összeköttetést kap a felhasználó, amely csak az övé, viszont a szolgáltató utolsó eszközétől – ami rendszerint egy WiFi-képes routermodem – a szolgáltató már nem tud minőségi garanciákat vállalni a szolgáltatás paramétereire. A rádiós hozzáférési hálózatokon ugyanez a helyzet, legfeljebb a rádiós összeköttetés szakasztávolsága lényegesen nagyobb, mint az előző esetben, ahol a WiFi nyilván csak az otthoni és kis irodai (SOHO) igények kielégítésére szolgál. A szolgáltatásminőségi problémák önmagukban az egyre növekvő átbocsátóképesség és csökkenő hálózati késleltetés miatt látszólag nem okoznak jelentős gondokat, egy weboldal letöltése vagy egy film megnézése során nem veszünk észre semmit. Persze ennek az az oka, hogy a weboldal még a rosszabb minőségű kapcsolaton is olyan gyorsan töltődik le, hogy az emberi megfigyelő nem érzékeli a különbséget, míg a médiafolyamok esetén a szolgáltatás a gyengébb minőségű hálózat esetén hosszabb előpufferelést végez és lejátszás közben adaptívan változtatja a forrássebességet, ha ez szükséges. Elsősorban a valós idejű kétirányú kommunikáció esetén jelenhet meg a szolgáltatásminőség romlásának a következménye az alkalmazás tapasztalati minőségében (Quality of Experience, QoE).

A hozzáférési hálózatok megbízhatóságának és átbocsátóképességének növekedése megteremtette a lehetőséget, hogy sok felhasználó szükség esetén otthonról végezze a munkáját. Az ehhez szükséges technológia már korábban is rendelkezésre állt, hiszen a vállalatok távoli telephelyeit már korábban is összekötötték olyan módon, hogy az úgy létrejövő egyesített hálózat a jól menedzselt lokális magánhálózatok megbízhatóságát és biztonsági szintjét nyújtsa (2. ábra). A távoli hozzáférésű virtuális magánhálózat (VPN) kiemelt szerephez jutott a COVID-19 okozta járványhelyzet káros gazdasági hatásainak mérséklésében, mivel lehetővé tette, hogy a munkavállalók a távolságtartás szabályait figyelembe véve, mégis normális mértékben tartsák a munkatársaikkal a kapcsolatot és együtt dolgozhassanak a közös projekteken.

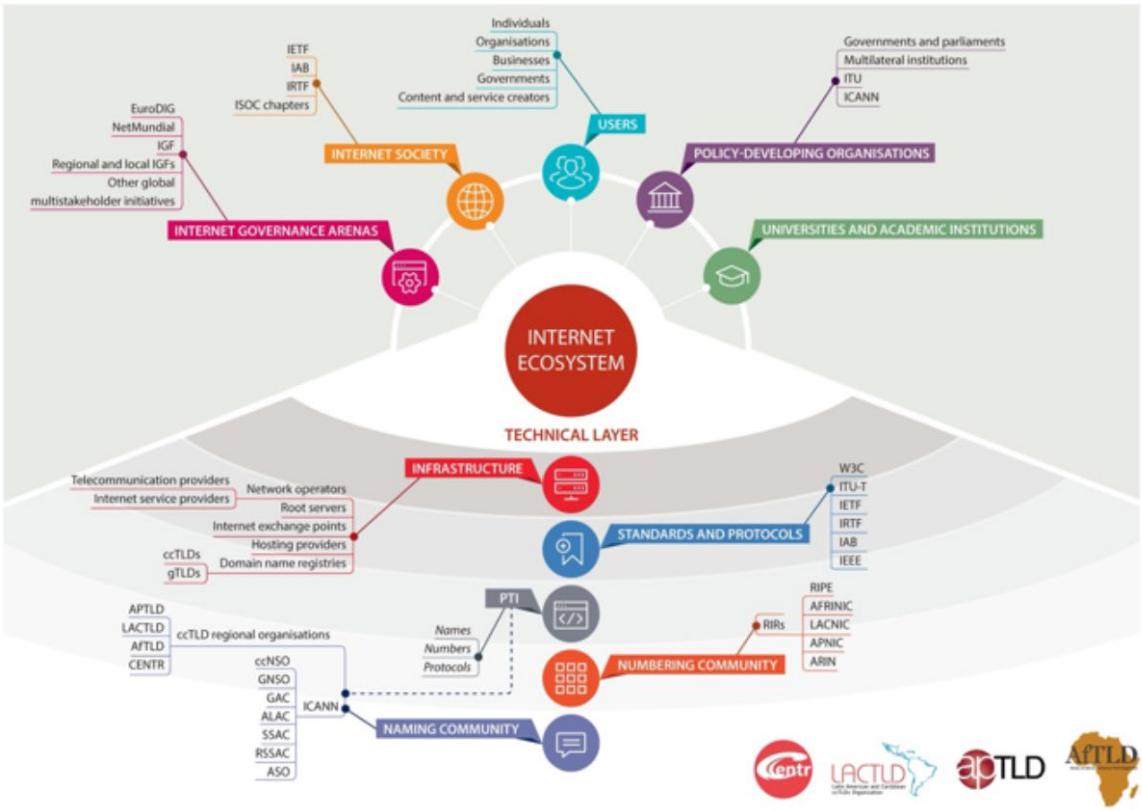


2. ábra A virtuális magánhálózatok típusai

A területen a közeljövő legfontosabb jelensége a szoftverizáció előretörése lehet. A szoftvervezérelt hálózatok koncepciójának megfelelő adaptálása akár az Internet adatkicserélő központban lehetővé teszi a hálózati erőforrások nagyon gyors átkonfigurálását valamilyen összeköttetés kiesése esetén. Ez nélkülözhetetlen ahhoz, hogy például az automatizált gyártósorok nagy gazdasági károkat okozó, előre nem tervezett vészhelyzetszerű leállásait elkerüljük, vagy hogy az előbb-utóbb mind szélesebb körűen autonómmá váló kötöttpályás és nemkötöttpályás közlekedést fenn lehessen tartani. Nyilván a kritikus infrastruktúra kommunikációjának megbízható biztosításához még komoly mértékben kell tartalékkapacitásokat beépíteni a rendszerbe, de az autonóm rendszerek elterjedése akkora forgalomnövekedéssel jár majd, hogy a veszteségek csökkentésének érdekében mindenképpen célszerű lesz a hálózat szoftveres vezénylését megvalósítani.

A tanulmány 4. fejezetében a Domain Name Service-t vagyis az Internet névtérszolgáltatását tekintjük át (3. ábra). A DNS arra szolgál, hogy az IP hálózatok végpontjait azonosító bináris számsorozatok – amelyeket a könnyebb emberi kezelhetőség végett oktetenként szoktunk értelmezni – és az emberek által még könnyebben megjegyezhető szimbolikus nevek közötti kapcsolatot megteremtse. Mivel szinte az összes szolgáltatás, melyeket mi emberek igénybe

veszünk, a szimbolikus neveket használja, ezért a név-IP cím összerendelés és inverze az Internet működésének kritikus, nélkülözhetetlen eleme.



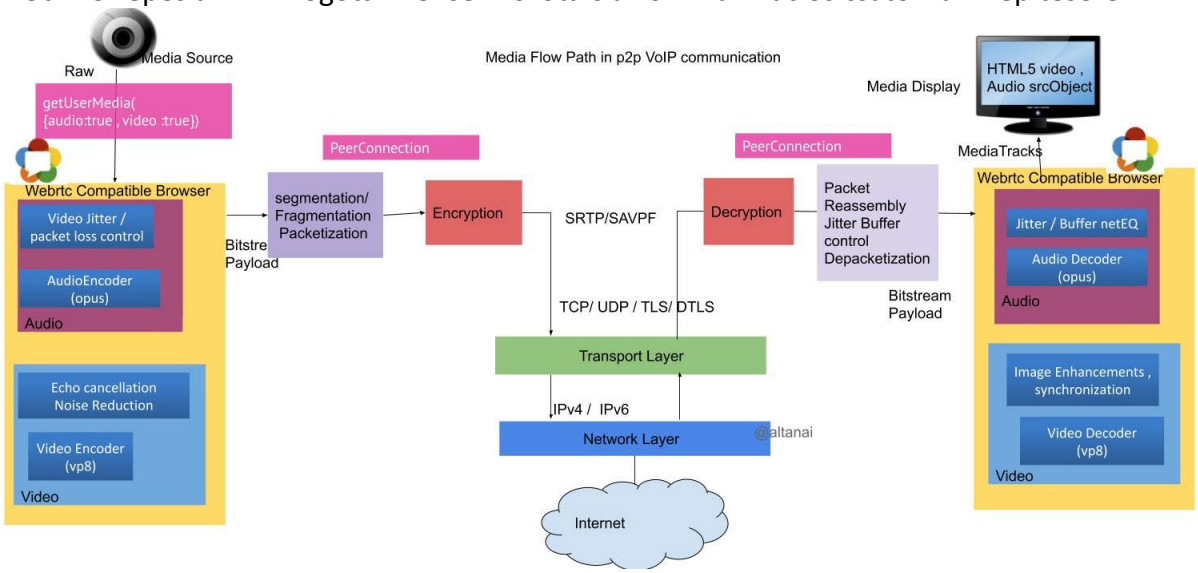
3. ábra Az internet ökoszisztémája

Mint kritikus elemet, gyakran érik különböző típusú internetes támadások, amelyek a protokoll egy-egy sajátosságát kihasználva próbálják a szolgáltatást részben vagy egészen megbénítani. Mivel a névtér hierarchikus és elosztott és a legfelsőbb szintű domének kezelését külön-külön kiszolgálók végzik, ezért a teljes szolgáltatás működésképtelenné tétele nehéz. Viszont a támadások csak nagyon ritkán célozzák a teljes szolgáltatást, inkább annak egyes részeit, akárcsak a lokális DNS kiszolgálót. Tanulmányunkban áttekintettük a jellemzően használt támadástípusokat és az ismert védekezési lehetőségeket. A szolgáltatásra vonatkozó jövőképünkben a legnagyobb hangsúlyt a biztonság kérdése kapja, vagyis az, hogy mit tehetnek a felhasználói szoftverek – operációs rendszerek és alkalmazások – gyártói és a szolgáltatók, a hálózatok üzemeltetői a biztonságos és gyors DNS szolgáltatás fenntartásáért. A felhőszolgáltatások ezen területen való megjelenése egy kellően elosztott és redundáns, a terhelés változásaira jól skálázódó, a támadásoknak ellenálló szolgáltatás képét mutatja fel, ami egyébként kedvező lenne abban a tekintetben is, hogy a szolgáltatás minél nagyobb része kerülhetne ki állami kézből.

Az elmúlt évtizedben az adatbiztonság és privát szféra védelme egyre fontosabbá vált. Ennek a védelemnek egyik eleme, hogy a felhasználók meggyőződhetnek arról, hogy a szolgáltatók és a kommunikációs partnereik azok, akiknek állítják magukat. Erre a célra szolgálnak az 5. fejezetben bemutatott digitális tanúsítványok. A tanúsítványokhoz kötődő nyilvános kulcsú infrastruktúra (PKI) és a tanúsítványkiadó hatóságok (Certificate Authorities, CA-k) ennek a területnek a legfontosabb szereplői. A digitális tanúsítványok mind a továbbított vagy tárolt információ valódiságának ellenőrzéséhez, mind az átvitel vagy tárolt adat titkosításához használatosak. Az infokommunikációnak ez a tudományterülete is fejlődésben van, például a

kvantumbiztos kriptográfiai eljárások megtalálása nélkülözhetetlen ahhoz, hogy az egész rendszer fenntartható maradjon. Ugyanakkor a mérnöki fejlesztés, a szabványosítási és a szabályozói tevékenység is fontos. A mérnöki fejlesztésre talán a jó példa a rövidlejáratú tanúsítványok alkalmazásának elterjesztése, a szabványosítási lépések közé sorolható az S/MIME alapkövetelmények megújítása, míg a szabályozás körébe sorolható a gyenge CA gyökértanúsítványok kivezetése.

A 6. fejezetben a személyközi kommunikáció aktuális helyzetét tekintjük át. Ugyan mobil és vezetékes környezetben is rengeteg alkalmazás közül választhatunk, a mögöttük lévő technológiák száma azért eléggé behatárolt. Az IP alapú hangszolgáltatás a távbeszélő hálózatokban tulajdonképpen teljesen általánosnak tekinthető, hiszen a vezetékes készülék esetén is igazából csak az utolsó néhány méter lehet analóg átvitelű. A végponttól végpontig terjedő IP telefónia alkalmazási területeit a felhasználási cél és a szolgáltatás tulajdonosa szerint feloszthatjuk az IP-alapú hálózatokon működő privát telefonrendszerekre (pl. vállalati, irodai belső telefonrendszerek), az Interneten nyújtott nyilvános kommunikációs szolgáltatásokra (például szabványos protokollokra épülő ingyenes és üzleti VoIP szoftverek és rendszerek segítségével nyújtott telefonszolgáltatás, üzenetküldő alkalmazások, videókonferencia rendszerek) és mobil távközlő hálózatokban nyújtott hangszolgáltatásra. A felhasznált technológiák elég jól ismertek, a SIP-et régóta használják a vezetékes és rádiós környezetben is, a WebRTC pedig, mint a SIP-alapú VoIP technológia újgenerációs kibővítése, továbbfejlesztése, mellyel webes böngészőkben, mindenfajta előzetes telepítés igénye nélkül nyújtható valósidejű videó- és hangkommunikációs szolgáltatás (4. ábra). A WebRTC megalkotásakor a valósidejű kommunikáció mellett a biztonság is nagy hangsúlyt kapott, ezért a végpontok között minden esetben titkosított a jelzés és média kommunikáció. A böngészők erős titkosítási funkcióinak hasznosítása biztonsági szempontból komoly előny a korábbi tisztán SIP-alapú VoIP szolgáltatásokkal szemben, melyek gyakran gyártóspecifikus biztonsági megoldásokat alkalmaztak. Szintén a böngészőhöz kapcsolódó eredete miatt a WebRTC képes a NAT mögötti kliensek között is a kommunikációs csatornák kiépítésére.

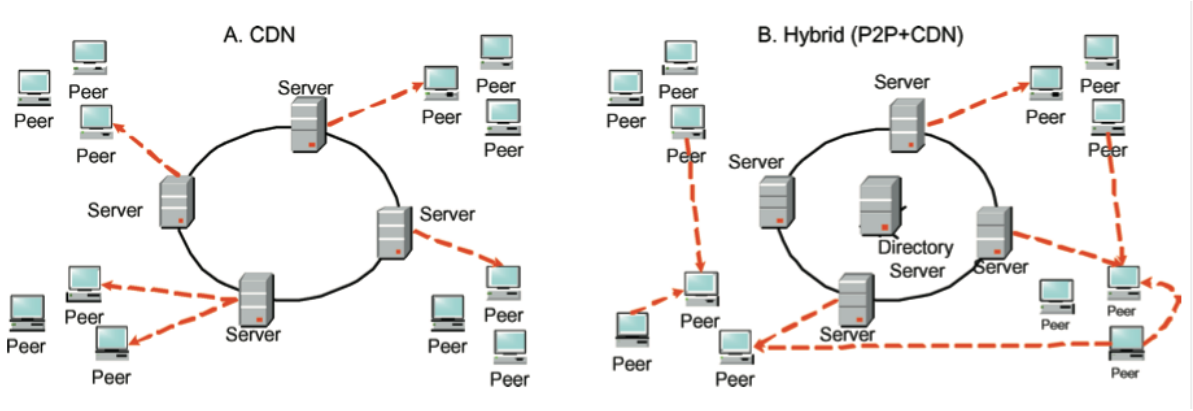


4. ábra WebRTC végpontok közötti kommunikációs útvonal

A hangátvitelen kívül a WebRTC számos olyan felhasználási esetet (például többrésztvevős videókonferencia, képernyőmegosztás, e-learning, stb.) támogat, amelyek a modern kommunikációs szolgáltatások kihagyhatatlan komponensei. WebRTC-t használ többek között a Google Meet, a Meta kapcsolatteremtő szoftverei vagy éppen a Discord is.

A mobil távbeszélő hálózatokban a jelenleg legelterjedtebb a Voice over LTE technológia, amely 4G LTE mobilhálózaton valósít meg kommunikációs szolgáltatást az IP Multimedia Subsystem (IMS) alrendszer felhasználásával. A VoLTE szolgáltatás mind a jelzés, mind a multimédia információt adatként továbbítja a felhasználók között, a klasszikus áramkörkapcsolt infrastruktúra használata nélkül. Napjainkra a legtöbb mobil operátor bevezette a VoLTE szolgáltatást az LTE hálózatokban. Az IMS, mint központi szereplő, valójában egy önálló, az LTE hálózattól független rendszer. A két hálózat specifikus interfészeken kapcsolódik egymáshoz és amíg az LTE számára a hívás vezérlő és média forgalma is felhasználói forgalom, az IMS-ben ezek szétválasztásra kerülnek.
A telepítés alatt álló 5G hálózatokban a Voice over New Radio technológiát használják továbbra is az IMS alrendszerre építve, vagyis a felhasználói végberendezés és az IMS rendszer között az LTE helyett felhőalapú 5G rádiós és maghálózat biztosítja az összeköttetést. A VoNR előnyei a VoLTE-hez képest a gyorsabb hívásfelépítés, a magasabb hangminőség támogatása, hatékonyabb QoS menedzsment és nagyobb átviteli kapacitás.
A személyközi kommunikáció jövője egyrészt a mobilitási képesség további előretörése, az olcsóbb és robusztusabb üzemeltetés lehetősége magasabb hozzáadott értékű szolgáltatások nyújtása mellett, másrészről pedig a WebRTC által nyújtott lehetőségek kihasználása. A verseny erősödése várható tehát, ugyanakkor a szolgáltatói oldalról egyre inkább jellemző lesz a szoftverizáció és a felhőszolgáltatások alkalmazása.

A tanulmányunk 7. fejeztében az internetes tartalmak gyorsítótárazását taglaljuk. Az online szolgáltatások igénybevételéhez kapcsolódó felhasználó élményt jelentősen befolyásolhatja az elérni kívánt tartalmak betöltési ideje. A gyorsítótár használata lehetővé teszi, hogy egy kérés kiszolgálási ideje lerövidüljön, mivel a tartalom egy hozzá közelebb eső cache-ből származik. Másrészről a tartalomszolgáltató hálózat magjának teljesítménygazdálkodását is segíti, ha nem kell minden kéréssel neki foglalkoznia, hanem azt megbízható „ügynökként" kiszolgálja helyette egy, a felhasználóhoz közelebb elhelyezett gyorsítótár. A Content Delivery Network (CDN) szolgáltatók olyan átfedő hálózatokat képeznek, amelyek képesek gyorsítótárazni az elsősorban publikus, nagy tömegek által letöltött tartalmakat. A publikus CDN szolgáltatókon túl további speciális CDN hálózatok is léteznek (5. ábra).

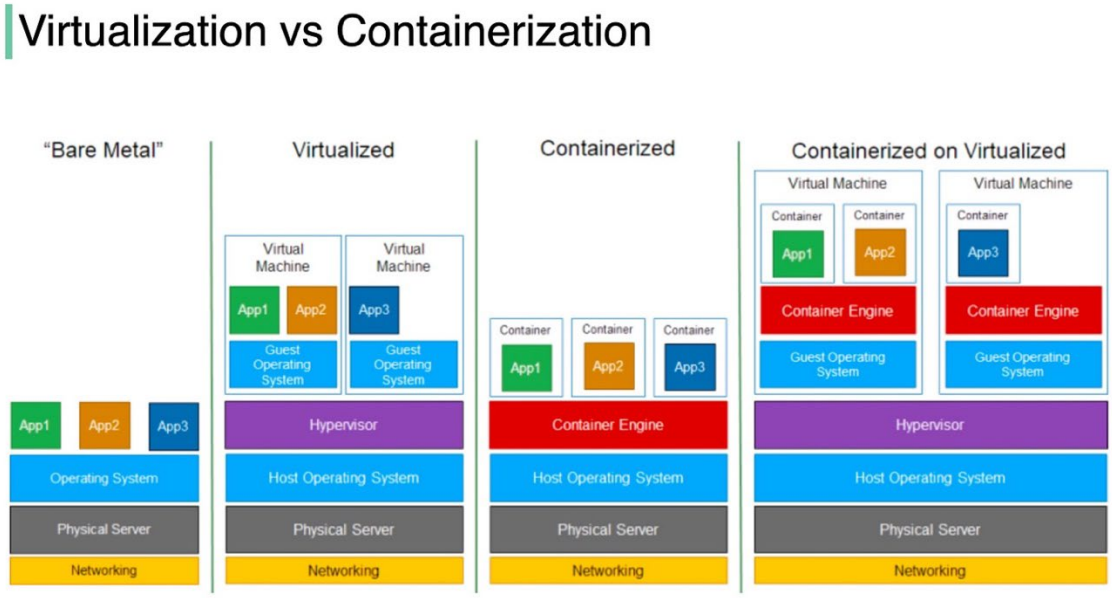


5. ábra A hagyományos CDN és hibrid CDN+P2P architektúrák összehasonlítása

A statikus tartalmi elemek másik jellemző gyorsítótárazási módszere a fordított proxy-k alkalmazása. Ez a szolgáltatás egyfajta előtétet képez a backend webalkalmazás előtt a külvilág felé. A gyorsítótárazás mellett terheléselosztási, SSL/TLS végződtetési és biztonsági védelmi funkciói is lehetnek. Egy lehetséges harmadik megoldás a tartalomadaptációs proxy-k használata, amelyek a végfelhasználóhoz közel elhelyezkedve nem csak továbbító és

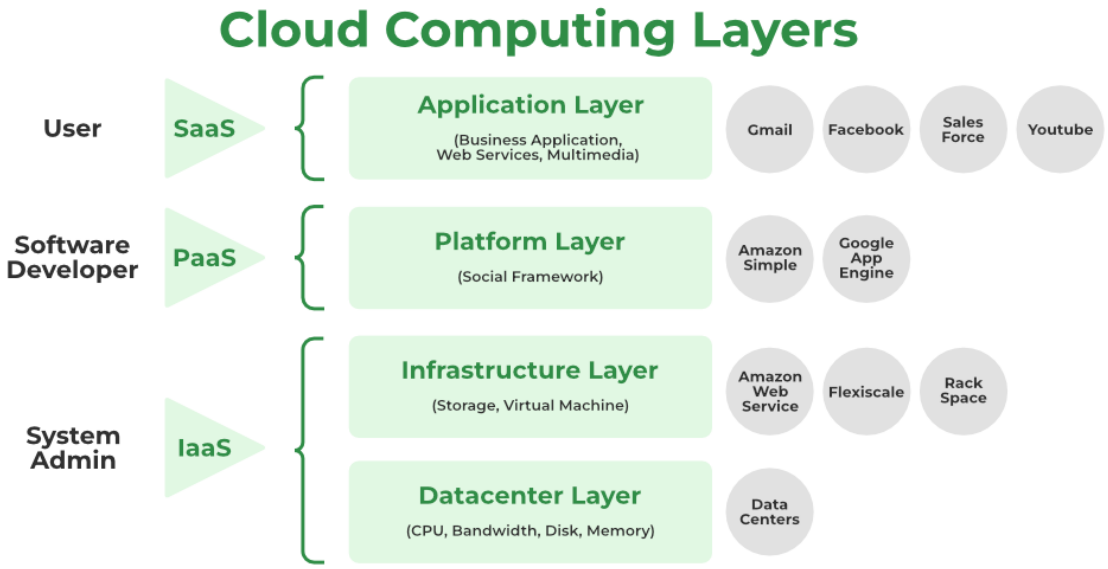
gyorsítótárazó funkciót látnak el, hanem a lekért tartalommal kapcsolatos vizsgálatokat és szűrést (pl. víruskeresés), esetleg módosítást (komplex tartalomszűrés, nyelvi fordítás, A/V transzkódolás) is végezhetnek. Ezek a vizsgálatok erőforrásigényesebbek, ezért az említett funkciókat valamilyen interfész segítségével kapcsolják a hagyományos proxy-khoz. A tartalomadaptációs proxy-kat jellemzően vállalati környezetben alkalmazzák valamilyen vállalati kategóriás tűzfal megoldással kombinálva. Végül meg kell említenünk még olyan megoldásokat is, mint a transzparens proxy, a keresőmotorok gyorsítótárazása és a kliens oldali gyorsítótárazás.

A 8. fejezet a felhőalapú számítástechnikáról szól. Egy új szolgáltatás indulásához szükséges szoftver és hardver erőforrásokat a leggyorsabban és leghatékonyabban a felhőszolgáltatók tudják biztosítani. A legismertebbek a publikus felhőszolgáltatások, de valójában több dedikált felhőinfrastruktúra épült a népszerű szolgáltatások (pl. közösségi hálózatok, videómegosztók) kiszolgálására is. A felhőbe költözés legfontosabb előzetes lépése a virtualizáció, vagyis annak elérése, hogy egy adott szolgáltatás ne egy adott hardverhez kötődjön. Két fontos formája a hardver virtualizáció és a konténeralapú virtualizáció (6. ábra).



6. ábra Virtualizációs és konténerizációs lehetőségek

A felhőszolgáltatás tekintetében megkülönböztethetünk publikus felhőket, amelyek üzleti céllal létrehozott szolgáltatások, privát felhőket, amelyeket jellemzően ipari szereplők, multinacionális nagyvállalatok, államigazgatási szervek és népszerű tartalomszolgáltatást alakítanak ki azért, hogy saját IT szolgáltatásaiknak legalább egy részét saját maguk által épített és felügyelt adatközpontokkal biztosítják, valamint multi és hibrid felhőket (7. ábra).
A legfontosabb várható jelenségek ezen a területen: a felhőnatív alkalmazások terjedése, a hálózati szoftverizáció, a gépi tanulás és a mesterséges intelligencia alkalmazása, a biztonsági szempontok erőteljes érvényesítése a DevOps gyakorlatban, a Function-as-a-Service koncepció terjedése, a multifelhő népszerűsödése és a blokklánc technológia használata.

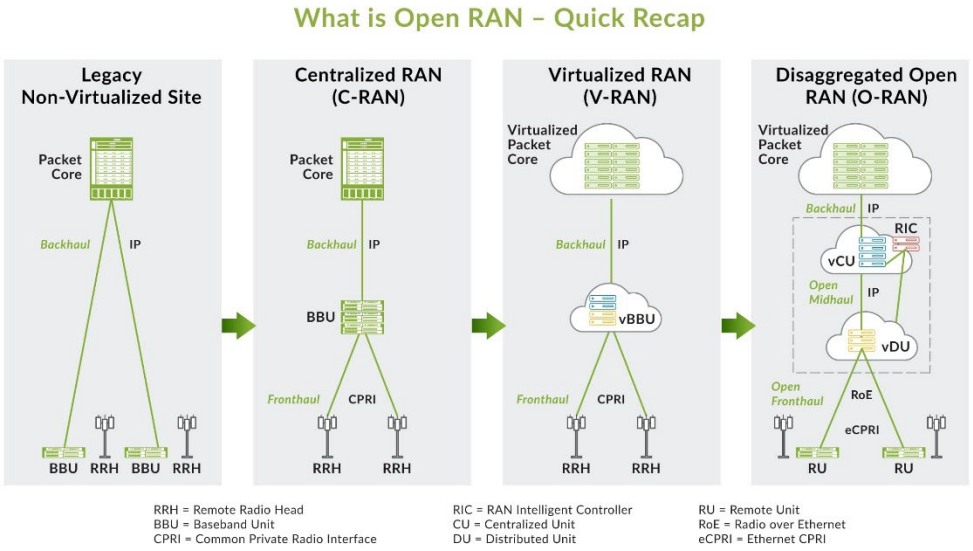


7. ábra A felhőben jellemző szolgáltatásrétegek

A területet érintő legfontosabb kihívások a biztonság, a költséghatékonyság, az integráció és a szolgáltatófüggőség feloldására a nyílt forráskód használata.

A 9. fejezetben az 5. generációs mobilhálózatokat mutatjuk be. Az 5G vagy ötödik generáció a cellás mobilhálózatok legújabb generációja, mely jelentős előrelépést jelent a korábbi 4G/LTE technológiához képest a sebesség, a kapacitás, a késleltetés és a támogatható alkalmazások köre tekintetében. A korszerű virtualizációs technológiák, a mikroszolgáltatás architektúra és a hiperautomatizáció együttesen alakítják az újgenerációs mobilhálózatok által nyújtott képességeket.
Jelenleg kétféle 5G telepítéssel találkozhatunk, a non-stand alone (NSA) konfiguráció esetén a meglévő LTE hálózatba építjük be az 5G hálózati komponenseket (gyorsan kivitelezhető barnamezős telepítések). Jellemzően egy 5. generációs rádiós hozzáférési hálózatot kapcsolnak össze a meglévő LTE EPC maghálózattal. Ebben az esetben az új technológia előnyei csak korlátozottan érhetőek el és az 5G NSA hálózatokat átmeneti megoldásnak tekinthetjük a teljesen önálló, ún. stand-alone (SA) 5G hálózatok felé, melyek végponttól végpontig biztosítják az 5. generációs mobilhálózati összeköttetést.
Az 5. generációs kommunikációs hálózatok kulcsfontosságú eleme a felhőalapú maghálózat és a Cloud RAN technológia, amely központosítja az alapsávi feldolgozást, mely a RAN alapsávi szoftver és a RAN alapsávi hardver szétválasztásán alapul. Az 5. generációs kommunikációs hálózatok szempontjából talán a legfontosabb újdonsága a felhőalapú rádiós hálózatoknak az erőforrások hatékony menedzsmentje a központosításnak köszönhetően. Lehetővé válik az erőforrások dinamikus, igény szerinti kiosztása, miáltal csúcsidőszakokban is biztosítható az alacsony torlódás és a megfelelő QoS szint. Az 5G felhasználási esetek (virtuális valóság, autonóm járművek, ipari IoT) szempontjából kulcsfontosságú az alacsony átviteli késleltetés és a nagy áteresztőképesség. Az adaptív erőforrásallokációval a C-RAN is hozzájárul ezen kritériumok teljesüléséhez. Nem utolsó szempontként a hálózati skálázhatósága is jelentősen növekszik a korábbi technológiákhoz képest.
Az Open RAN egy hálózati architektúra és technológiai koncepció, amelynek célja a RAN összetevőinek szétbontása és szabványosítása, amely magában foglalja az alapsávi egységet (BBU) és a rádióegységet (RU). Fontos továbblépés, hogy az Open RAN kiterjeszti a C-RAN-ban megjelenő szétválasztás koncepcióját a szabványosítás igényével. Ez a megközelítés

nagyobb rugalmasságot, interoperabilitást és innovációt tesz lehetővé a vezeték nélküli hálózatok tervezésében és telepítésében.



8. ábra RAN modellek összehasonlítása

Mind az Open RAN, mind a Cloud RAN innovatív megközelítés a rádió-hozzáférési hálózatok modernizálására és hatékonyságának javítására (8. ábra). Mindkét megközelítésnek megvannak a maga erősségei és potenciális előnyei, és a választás a konkrét felhasználási esetektől és követelményektől függ.

Végső soron az O-RAN és a C-RAN közötti választás több tényezőtől függ: i) a hálózat speciális követelményei, ii) a szolgáltató preferenciái és iii) a meglévő infrastruktúra. Összességében elmondható, hogy a következő öt éves időszakban az O-RAN technológia jelentős elterjedése prognosztizálható. Ugyanakkor az Európai Unió megbízásából elvégzett szakértői vizsgálatok arra jutottak, hogy az Open RAN jelenlegi fejlettségi szintjén potenciális biztonsági kockázatokat rejt magában.

Az 5G hálózatokban alkalmazható network slicing technológia lehetővé teszi egyetlen fizikai hálózati infrastruktúra felosztását több virtuális hálózatra, amelyek mindegyike egyedi felhasználási esetekre és alkalmazásokra van szabva (pl. rendkívül megbízható alacsony késleltetésű kommunikáció kritikus alkalmazásokhoz, továbbfejlesztett mobil szélessáv a nagy sebességű internethez stb.). Mindegyik hálózati szelet önálló hálózatként működik, egyedileg definiált specifikus karakterisztikával és erőforrásokkal. Az 5. generációs hálózatok a dinamikus menedzsmentfunkciók bevonásával új üzleti modellek létrejöttét is támogatják.

Ezáltal a nyilvános infrastruktúrán lehetségessé válik privát mobilhálózatok működtetése. Ezeket egy-egy szervezet egyedi kommunikációs céljaira hozzák létre általában egy meghatározott földrajzi területen és a teljes hálózat a szervezet specifikus üzleti céljai szerint kerül kialakításra. A privát LTE és 5G hálózatok iránt jelentős érdeklődés mutatkozik, különösen az olyan területeken, mint a gyártás, az egészségügy, a közlekedés, a közművek és az intelligens városok. Lehetővé teszik a szervezetek számára, hogy ellenőrzött és biztonságok környezetben aknázzák ki a fejlett vezeték nélküli technológiákat a kritikus fontosságú alkalmazásokhoz, és kihasználják az olyan feltörekvő technológiák előnyeit, mint az IoT és az automatizálás.

A bemutatott képességek és funkciók együttesen egy olyan jövő felé mutatnak, ahol a mobilhálózatok az alkalmazások széles skálájának szerves részét képezik, és hatással lesznek az iparágakra, az egészségügytől és a közlekedéstől a szórakoztatásig és a gyártásig. A

mobilhálózatok folyamatos fejlődése döntő szerepet fog játszani a jövő digitális világának kialakításában. Az 5G generációs kommunikációs hálózatok terjedésének és az általuk nyújtott szolgáltatások fejlődésének egyik erőteljes katalizátora lehet az Open RAN technológia. Mind európai, mint globális szinten egyértelmű tendencia az első O-RAN hálózatok megjelenése produktív környezetben. A következő években exponenciális növekedést várunk az O-RAN technológiát alkalmazó kommunikációs hálózatok számában. Az 5. generációs mobilhálózatok ipari elterjedésével a peremszámítástechnika is egyre jelentősebb szerephez jut a fenti kritériumok teljesítésében. Az 5G hálózatokon megjelenő alkalmazások széles spektruma a hálózat- és szolgáltatásmenedzsment feladatokat is jelentősen komplexebbé teszi. A napi üzemeltetési feladatok jelentős részének automatizálása elkerülhetetlenné válik a megfelelő szolgáltatásminőség fenntartásához. Ezekre a jövőben mesterséges intelligencia alapú technológiákat fogunk használni, melyek segítségével a feladatok egy részében a human-in-the-loop működésről az operátorok átállhatnak human-on-the-loop megközelítésű működésre.

A 10. fejezet az online platformokat mutatja be, amelyek a jelenkori Internet fejlődésének, bővülésének hajtómotorjai, mivel az internet hozzáférési szolgáltatás segítségével a világhálóhoz kapcsolódó előfizetőket az online platformok által nyújtott szolgáltatások és tartalmak felhasználókká és fogyasztókká „alakítják át", az előfizetői szokások és igények változása pedig a fejlesztések kiindulópontja tulajdonképpen minden, az Internet működéséhez, szabályozásához és fejlesztéséhez kapcsolódó területen. A fejezetben négy részben bemutatjuk először az információk és tartalmak online megosztását lehetővé tevő szolgáltatásokat, majd a közösségi hálózatokat, a videómegosztó platformokat, végül pedig röviden beszélünk az online piacterek némely típusáról. A különböző platformok a sajátos jellegzetességeik miatt külön-külön is mind fontosak a technológiai fejlődés szempontjából. Fontos látnunk amikor egy-egy platformtípusról vagy akár azon belül egy-egy konkrét szolgáltatásról beszélünk, hogy az egyes alkalmazások és szolgáltatások besorolása sokszor nem egyértelmű, némelyik több platformnak a jellemző sajátosságait is magán viseli. Sőt a fejlesztések iránya is az, hogy egyre több szolgáltatást nyújtó, minél inkább univerzálisan felhasználható és ezért minden másik alkalmazás használatát feleslegessé tevő, egy tulajdonosi kézben lévő ökoszisztémák jöjjenek létre. Ezeket nagyon jól példázzák az Alphabet és a Meta törekvései.

A webes fáljtárolás és fáljmegosztás még mindig egy nagyon széles területet takarhat, amibe a torrentoldalakat éppen úgy bele lehet érteni, mint a bizonyos típusú médiatartalmak – például képek – megosztására szerveződött szolgálatatásokat és még számtalan mást is. Ha elég szűkre húzzuk az értelmezés lehetőségét, akkor leginkább olyan szolgáltatásokat kell vizsgálnunk, amelyek webes szolgáltatások, tehát mind a fájl elhelyezése, mind annak elérése leginkább egy böngészőn keresztül történik, az elhelyezett és elért digitális állományoknak, vagyis a fájloknak, nincs valamilyen jellemző szűkítő értelmet hordozó jelzőjük vagy jellemzőjük, tehát például nem képek vagy éppen nem programkódok, a fálj elhelyezése történhet kizárólag tárolási céllal, de a különböző megosztási lehetőségeket használva a felhasználók a tárolt állományaik egy halmazát vagy egészét elérhetővé tudják tenni más felhasználók számára is akár az elhelyezés után közvetlenül, akár számottevően később és végül az állomány elhelyezője és az elérést kezdeményező személyek között valamilyen kapcsolat áll fenn.
Elvileg megkülönböztethetünk file hosting és file sharing rendszereket, azonban ezek ma már nem igazán léteznek ilyen tiszta állapotban. Sőt, a legtöbb ilyen rendszerhez már számtalan

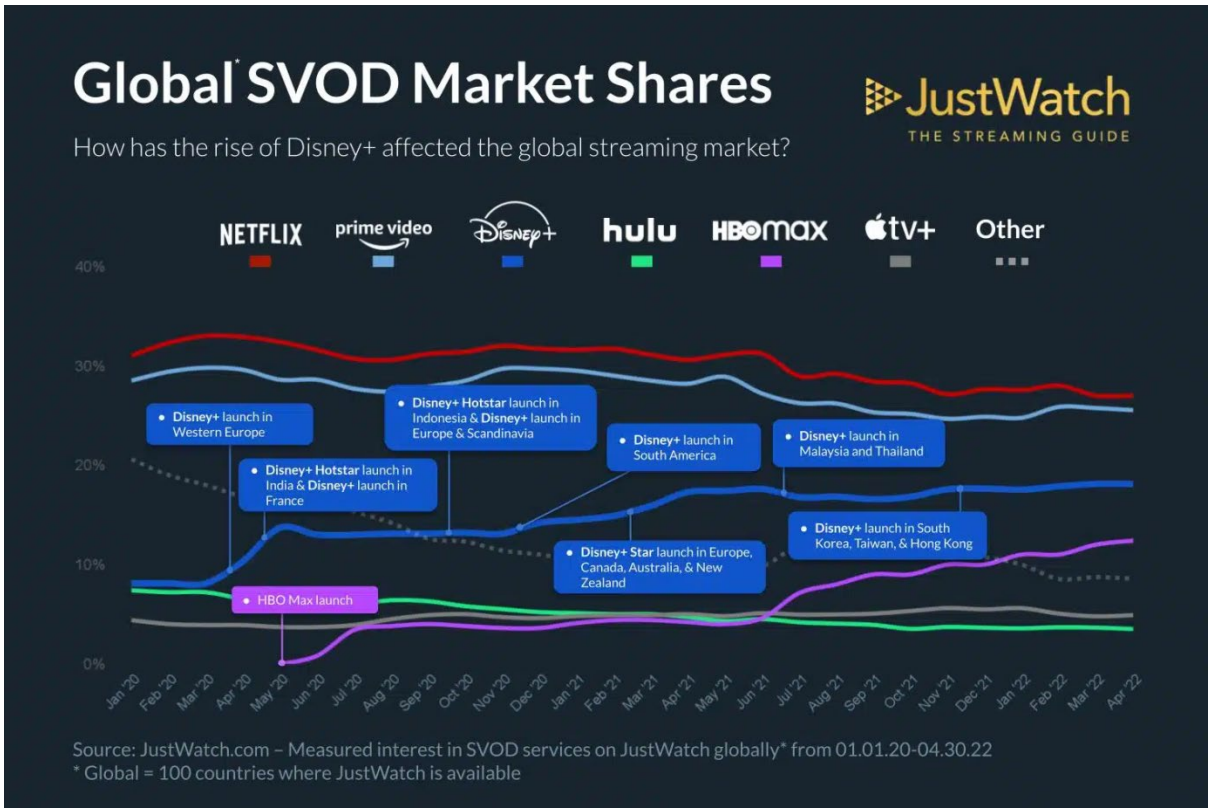
egyéb szolgáltatás is kapcsolódik, például a felhasználói könyvtárral való szinkronizálás, vagy éppen az ütemezett biztonsági mentés. Ezek rendszerek ma már többnyire felhőalapúak, értelemszerűen a nagy felhőszolgáltatók (Amazon, Google, Microsoft) önálló platformokat is nyújtanak, amelyek egyébként a piacai felmérésekben a népszerűségi vagy ismertségi listák első felében szerepelnek. Ugyanakkor konkrét piaci arányokat nagyon nehezen állapíthatunk meg, mivel az egyes elérhető elemzések jelentős eltéréséket mutatnak, ráadásul a vizsgálat vagy akár csak a rangsorolás módszertana sem teljesen világos a legtöbb esetben. Fontos még látni, hogy a digitális állományok online tárolására és megosztására szolgáló platformok sok esetben nem önállóak, hanem egy-egy fokozatosan kialakuló, manapság is bővülő szolgáltatáshalmazú kollaboratív szoftvercsomag részei, ami azzal is jár, hogy magának a file hosting és sharing szolgáltatásoknak az ismertsége vagy népszerűsége nem választható el a kollaboratív rendszer felhasználói körének nagyságától.
Az ismert nagy felhőszolgáltatók mellett mindenképpen említeni kell még tőlük független szereplőket, akik többnyire tényleg csak a fájltárolással és –megosztással foglalkoznak, illetve az ezekkel szorosan összefüggő szolgáltatásokat nyújtanak. A legismertebbek ezek közül a Box, a Dropbox, a Baidu Wangpan, a MediaFire, a Mega és még talán a Yandex. Ez utóbbi leginkább Oroszországban népszerű, a Baidu Wangpan leginkább Kínában, míg a többiek nemzetköziek. Azt látnunk kell, hogy ebben a szegmensben nagyon jelentős a technológiai vagy gazdasági alapú piaci mozgás, vagyis az elmúlt évtizedek trendjei alapján eléggé valószínűnek mondható, hogy 10 éven belül az ebbe a csoportba sorolható szolgáltatások jelentős része – akár a fele is – már nem lesz elérhető.
Egy külön csoportot képez egymagában az Apple iCloud szolgáltatása, amely nemcsak az állományok – elsősorban a felhasználó által készített saját médiatartalmak és a biztonsági mentések – hosszútávú, biztonságos és kényelmes tárolására szolgál, hanem emellett levelezési lehetőséget, illetve a kontaktlista és a naptár szinkronizálására is lehetőséget nyújt. Ennél is lényegesebb azonban az, hogy több rendszerszolgáltatás és az Apple által fejlesztett applikáció számára az iCloud a backend. Mivel ezek az Apple-ökoszisztéma legfontosabb részei, amelyek kiemelten szolgálják a felhasználók kényelmét és biztonságát, ezért az iCloud előreláthatólag hosszútávon a piac jelentős szereplője marad.
Az információk és tartalmak online tárolására és megosztására szolgáló rendszerek legfontosabb „értékei” a rendelkezésreállás és a biztonság. Ebben a tekintetben a felhő alapú szolgáltatások hosszútávú előnye mutatkozik, de akár a nagyobb rendszerleállások globális szolgáltatóknál vagy a kisebbeknél bekövetkezett zsarolóvírusos támadások azt mutatják, hogy mindkét téren van még lehetőség az előrelépésre.

A fejezet második része a közösségi hálózatokkal foglalkozik, vagy ha technikailag pontosabban akarunk fogalmazni, akkor a közösségi hálózatok tagjai közötti kommunikációt támogató platformokkal. Ezek széleskörű megjelenése és elterjedése a harmadik évezred jelensége. A magyar terminológiában a social media vagy közösségi média gyakran előfordul és régóta használjuk a social networking helyett. Az előbbi eredetileg szűkebb értelmű volt, bár mostanra a jelentések összemosódása az angol nyelvterületen is tapasztalható.
A közösségi média olyan interaktív technológiák és virtuális térben végzett tevékenységek összessége, amelyek elősegítik információk, ötletek, érdeklődési körök és egyéb kifejezési formák létrehozását és megosztását virtuális közösségeken és hálózatokon keresztül. A tanulmányunkban röviden bemutatjuk a Meta által irányított közösségi média platformokat (Facebook, Messenger, Instagram, WhatsApp), az USA-ban nagy jelentőségű X-et (Twitter) és a Kínában abszolút dominánsnak számító WeChatot. A közösségi média piac mostanra telítetté vált és úgy tűnik, hogy újabb felhasználókat már csak egymástól tudnak szerezni a

kisebb-nagyobb szereplők, amit az a tény is hangsúlyoz, hogy csak 10 olyan ország van a Földön, amelyben nem a Meta valamelyik platformja a piacvezető. A cégek a kihívásokra reagálva különböző irányokban keresi a kitörési lehetőségeket, amelyek azonban sérthetik a saját felhasználóik vagy más, szektoron kívüli gazdasági szereplők érdekeit is. Az egyik ilyen lépés a felhasználók által előállított médiatartalmak mellett az átvett vagy gyártott média megjelenése, amely a hagyományos sajtótermékeket fosztja meg a hirdetési bevételeiktől. A másik lépés a felhasználók nagyon részletes személyi profiljának kereskedelmi célú felhasználása. A Meta esetében ez azt is jelenti, hogy a kevésbé aktív felhasználók profilját célzott hirdetésekre adott reakciók alapján egészítik ki.
A közösségi hálózatokkal kapcsolatban időről időre felmerülnek különböző problémák, amelyek közül a jelentősebbek a felhasználói profilokban tárolt információk kereskedelmi és politikai célú felhasználása a felhasználó engedélye nélkül, a „tényellenőrzés" névvel illetett tevékenység transzparenciájának hiánya, a „tényellenőrzés" következtében megjelenő cenzúra és a véleményszabadság megsértése, a politikai befolyásszerzés, a hálózatsemlegesség elveinek megsértése, illetve a felhasználók személyiségi jogainak és személyes adataikhoz fűződő jogainak megsértése.

A videóforgalom mostanra a publikus Internet teljes forgalmának nagyjából 71%-át adja, de ez az arány az előrejelzések szerint tovább növekszik majd a következő 5 évben 80%-ra. Emellett egy olyan típusú szolgáltatásról beszélünk, amely szolgáltatásminőségi követelményei és az általa igényelt nagy átbocsátóképesség miatt folyamatos kihívás elé állítja a hálózatok fejlesztőit és üzemeltetőit. A videómegosztó platformok és szélesebb körben a VoD-jellegű szolgáltatások ugyanakkor egyre növekvő bevételeket generálnak az ilyen platformok tulajdonosainak.
Amikor videómegosztó platformról beszélünk a 10. fejezet harmadik részében, akkor a legtöbb esetben a Youtube merül fel példaként, amely a Similarweb szerint az Internet második legmagasabb forgalmát produkáló platformja. A Youtube a hagyományos videómegosztók közé tartozik, ahol a nagy fogyasztói közönség mellett jelentős számú feltöltő is van, vagyis akik a tartalmakat hozzáadják. Ezek a tartalmak nagy változatosságot mutatnak mind hosszukat, mind minőségüket, mind műfajukat és céljukat tekintve. Vannak ún. csatornák, melyek ugyanattól a szerzőtől származó videók halmazát jelenti. A videók megtekintése legtöbbször ingyenes, a felhasználó hirdetéseket tekint meg a videó elején – hosszabb videó esetén időnként közben is – amelyből az üzemeltetőnek bevétele keletkezik. Másrészt előfizetési díj fejében a szolgáltatás reklámmentessé válik. A nagy nézettségű tartalmak elhelyezőit a Youtube premizálja. A Youtube nemcsak széleskörű kínálatával, hanem a szolgáltatás színvonalával, a mögötte meghúzódó folyamatos mérnöki innovációval is élenjáró a hasonló platformok között.
A hagyományos videómegosztók megjelenésükkor hirtelen jelentős, ráadásul egyre növekvő felhasználói bázisú vetélytársat jelentettek a hagyományos műsorszórók számára. Hasonló konkurencia lett aztán például a Youtube számára a Netflix, amely online DVD-kölcsönzőként indult még 1998-ban és emellett indult be a 2000-es évek közepén a streaming szolgáltatás. Bár a Netflix streaming szolgáltatása ugyanúgy online videómegosztó, mint a Youtube, azért markáns különbségeket látunk, mivel a Netflix kezdettől fogva jogvédett tartalmakat is kínált, amelyekért havi előfizetési díjat kellett fizetni és a Netflix lassan már egy évtizede mutat be saját gyártású tartalmakat.
A Netflix előfizetőinek száma nagyjából 240 millió, ami ugyan kevesebb, mint a tizede a Youtube 2,5 milliárd feletti felhasználójának. Ugyanakkor ez az összehasonlítás csalóka,

hiszen amíg a többieknél többnyire egyéni ügyfelekről beszélünk, akik a szolgáltatásért nem fizetnek, a Netflix esetén minden előfizető bevételt termel és az előfizetés nem személyre, hanem háztartásra vonatkozik és így az elért nézők száma milliárdos nagyságrendbe eshet.
A Netflix nyomdokán haladva több konkurens szolgáltatás is megjelent a piacon, például a Hulu, a Disney+, az Apple TV+, az Amazon Prime és a HBO Max, hogy csak a legismertebbeket nevezzük meg (9. ábra). Ezek a szolgáltatók hasonló modell szerint működnek, mint a Netflix, gyártanak saját tartalmakat is, amely között kifejezetten nagy költségvetésű filmek vagy sorozatok is vannak. A forgalmat tekintve a Netflix máig a legnépszerűbb közöttük, de piaci részesedéséből veszített az elmúlt években. Az előfizetések számát tekintve Amazon Prime Video mellett a dinamikusan bővülő Disney-csoport (a Disney+, a Hulu és az ESPN együtt) is nagyon közelíti már.



9. ábra A videó streaming szolgáltatók piaci részesedésének alakulása 2020.01-2022.04 között

A harmadik csoportnak a legismertebb képviselője a TikTok, amely nagyon rövid idő alatt lett a piac egyik domináns szereplője, hiszen a 2016-os alapítású kínai vállalat mostanra a 1,6 milliárd felhasználóra tett szert, amibe még nem számoltuk bele kínai változatának, a Douyinnak csaknem 800 millió felhasználóját. A TikTok eredetileg nagyon rövid, lipsyncinges és táncolós videótartalmak megosztására adott lehetőséget, tulajdonképpen mondhatnánk ezeket vírusvideónak is. Mostanra természetesen teljes értékű videószolgáltatássá nőtte ki magát, azonban az eredete és jellege is sokkal inkább rokonítja a közösségi médiával, mint például a Youtube-bal. A rövid idő alatt hatalmas picra szert tevő platform természetesen „megihlette" a távolabbi konkurenseit is, a Youtube például 2020-ban jelentette be a Youtube Shorts szolgáltatását, amelyet általánosan a TikTokhoz hasonlítanak. Ugyanakkor a TikTok elterjedése valamelyest meg is „tisztította" a Youtube-ot, vagyis miután a „TikTok-stílus" kedvelőinek lett egy önálló platformja, a Youtube-on jelentősen lecsökkent az ilyen típusú videók száma és az ajánlatokban való felbukkanásuk gyakorisága is.

Az összes különbözőség ellenére mindhárom szolgáltatástípus esetén a működés, a népszerűség növekedésének és az új felhasználók bevonzásának kulcsa a nagyon jól működő ajánlórendszer, vagyis az az algoritmus, amely a felhasználó által korábban és aktuálisan megtekintett videók jellemzői alapján ajánlatokat tesz a következő videóra.
A jövőben vélhetően a különböző típusú platformok konvergenciája sokkal inkább észrevehető lesz, és itt elsősorban az online médiamegosztó platformokra és a közösségi hálózatokra gondolhatunk. A Facebookon történő előre felvett vagy élő videó közvetítése belátható módon technológiai szempontból semmiben nem különbözik attól, ahogyan ezt a videómegosztók végzik. A videómegosztókon elhelyezett értékelések és kommentek ugyanígy jellegükben nem különböznek a közösségi oldalak posztjaitól és a posztokra adott hangulatjelektől.
A TikTok és hozzá hasonló társai a rövid idejű, gyorsan fogyasztható videók mellett az egészen kitűnő ajánlórendszereiknek köszönhetik az elnyert népszerűségüket. Ugyanakkor az ajánlórendszerek által az egyes felhasználókról gyűjtött masszív adatmennyiség nagyon komoly aggodalmat keltett – és nem csak az ún. „nyugati világban" –, olyannyira, hogy több országban betiltották vagy korlátozták a használatát.
A pornográf tartalmak megosztására szolgáló online platformokkal a videómegosztó platformokon belül érdemes foglalkozni, mivel a pornográf médiaforgalom túlnyomó része videó. Az ezzel foglalkozó oldalak közül négy is szerepel az Similarweb internetforgalmi rangsorának első 25 helyezettje között. Előfizetők számára vonatkozó friss adatokat értelemszerűen nehéz találni, viszont a tanulságos látni, hogy 2022 novemberében a legnagyobb látogatottságú oldalak rangsorában a negyedik és az ötödik pozíciót foglalta el a Pornhub (10,2 milliárd oldalfelkeresés) illetve az Xvideos (8,7 milliárd oldalfelkeresés).
A pornográf videómegosztók működésével kapcsolatban hasonló kérdések merülnek fel, mint a hagyományos videómegosztókkal kapcsolatban. Az egyik ilyen kérdés lehet a megosztott videófelvételek szerzői joga. Ezzel kapcsolatban a pornográf videómegosztók ugyanazon elvek szerint jártak el, mint a hagyományos megosztók, vagyis törölték a megosztott videókat. Egy másik kérdés lehet a felhasználók személyiségi jogainak védelme. Ez a probléma itt még nagyobb jelentőséggel bír, mint a hagyományos videómegosztóknál, mivel a látogatók és az előfizetők túlnyomó többségükben szeretnék a személyazonosságukat elrejteni. A nagyobb oldalak természetesen titkosítással védik az adatokat, de attól még időről időre előfordulnak kisebb adatbiztonsági incidensek.

A 11. fejezetben nagyon röviden kitérünk arra, hogy a hétköznapi felhasználók számára látszó Internet valójában az infrastruktúra és a rajta keresztül elérhető online platformok szolgáltatásainak elválaszthatatlannak tűnő egysége. Az iparági gyakorlatban azonban a két rész tulajdonosi köre, érdekei, bevételei változásának dinamikája eltérőek. A mostani helyzetben az online platformok üzemeltetői jóval nagyobb hányadát kapják az Internet által termelt nyereségnek, mint az ISP-k, míg az erőforrásbővítés terheinek jelentős része az ISP-kre hárul. Ez feszültséghez vezet a két csoport között, amit azzal lehetne feloldani, ha a tartalom és alkalmazásszolgáltatók is részt vállalnának az infrastruktúra fejlesztésében. Ezeknek a problémáknak egyébként hálózatsemlegességi aspektusa is van, a jelenlegi trendek a technológiák és a platformok szabad versenye helyett az oligopol piac kialakulása felé mutatnak.

2 Bevezetés

Az Internet és a hozzá kapcsolódó, rajta keresztül elérhető szolgáltatások az emberiség egészére és külön-külön is az egyének többségének életére jelentős hatást gyakorolnak. Az információ elérése korábban sosem volt még ilyen egyszerű, az alapműveltség és a tudás megszerzése még sosem volt ilyen könnyű, a szórakozás, a kapcsolatteremtés lehetősége még soha nem volt a többség számára ennyire elérhető. Ugyanakkor egy hír megbízhatósága semmit sem javult attól, hogy az interneten keresztül jutott tudomásunkra, a tanulás folyamatát nem segíti, ha egyszerre befogadhatatlan mennyiségű, rendszerezetlen, némileg megbízhatatlan és esetleg egymásnak ellentmondó tudásmorzsa temet maga alá minket, ahogy a szórakozás sem önmagában értékes, hanem attól, amit kapunk általa. Az emberi kapcsolatok terén a személyes ismeretséget, a barátságot és az emberi közelséget nem pótolhatja akárhány like sem, ugyanakkor a dislike fájhat ugyanannyira, mint egy személyes sértés.

A technológia és a szolgáltatások működésének ismerete, a háttérben többé-kevésbé eldugott gazdasági, társadalmi, politikai motivációk feltárása segít bennünket eligazodni ebben a világban, segít a helyén kezelni ezt a nagy és folyamatos változást.

Ennek a tanulmánynak a célja, hogy áttekintést nyújtson az online ökoszisztémákról, azokról a rendszerekről, amelyekből összeáll az a nagy egész, amit internetnek hívunk. Az áttekintés nem lesz egyforma mélységű minden területen, nem is érinti az Internet minden elemét, hanem arra igyekszünk fókuszálni, ami a felhasználók számára látható, megtapasztalható, igénybevehető szolgáltatások létezését lehetővé teszi.

A jelen dokumentum 3. fejezetében az Internet egyes architekturális elemeit mutatjuk be, az Internet adatkicserélő központ okat és az átalunk nyújtott társviszonyt, az interneten nyújtott tranzitszolgáltatást, az internet hozzáférési szolgáltatást – külön kitérve a rádiós hozzáférési lehetőségekre – és a virtuális magánhálózatokat.

A 4. fejezetben az Internet névtérszolgáltatásának, a DNS-nek a működését tekintjük át. Mivel ez egy kritikus eleme az Internetnek, ezért részletesen bemutatjuk a jellemző támadástípusokat és a használatos védelmi eljárásokat is.

Az 5. fejezetben az Internet biztonságos működése szempontjából elengedhetetlen digitális tanúsítványkiadó hatóságokkal és a nyilvános kulcsú infrastruktúrával foglalkozunk.

A 6. fejezet az IP feletti személyközi kommunikációról szól, a publikus Interneten történő médiakommunikáció mellett a 4G-s mobilhálózatokban használatos Voice over LTE és az 5G-sekben használt Voice over New Radio megoldásokat is bemutatjuk.

A 7. fejezetben a digitális tartalmak gyorsítótárazásáról írunk, amely a felhasználói élményre gyakorolt pozitív hatása mellett a tartalom eredeti kiszolgálójának erőforrásait is kíméli.

Korunk egyik internetes csodafegyvere a felhőalapú számítástechnika, amelyről a 8. fejezet szól. Az eddig is meglévő felhasználási esetek mellett újak kialakulását látjuk jelenleg, amelyeket többek között a mesterséges intelligencia alkalmazása, a dolgok internetének evolúciója és robbanásszerű elterjedése és az 5G-s mobiltechnológia mind szélesebb körű telepítése is hajt.

Ez utóbbi a témája a 9. fejezetnek, amelyben a Cloud RAN és az Open RAN versengő koncepcióinak felmutatása mellett a következő öt éves időszakban az O-RAN technológia térnyerését prognosztizáljuk.

A 10. fejezetben az Internetnek a felhasználók számára legismertebb részei, az online platformok kerülnek górcső alá. Részletesen írunk az online fájltároló és megosztó rendszerekről, bemutatva néhány, valamilyen szempontból említésre méltó piaci szereplőt.

Aztán a közösségi hálózatokról nyújtunk egy rövid elemzést, amelyben külön kitérünk a velük kapcsolatban felmerült kritikus észrevételekre is. A videómegosztó platformok jelentőségét nem lehet eléggé hangsúlyozni, hiszen jelenleg is az Internet forgalmának már több, mint 70%-át adják. A klasszikus elvek szerint működő platformok mellett szóba kerülnek a VoD streaming szolgáltatások és a TikTok-stílust követő új versenyzők is. Végül az online piacterek néhány példáját mutatjuk be.
A 11. fejezetben arról írunk, hogy a világháló architektúráját fejlesztő és működtető vállalkozások és az online platformok üzemeltetői miként tehetnek közösen azért, hogy az Internet működésével a felhasználók elégedettek legyenek.

3 Az Internet architektúrája

Internetnek hívjuk a világszerte infokommunikációs eszközök milliárdjait összekötő hálózatot. Amikor jelen tanulmányunkban az Internet architektúrájáról beszélünk, akkor ebbe ténylegesen csak azokat az elemeket értjük bele, amelyek a hálózati végpontok közötti kapcsolatok kiépítésében és fenntartásában szerepet játszanak. A végpontok sokfélék lehetnek: érzékelők, beavatkozók, kliensek, kiszolgálók vagy éppenséggel egyenrangú eszközök. Az ezeket összekötő hálózatrészeket többek között a szerepük, az elhelyezkedésük, a tulajdonosi és felhasználói körük szokták csoportosítani.
A továbbiakban röviden értekezünk internet kapcsolódási pontokról (IXP), az internet továbbítási szolgáltatásról (IP transit), az internet hozzáférés szolgáltatásról (IAS), a vezeték nélküli hozzáférési pontokról (WiFi HotSpot) és a virtuális magánhálózatokról (VPN).

3.1 Internet adatkicserélő központok (IXP)

3.1.1 Mi az Internet Exchange Point?

Az Internet adatkicserélő központ[1] (Internet Exchange Point, IXP) egy olyan fizikai hely, amelyen keresztül az internetes infrastruktúrához kapcsolódó szolgáltatásokat nyújtó vállalatok közvetlenül csatlakoznak egymáshoz abból a célból, hogy internetes forgalmat cseréljenek. Ezek a vállaltok lehetnek például internetszolgáltatók (ISP-k) és tartalom közvetítő szolgáltatók (CDN-k), tartalomszolgáltatók, felhőszolgáltatók és SaaS szolgáltatók.
A fentebb említett vállalatok nézőpontjából ezek a helyek a hálózataik „szélén” (edge) találhatóak és lehetővé teszik számukra, hogy a saját hálózatukon kívülre forgalmat továbbítsanak, vagyis tulajdonképpen tranzitszolgáltatást tudnak igénybe venni. Ha az IPX, mint önálló szereplő oldaláról nézzük a helyzetet, akkor az IPX egy olyan fizikai helyen található, ahol több különböző hálózat ér össze. Ilyen helyek például az adatközpontok. Az IPX ezeken a helyeken fizikai hálózati kapcsolók – switchek – felhasználásával összeköttetést biztosít ezeknek a hálózatoknak.
Az IPX-ben való jelenlét lehetővé teszi a résztvevő vállalatok számára, hogy a kifelé menő forgalmuk kisebb hányadát kelljen a tranzitszolgáltatókon keresztül továbbítaniuk, csökkentve ezáltal a szolgáltatásuk átlagos bitenkénti szállítási költségét (per-bit delivery cost). Ugyanilyen jelentősnek mondható előny, hogy az IPX-n keresztül esetleg több útvonal érhető el, ami megengedi az optimalizálást és növeli a hibatűrést. Az optimalizálás a felhasználók számára is észrevehető minőségnövekedést eredményezhet, hiszen a rövidebb útvonal kisebb késleltetést jelenthet és a közvetlen összeköttetésen adott esetben magasabb sávszélesség juthat neki.
Az IXP-ek elsődleges alternatívája a privát peering, ahol az internetszolgáltatók közvetlenül kapcsolják össze hálózataikat.

3.1.2 Hogyan működik egy internetes cserepont?

Az IXP egy nagyméretű második rétegben működő lokális hálózat (Layer 2 LANs), amely egy vagy több összekapcsolt Ethernet switch-ből áll, az IXP-ben résztvevő taghálózatok pedig

[1] Például: https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/, https://www.jpnap.net/en/articles/about_ixp.html, https://www.internetsociety.org/issues/ixps/, https://www.thousandeyes.com/learning/techtorials/internet-exchange-point

ezekhez csatlakoznak. Az infrastruktúra és a szolgáltatás telepítési és üzemeltetési költségeit a csatlakozó ISP-k felosztják maguk között, viszont a kölcsönösség elvén többnyire nem számolnak fel költségeket a továbbított forgalomért. Az IPX-ben található hálózat – amely szükség esetén akár több épületre is kiterjedhet – jellegét tekintve nem különbözik a többi Ethernet-hálózattól, átbocsátóképessége, kapcsolási kapacitása azonban akár több Tbps is lehet.

3.1.3 Miért fontosak az internetes cserepontok?

Az IXP-ek alkalmazása nélkül a hálózatok közötti forgalom potenciálisan egy közvetítő hálózatra támaszkodna, amely leginkább – vagy szinte kizárólag – csak az internetes infrastruktúrához kapcsolódó szolgáltatásokat nyújtó vállalatok hálózatai között továbbítana forgalmat. Ezeket tranzitszolgáltatóknak nevezzük és így folyik a nemzetközi internetes forgalom nagy része. Néha ezeknek a használata elkerülhetetlen, mivel költséges a közvetlen kapcsolat fenntartása a világ minden egyes internetszolgáltatójával. Amikor a forgalomforrást és a nyelőt tartalmazó hálózatok elég messze vannak egymástól, akkor nagy biztonsággal állíthatjuk, hogy a tranzithálózati szolgáltatás használata optimális választás és ezekben a helyzetekben nem okoz gondot.
Ugyanakkor a helyi vagy földrajzilag közeli hálózatokba menő forgalomnak a gerinchálózatra való felvitele ronthatja a teljesítményt, néha azért, mert a gerinchálózati szolgáltató egy távoli földrajzi helyen található hálózaton keresztül küld adatokat. Amellett, hogy ez a gerinchálózaton felesleges terhelést okoz, az összeköttetés késleltetését is feleslegesen megnöveli.
Az IXP-rendszerre való 1992-es átállás óta az IXP-eken kicserélt internetes forgalom mérése volt az elsődleges adatforrás az internetes sávszélesség használatáról: hogyan növekszik az idő múlásával és hol keletkezik.

3.1.4 BGP, az Internet gerincprotokollja

Az IPX-ben a hálózatok a BGP (Border Gateway Protocol) segítségével kommunikálnak egymással. Ez a protokoll lehetővé teszi, hogy az IPX-ben összeérő hálózatok világosan elkülönítsék a hálózaton belüli menedzselési szempontokat és a hálózatok közötti kapcsolatok szabályozását. Az IXP-kben az összes peering viszony BGP-t használva jön létre.
Az IXP-ben résztvevő hálózatok közötti internetes forgalom cseréjét a köztük lévő Border Gateway Protocol (BGP) útválasztási konfigurációk segítik elő. A hálózatok a társviszonyokon (peering relationships) keresztül hirdetnek meg útvonalakat, amelyek vagy a saját címeikre mutatnak vagy más internetszolgáltatók címeire, olyan internetszolgáltatókéra, amelyekhez a hirdető hálózat kapcsolódik. A társviszonyban részt vevő másik fél ezután útvonalszűrést alkalmazhat: elfogadhatja ezeket az útvonalakat és ennek megfelelően irányítja a forgalmat, vagy figyelmen kívül hagyja ezeket az útvonalakat és más útvonalakat használhat a címek eléréséhez.
Sok esetben egy internetszolgáltató közvetlenül kapcsolódik egy másik internetszolgáltatóhoz és elfogadja egy útvonal hirdetését a másik internetszolgáltatóhoz az IXP-en keresztül is, utóbbit általában kihasználatlanul hagyva. Ha a közvetlen kapcsolat meghibásodik, a forgalom az IXP-en keresztül áramlik tovább. Ily módon az IXP tartalék hivatkozásként működik.

3.1.5 Hol vannak az IXP-ek?

Az IXP-ekre ott számítunk, ahol különböző szolgáltatói hálózatok találkoznak. Ahol a forgalom nagy, ott a kapacitásuk várhatóan nagyobb vagy éppenséggel több van belőlük. A pontos elhelyezkedésüket követhetjük egy térképen[2] vagy lekérhetjük adatbázisból[3].
Szervezetileg az IXP-ket többnyire független non-profit társaságok üzemeltetik, amelyeket az összekapcsolt ISP-k összessége vagy egy része finanszíroz, ugyanakkor lehetséges, hogy egy IXP-t egy szolgáltatósemleges, profitorientált gazdasági társaság tart fenn, de lehet a fenntartó egy egyetem vagy kormányzati szerv is, illetve létezik olyan modell is, ahol nincs fenntartó szervezet, a résztvevő hálózatok informális megállapodása működteti az IXP-et.

3.2 Internet továbbítási szolgáltatás (IP transit)

Az Internet továbbítási szolgáltatás[4] egy olyan szolgáltatás, amelyben az internetszolgáltató (ISP) lehetővé teszi a forgalom áthaladását a hálózatán, hogy a forgalom elérje az internet többi részét – vagyis a forgalom egy olyan hálózatban kerül továbbításra, amelyik sem a forgalomforrást, sem a nyelőt nem tartalmazza. Általában arra használatos, hogy egy kisebb internetszolgáltató (ISP) számára a teljes világhálóhoz való hozzáférést biztosítsuk, amint ezt a 10. ábra[5] is illusztrálja.

10. ábra Kapcsolódás az Internethez IP tranziton keresztül

Technikailag két összekapcsolódó szolgáltatásból áll:

- Az ISP a saját útvonalait hirdeti más internetszolgáltatók felé, ezáltal bejövő forgalmat kérve tőlük a saját hálózata felé,
- Harmadik fél internetszolgáltatók útvonalainak hirdetése (általában, de nem feltétlenül alapértelmezett útvonal vagy útvonalak teljes készlete formájában az interneten található összes célállomásra) az internetszolgáltatóhoz más internetszolgáltatóknak, ezáltal a saját hálózata felől kimenő forgalmat irányítva e hálózatok felé.

Az IP tranzit szolgáltatás az AS-ek (Autonomous System) számára érhető el és az útvonalak adatainak terjesztése a BGP-vel történik. Az IP tranzit ügyfélnek fizetnie kell az IP tranzit szolgáltatónak azért, hogy hozzáférjen a szolgáltató kiterjedt BGP Internet routing táblájához.

---

[2] https://www.internetexchangemap.com/
[3] https://www.peeringdb.com/
[4] Például: https://drpeering.net/core/ch2-Transit.html, https://fiberguide.net/ip-transit/, https://zet.net/ip-transit.php, https://www.iptp.net/en_US/what-is-ip-transit/
[5] Az ábrák forrása az „Internet továbbítási szolgáltatás” című fejezetben: https://www.iptp.net/en_US/what-is-ip-transit/

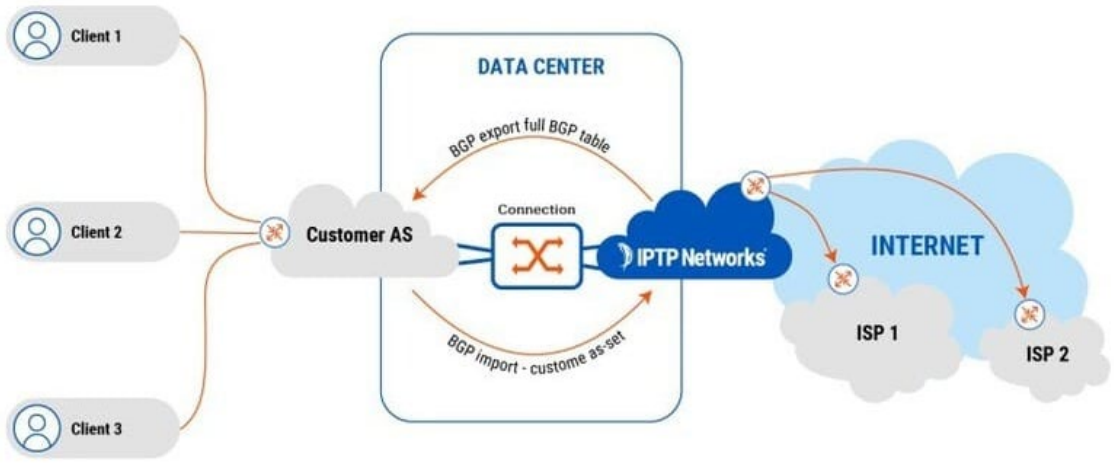
Az 1970-es évek végének és az 1980-as évek elejének Internetjéről még azt feltételezték, hogy minden hálózat teljes tranzitszolgáltatást biztosít az összes többi hálózat számára. A modern magánszektorbeli internetben az összekapcsolási megállapodások két formája létezik az internetes hálózatok között: a tranzit és a peering. A tranzit eltér a társviszonytól, amely utóbbiban csak a két internetszolgáltató és az általuk tranzitszolgáltatással kiszolgált hálózatok közötti forgalom cserélődik és egyik internetszolgáltató sem láthatja a felfelé irányuló útvonalakat a társviszony kapcsolaton keresztül. Egy tranzitmentes hálózat csak társviszonyt használ, ezen belül az a hálózat, amely csak térítésmentes társviszonyt használ és a teljes internethez kapcsolódik, Tier 1 hálózatnak minősül.
Az 1990-es években az Internet adatkicserélő központ ok koncepciója biztosította a tranzit egyik formáját.

3.2.1 Autonóm rendszer (Autonomous system - AS) / Autonóm rendszer sorszám (ASN – AS number)

Az autonóm rendszer (AS) egy olyan hálózatot jelent, amelynek csomópontjai azonos adminisztratív irányítás alatt állnak, menedzselésük ugyanazon szabályok szerint történik. Ez legtöbbször egy internetszolgáltatót vagy egy nagy szervezetet jelent, amely független kapcsolatokkal rendelkezik más hálózatokhoz. Minden AS-nek egyedi regisztrált autonóm rendszerszáma (ASN) van, amely azonosítóként kommunikál a többi AS-sel.
Csak azok jogosultak IP tranzit szolgáltatásra, akik saját AS-t üzemeltetnek, vagy más szóval, hozzárendelt ASN-sel rendelkeznek.

3.2.2 Border Gateway Protocol (BGP)

Az IP tranzit szolgáltatás a BGP-n alapul (11. ábra). A BGP-t az AS-ek arra használják, hogy interakcióba lépjenek egymással, és lehetővé tegye az IP-továbbítást az elérhetőségi információkon keresztül.



11. ábra A Border Gateway Protocol működése

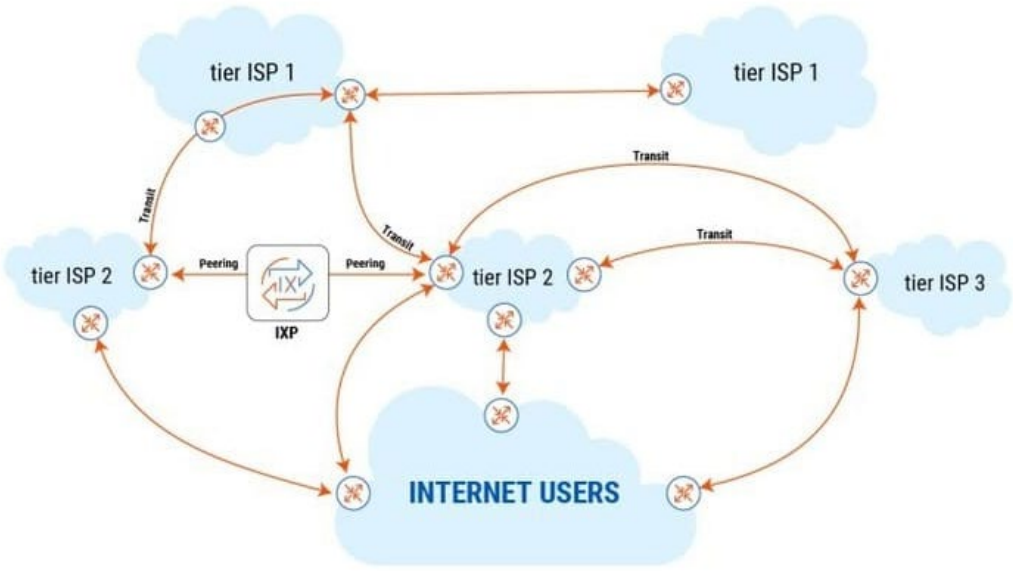
Az AS-ek BGP-t használva hirdetik meg (announce) az elérhetőségi információkat, beleértve a két listát a küldő AS és a fogadó AS által vezérelt IP-címekkel. A BGP meghatározza a legoptimálisabb útvonalat az adatcsomag továbbítására.

3.2.3 Az IP tranzit szolgáltatók besorolása

Az internetszolgáltatókat (ISP) szokás három szintre besorolni a képességeik és a lehetőségeik alapján (12. ábra):

- Az 1. szintű internetszolgáltatók (Tier 1 ISPs) jelentik az internet gerincét, globális kiterjedtségük van és az infokommunikáció meghatározó szereplői. Nem fizetnek a tranzitért és a társviszony (peering) is ingyenes számukra. Az 1-es szintű hálózatok összekötik az alacsonyabb szintű (Tier 2 és Tier 3) internetszolgáltatókat, és az alacsonyabb szintű internetszolgáltatóktól tranzitdíjat számítanak fel hálózataik használatáért.
- A 2. szintű internetszolgáltatók (Tier 2 ISPs) kiterjedt regionális vagy nemzeti szintű hálózattal rendelkeznek. Csak néhány Tier 2 internetszolgáltató képes kiszolgálni a fogyasztókat több kontinensen. A Tier-2 szolgáltatók más Tier-2-vel együttműködnek, hogy minimalizálják az IP forgalom továbbításának költségeit, de továbbra is meg kell vásárolniuk az IP tranzitot az 1. szintű internetszolgáltatóktól, hogy elérjék az internet többi részét.
- A 3. szintű internetszolgáltatók (Tier 3 ISPs) regionális szolgáltatók, amelyek hálózata néhány országot vagy régiót fed le. A 3. szintű internetszolgáltatók csak vásárolják az internetes forgalomtovábbítást – nincs társviszony. A Tier 1 IP tranzit magas költségeinek elkerülése érdekében gyakran vásárolnak IP tranzit szolgáltatást a Tier 2 szolgáltatóktól. A 3. szintű internetszolgáltatók általában nem rendelkeznek tranzit ügyfelekkel és általában a helyi vállalati és fogyasztói piacokkal foglalkoznak.

Az internetszolgáltatók hierarchiája a magasabb szinttel rendelkezőket Upstream, az alacsonyabb szinttel rendelkezőket pedig Downstream kategóriába sorolja. Például amikor a forgalom egy Tier 3 ISP-ről egy Tier 2 ISP-re áramlik, az felfelé halad. Ebben az esetben az alacsonyabb szintű (vagyis a Tier 3) ISP egy downstream szolgáltató, aki IP tranzit szolgáltatást vásárol a Tier 2 ISP-től – egy upstream szolgáltatótól. A hasonló szintű internetszolgáltatók, például két Tier 1 ISP, egyenrangú partnerek.



12. ábra Az Internet globális képe az IP tranzittal és a társviszonnyal

3.2.4 Hogyan működik az IP tranzit

Az IP tranzit összeköti az ügyfél hálózatát az internettel és egyértelmű útvonalat biztosít a forgalom számára, hogy megérkezzen a rendeltetési helyére. Az ügyfél tranzitdíjat fizet, hogy csatlakozzon egy szolgáltatási ponthoz, amelyet általában POP-nak (Point of Presence) neveznek. A szolgáltató ezután gondoskodik arról, hogy az ügyfél hozzáférjen az internet bármely szerveréhez, valamint az összes internetes szerver hozzáférjen az ügyfél szerveréhez.

Az internetes tranzit árai különböző időpontokban és földrajzi helyeken változnak. A tranzitszolgáltatás ára jellemzően megabit/másodperc/hónap egységben számolódik és az ügyfeleknek gyakran el kell kötelezniük magukat egy minimális sávszélesség mellett és általában minimális szolgáltatási időtartamra is. Az SLA[6] (Service Level Agreement) általában az IP tranzit szolgáltatás részét képezi. Az SLA meghatározza a szolgáltatás minőségét és a visszatérítési feltételeket arra az esetre, ha az ügyfél huzamosabb ideig nem tud hozzáférni az internethez vagy a szolgáltatás minősége nem megfelelő.

A hálózat méretétől és szintjétől függően a szolgáltatónak fizetnie kell egy vagy több hálózatért, hogy az ügyfél[7] forgalmát a kívánt célállomásra irányítsa az upstream tranzitján keresztül.

3.2.5 IP tranzit vagy IX tranzit vagy MPLS vagy DIA – Mit válasszunk?

Az IP tranziton kívül három másik csatlakozási szolgáltatás is biztosít internet hozzáférést: IX tranzit (Peering IXP-en keresztül), MPLS és DIA (Direct Internet Access).

Az IX tranzit egyfajta nyilvános társviszony-szolgáltatás az Internet Exchange Pointon (IXP) keresztül. Az IXP olyan csatlakozási pontként szolgál, ahol az internetszolgáltatók hálózatai csatlakozhatnak és internetes forgalmat cserélhetnek. Az IX tranzit eképpen egy részleges IP tranzit, amely lehetővé teszi, hogy a forgalom a társult internetszolgáltatók és az általuk kiszolgált downstream internetszolgáltatók hálózatai között kicserélődjön. Ez a teljes IP tranzithoz képest költséghatékonyabb megoldás és a késleltetés szempontjából is optimális.

Az MPLS (Multi-Protocol Label Switching) egy dedikált Layer 2 csatlakozási szolgáltatás. Az L2 MPLS privát utakat biztosít a globálisan szétszórtan elhelyezkedő hálózati szegmensek hatékony összekapcsolásához, szolgáltatásminőség biztosításával, szolgáltatási osztályok használatával, nagy sebességgel és biztonsággal. Emiatt természetesen drágább is, mint az IP tranzit.

A DIA (Direct Internet Access) ugyanúgy működik, mint az IP tranzit. A DIA a leggyakoribb internetes szolgáltatás azok számára, akik nem rendelkeznek ASN-nel. A DIA az IP tranzittal összehasonlítva sokkal olcsóbb választás, ugyanakkor a szolgáltatáskiesés várható időbeli hossza és a DIA minősége sok kívánnivalót hagy maga után.

A költségkeret, a partnerek száma, valamint a késleltetéstől való függés mértéke néhány olyan tényező, amelyet figyelembe kell venni az IP tranzit, IX tranzit, L2 MPLS vagy DIA választása során.

Aki nem rendelkezik saját ASN-nel és csak egyszerű és olcsó internetes szolgáltatást keres általános célokra, annak a DIA az ideális választás.

---

[6] Egy ilyen SLA-ra példa (https://zet.net/ip-transit.php): Network availability: 100%, Packet loss: < 0.1%, Inside Europe Latency: < 37ms, Transatlantic Latency: < 90ms, Ticket Response time: < 30 min

[7] Ne felejtsük el, hogy itt az szolgáltató (provider) és az ügyfél (customer) egyaránt hálózatüzemeltetők, vagyis nem természetes személyek. A SLA az adott hálózaton belüli kiszolgálásra vonatkozik.

Az IX tranzit azoknak felel meg, akik késleltetésre érzékeny alkalmazásokat használnak, szívesebben foglalkoznak a forgalomirányítással és a hálózatoptimalizálással és a költségvetésük korlátozott.
Az L2 MPLS több irodával rendelkező nagyvállalatok számára ajánlott, akiknek privát, dedikált és biztonságos hálózatra van szükségük.

3.3 Internet hozzáférés szolgáltatás (IAS)

Az Internet hozzáférés szolgáltatás definíciója[8] többféle is lehet, a forgalom volumenének, a forgalom továbbítására vonatkozó időbeli követelményeknek és főként a forgalmat generáló alkalmazásoknak a folyamatos változása újabb és újabb értelmezéseknek enged teret. Eszerint az internet-hozzáférési szolgáltatás ...

- „… kifejezés olyan szolgáltatást jelent, amely lehetővé teszi a felhasználók számára, hogy hozzáférjenek tartalmakhoz, információkhoz, elektronikus levelekhez vagy más, az interneten keresztül kínált szolgáltatásokhoz, és amely magában foglalhatja a védett tartalmakhoz, információkhoz és egyéb szolgáltatásokhoz való hozzáférést is. a fogyasztóknak kínált szolgáltatáscsomag részeként. Ez a kifejezés nem foglalja magában a távközlési szolgáltatásokat.” [47 USC § 231(e)(4)]
- „... mindig és szükségszerűen egyesíti a számítógépes feldolgozást, az információszolgáltatást és a számítógépes interaktivitást az adatátvitellel, lehetővé téve a végfelhasználók számára, hogy különféle alkalmazásokat (például e-mailt) futtassanak, és hozzáférjenek weboldalakhoz és hírcsoportokhoz.” [In the Matters of Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities, 20 FCC Rcd. 14853, 14860 (2005).]
- „… nyilvánosan elérhető elektronikus hírközlési szolgáltatás, amely internetcsatlakozást és ezáltal az internet lényegében valamennyi végpontjával összekapcsolási lehetőséget biztosít, tekintet nélkül az alkalmazott hálózati technológiára és a használt végberendezésre.” [Az Európai Parlament és a Tanács (EU) 2015/2120 rendelete (2015. november 25.) a nyílt internet-hozzáférés megteremtéséhez szükséges intézkedések meghozataláról, továbbá az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv és az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming) szóló 531/2012/EU rendelet módosításáról]

Amikor az Internet architektúrája egyik részeként kezeljük, akkor az internet hozzáférés egyének és szervezetek azon képessége, hogy infokommunikációs eszközök – amelyek közé itt most a számítógépes terminálokat, kisebb vagy nagyobb számítógépeket, személyi kommunikációs eszközöket (például telefon, tablet, okosóra), médiamegjelenítő eszközöket, háztartási vagy ipari, esetleg katonai jellegű „okoseszközöket” és még sok más egyéb eszközt is beleértünk – segítségével csatlakozzanak az Internethez, elérjék annak tartalmait és igénybe vegyék a szolgáltatásait. Tehát az internet hozzáférés szolgáltatás egy, a hálózat szélén lévő eszközt kapcsol be a hálózatba, amelyik általánosan véve a mögötte lévő személy vagy közösség számára a hálózat szolgáltatásait nyújtja.

[8] https://itlaw.fandom.com/wiki/Internet_access_service,

Az internet hozzáférést internetszolgáltatók (ISP-k) értékesítik, amelyek különféle hálózati technológiákon keresztül az adatátviteli sebességek széles skáláján biztosítanak kapcsolatot. Számos szervezet, köztük egyre több önkormányzat is ingyenes – és ezzel együtt többnyire korlátozott felhasználhatóságú – vezeték nélküli hozzáférést biztosít.
Az internet hozzáférés elérhetősége a XX. század utolsó évtizedének első felében még erősen korlátozott volt, de később folyamatosan és gyorsan nőtt. Ma már nemcsak a fogyasztók személyes igénye, hanem a hálózatba kötött eszközök használata által remélt előny is a lefedettség és a teljesítmény növelésének hajtómotorja. Az internet hozzáférés szolgáltatással kapcsolatban beszélhetünk a lefedettségről, vagyis a szolgáltatás elérhetőségről, az alkalmazott technológiákról és a szolgáltatás teljesítményéről vagy minőségéről (QoS). Ezek a szempontok nem kezelhetőek tisztán, hiszen nem minden földrajzi helyen alkalmazható a hálózat építésére az összes technológia, amelyek aztán befolyással bírnak az elérhető szolgáltatásminőségre is. Néha a technológiák közötti döntésnek nem csak technikai, hanem anyagi szempontjai[9] is vannak, akár az ISP, akár az ügyfelek oldaláról.

3.3.1 Elérhetőség

A helyhez kötött internet hozzáférési szolgáltatás hazánkban gyakorlatilag minden olyan helyen rendelkezésre áll, ahol ennek telepítése technológiai és anyagi szempontból lehetséges. Ezek a hozzáférési helyek többnyire otthoni, iskolai és munkahelyi környezetben találhatóak, de nyilvános helyeken – például könyvtárak – is előfordulhatnak olyan hálózati hozzáféréssel rendelkező számítógépek.
A vezeték nélküli hozzáférési pontok esetén a felhasználónak kell biztosítani a hozzáférést használni képes eszközt, a hozzáférési pont „gazdája” csak a többé-kevésbé védett hálózati csatlakozási lehetőséget nyújtja. Ennek igénybevételéhez a WiFi technológiát használni képes eszközre van szükség, a hozzáférési információ (pl.: SSID, jelszó) a potenciális felhasználói körnek átadják. Tipikus példaként hozhatók erre a közösségi terek: egyetemi aulák, városok meghatározott közterületei, strandok, bevásárlóközpontok, szálláshelyek, stb. Látható a példákból, hogy ezek a hozzáférési lehetőségek korlátozott földrajzi környezetben állnak rendelkezésre, tulajdonképpen az előbb említett helyhez kötött elérések kisebb kiterjesztései, amelyek csak kisebb mobilitást tesznek lehetővé (például a város főterén elérhető a hozzáférés, két utcával odébb már nem). Fontos megjegyezni, hogy ezek mellett a publikus, a köz számára elérhető hálózatok mellett ugyanazon a földrajzi területen a hozzáférési pont gazdája sokszor alakít ki párhuzamos hálózatokat, amelyeknek elérhetősége viszont jelentősen korlátozott és a felhasználói köre többnyire az adott helyen munkavégzési céllal tartózkodók köréből kerül ki (pl. a szálláshely vagy az orvosi váró vagy a sportlétesítmény saját, alkalmazotti hálózata).
A mobil hálózati technológiák már régebb óta lehetővé tették az Internethez való kapcsolódást, de ennek széleskörű ismertsége, majd robbanásszerű elterjedése az érintőképernyős „okostelefonok” megjelenésével vált általánossá. 2022-ben a Föld lakosságának többsége – csaknem 5 milliárd ember – használt mobil internet hozzáférést és az azokon keletkezett forgalom az Internet teljes forgalmának 60%-át közelítette[10].

[9] Rövid, lényegre törő és könnyen áttekinthető összefoglaló olvasható: https://www.electronicshub.org/internet-speed-comparison-chart/.
[10] https://www.statista.com/topics/779/mobile-internet/

A műholdas internet hozzáférés lehetősége szintén elég régen ismert már, de tulajdonképpen csak a jelen évtizedben vált globálisan ismerté és a népszerű a Starlink[11] szolgáltatása, amely elsősorban más technológiával nehezen elérhető helyeken nyújtott megfizethető és a szokásos felhasználói igényeket figyelembe véve megfelelő teljesítményű internet hozzáférési szolgáltatást. A Starlink mellett a HughesNet és a Viasat említhető, mint számottevő piaci szereplők[12], azonban az utóbbi két szolgáltatás elérhetősége leginkább Észak-Amerikára korlátozódik. Figyelembe véve, hogy a Föld felszínének túlnyomó részét tenger borítja, ami helyhez kötött vagy mobil internet szolgáltatással nem fedhető le, így nyilvánvaló, hogy potenciálisan a műholdas internet hozzáférés szolgáltatás lefedettsége a legmagasabb, megfelelő üzemeltetői szándék esetén a Föld – és bármely más, erre alkalmas bolygó vagy égitest – felszínének 100%-át közelítheti. Ezután nyilván a különböző generációjú mobil internet szolgáltatások következnek, hiszen ezek – a core hálózat kialakítása után – elég költséghatékonyan telepíthetőek.

3.3.2 Technológiák

Az internet hozzáférés szolgáltatás többféle technológián keresztül nyújtható. A legfontosabb felosztás a helyhez kötött és a mobil technológiák csoportjai. A kezdeti analóg modemes és bérelt vonalas megoldások mára gyakorlatilag teljes mértékben kiszorultak a modern piacokról és jellemző trend, hogy akár néhány év alatt is kiszorulhatnak technológiák és a jelentős mértékben növekvő teljesítményigények újabb hozzáférési lehetőségek elterjedését segítik. Magyar viszonylatban korábban meglehetősen pontos képet lehetett nyerni a Nemzeti Média és Hírközlési Hatóság gyorsjelentéseiből[13], azonban mostanában[14] ezekben a helyhez kötött hozzáférésekre vonatkozóan már nem található meg a technológia szerinti bontás. Ugyanakkor a sebességkategóriák által képviselt arányok azért utalnak arra, hogy az alacsonyabb sebességet lehetővé tevő megoldások – elsősorban az xDSL – egyre kevésbé elterjedtek. Helyettük az Európai Unió Next Generation Network kritériumának teljes mértékben eleget tevő kábelmodemes és optikai hozzáférési technológiák piaci súlya emelkedik folyamatosan, 2022. augusztusában meghaladva a 80%-ot. Ezen belül a kábelmodemes összeköttetések száma nagyjából stagnálni látszik, a növekedés az FTTx technológiájú összeköttetések számának bővüléséből fakad. Időközben az Európai Parlament és a Tanács további fejlődési pályát jelölt ki[15], amely szerint a helyhez kötött szolgáltatások tekintetében a gigabites hálózati hozzáférés biztosítását preferálja az évtized végére.
A mobil technológiák tekintetében egyszerűbb a helyzet, mivel a nagysebességű 4G/5G mobilinternet hozzáférések aránya nagyjából a 2018Q1-re jellemző 75%-ról 2022Q4-re 96%-ra növekedett a személyi kommunikáció szegmensében. Ebben nyilván a 3G szolgáltatás jó előre bejelentett lekapcsolása is szerepet játszik, mint ahogy a mobilkészülék gyártók közötti

[11] https://www.starlink.com/
[12] https://www.satelliteinternet.com/, https://www.zdnet.com/home-and-office/networking/best-satellite-internet/, https://www.cnet.com/home/internet/best-satellite-internet/
[13] https://nmhh.hu/dokumentum/230162/mobilpiacijelentes2018q12021q4.pdf, https://nmhh.hu/dokumentum/223230/vezetekes_gyorsjelentes_2021_julius.pdf
[14] https://nmhh.hu/dokumentum/238785/NMHH_mobilpiaci_jelentes_2022_masodik_felev.pdf, https://nmhh.hu/dokumentum/238859/helyhez_kotott_piaci_jelentes_2019_elso_2022_negyedik_negyedev.pdf,
[15] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata (2022. december 14.) a Digitális évtized 2030 szakpolitikai program létrehozásáról, OJ L 323

technológiai verseny is. Azt látnunk kell még, hogy 2022-ben csak a magyar háztartások 17,6%-a[16] rendelkezett 5G-s mobilinternet lefedettséggel.
A mobilinternet hozzáférési szolgáltatás érdekes szegmense az M2M kommunikáció. 2022 végére a magyarországi mobilszolgáltatóknál az aktívan forgalmazó M2M SIM-ek száma meghaladta az 1,36 milliót, amelyek adatforgalma összesen 909 TB 2022Q4-ben. Összehasonlítva az okostelefonos, mobilinternet forgalmat bonyolító 7,7 millió SIM-re átlagosan egyenként 11 GB jutott havonta, ami 2022Q4-ben 254100 TB, vagyis a nagyjából 280-szorosa az M2M forgalomnak. Fontos megjegyezni, hogy ezek az aktív M2M SIM-ek – a több mint feleannyi passzívval együtt – szinte mindegyike post paid modellben és nem lakossági felhasználással működik.

3.3.3 Teljesítmény

A helyhez kötött vezetékes internet hozzáférés szolgáltatás teljesítménye újonnan telepített előfizető esetén – leginkább a magyarországi és az európai lakossági előfizetők helyzetét figyelembe véve – tulajdonképpen bőségesen elegendő az átlagos háztartás számára, tekintettel arra, hogy a legkisebb előfizetői csomagok is 100 Mbps nagyságrendű letöltési sebességűek. A feltöltési irányban elérhető sebesség ugyan jellemzően kisebb, de a felhasználói szokásokkal ez egyezik, hiszen az NMHH által a 2019Q1-2022Q4 időszakra kiadott, korábban már idézett mobil gyorsjelentése szerint a letöltési irányú és a feltöltési irányú forgalom közötti arány a vizsgált időszakban stabilan 9:1.
A megjelenő Gbps nagyságrendű és egyre inkább azt meghaladó letöltési sebességgel rendelkező lakossági internet előfizetési díjcsomagokra vonatkozóan azt tudjuk mondani, hogy sokszor egy kapcsolódó eszközzel nem is tudjuk szaturálni a rendelkezésre álló sávszélességet.
A helyhez kötött rádiós internet hozzáférési szolgáltatás esetén a teljesítmény időbeli ingadozása sokkal nagyobb lehet és nemcsak a hálózati forgalom fluktuációja, az ennek következtében fellépő ideiglenes túlterhelés befolyásolja a szolgáltatás minőségét, hanem a rádiós szakaszra hatnak egyéb környezeti tényezők is, például az időjárás, az átviendő szakaszon a talaj fedettsége növényzettel vagy csapadékkal, naptevékenység, stb. Emiatt ilyen hozzáférési hálózati technológia esetén kevesebb minőségi garanciát várhatunk el.
Késleltetés tekintetében a vezetékes esetben akár az FTTx, akár a DOCSIS technológiákat használjuk, a mért terheletlen késleltetés többnyire nagyon alacsony lesz. Ugyanakkor az ISP-k saját útvonalirányításától függően lehetséges, hogy a terhelt hálózaton, akár a szolgáltatások egy része, akár összessége esetén a kétirányú késleltetés észrevehető mértékben meghaladja a felhasználó számára kényelmes értéket. Ezt a problémát az ISP képes orvosolni, ha nem is mindig hajlandó rá.
Ha a hozzáférési hálózatban rádiós szakasz is van, akkor az a késleltetést észrevehető módon megnövelheti.
A mobilinternet esetén a 4G-s hálózat 100 Mbps, az 5G-s hálózat 1 Gbps-os sebességgel kecsegteti a felhasználókat. Természetesen a ténylegesen elért sebesség függ az adott cella felhasználóinak számától is. A késleltetés tekintetében a modern vezetékes összeköttetésekkel összemérhető értékkel igazán csak a teljesen kiépített tiszta 5G-s hálózatokon számolhatunk majd.

[16] https://digital-agenda-data.eu/charts/desi-components#chart={%22indicator%22:%22desi_5gc%22,%22breakdown-group%22:%22total%22,%22unit-measure%22:%22pc_hh_all%22,%22time-period%22:%222022%22}

A műholdas internet hozzáférés esetén a hozzáférési sebesség nem túl magas, jellemzően 100 Mbps alatti, bár a Starlink egyik csomagjában magasabb letöltési sebesség is elérhető. Az RTT értéke a Starlink saját állítása szerint nagyjából 25 ms, ami az FTTx-es hálózatokhoz képest nem kevés.

3.3.4 Rendelkezésre állás

Az internet hozzáférés szolgáltatás rendelkezésre állását több tényező befolyásolja, ráadásul ezek némileg eltérhetnek az alkalmazott technológia függvényében. A szolgáltatás működéséhez mindenképpen szükséges megoldani a hálózati berendezések és a felhasználói készülék elektromos tápellátását. Ez természetesen lehet akkumulátoros is. A vezetékes hálózatok esetén az előfizetői hurok fizikai épsége esetén a rendelkezésre állást csak a szolgáltató gerinchálózatának működőképessége befolyásolja, ugyanakkor működéskiesés az ISP hatókörén kívül eső ok miatt is bekövetkezhet, például a DNS szolgáltatás általános hibája miatt, esetleg a tranzit vagy a peering szolgáltató hibája miatt. Természetesen az ügyfelet közvetlenül kiszolgáló ISP is lehet felelős a szolgáltatás elérhetetlensége miatt, például egy meghibásodott útválasztó vagy hálózati torlódás esetén.
A helyhez kötött, de rádiós szakaszt is tartalmazó internet hozzáférés szolgáltatás esetén, valamint mobil internet hozzáférés és műholdas internet hozzáférés esetén ehhez még hozzájönnek a rádiós szakasz okozta problémák, valamint a megosztott hozzáférési közeg miatt előforduló problémák. Ez utóbbiak azt jelentik, hogy a rádiós szakasz teljesítménye ugyanúgy korlátozott, mint a vezetékes hozzáféréseké, csak éppenséggel a versengő felhasználók száma jellemzően nagyobb, extrém esetben akkora, hogy az egy felhasználóra jutó sávszélesség nem elegendő semmilyen felhasználónak nyújtott szolgáltatás igénybevételére sem.

3.4 Vezeték nélküli hozzáférési pontok (WiFi HotSpot)

A vezeték nélküli hozzáférési pont (hotspot) egy olyan fizikai hely, ahol a felhasználók vezeték nélküli lokális hálózaton keresztül internet hozzáférési szolgáltatást vehetnek igénybe jellemzően Wi-Fi technológia[17] használatával. Tekinthetjük tulajdonképpen az fentiekben taglalt internet hozzáférési szolgáltatás egy megvalósítási lehetőségének. Ami a többi lehetséges megvalósítás közül kiemeli, az a nagyfokú rugalmassága és a viszonylag egyszerű és gyors telepíthetősége.
A vezeték nélküli hozzáférési pontokon keresztül nyújtott internet hozzáférés szolgáltatás elérhetősége lehet ideiglenes (például egy konferencia esetén) vagy tartós (egy egyetemi campus területén), lehet korlátozott (például egy szállodában) vagy nem korlátozott használatú, lehet nyilvános vagy magáncélú, lehet nyílt vagy jelszóval védett és még több más lehetséges felosztás is létezik.
Technikai szempontból a vezeték nélküli internet hozzáférés létrehozásához elegendő egy, valamiképpen internet hozzáféréssel rendelkező hozzáférési pont (access point, AP), amely útvonalválasztóként is képes működni. Az további kérdés lehet, hogy az AP internet hozzáférését miként biztosítjuk. Ennek az egyik legkézenfekvőbb módja a vezetékes internetkapcsolat, egy másik a mobil internetkapcsolat. Mindkét esetben tulajdonképpen egy olyan internetkapcsolat megosztásáról van szó, amelynek előfizetője és az AP aktuális

[17] Itt érdemes megjegyezni, hogy az internet hozzáférés vezeték nélküli megosztására a Wi-Fi-n kívül más technológiákat is tudunk használni. A legelterjedtebb például a Bluetooth.

felhasználói köre között nincs okvetlenül korreláció. Egy harmadik lehetőség, amikor egyéb módon nehezen ellátható területen, akár néhány kilométeres körzetben irányított antennák segítségével internet hozzáférés szolgáltatás jelleggel működtetünk hotspotokat. Ebben az esetben az előfizető és az aktuális felhasználó jobbára ugyanaz a személy.

3.4.1 Biztonsági problémák

A biztonság a Wi-Fi technológián alapuló internet hozzáférés egyik sarkalatos kérdése. Egyrészt a rádiós interfész titkosítás nélkül lehetőséget ad a felhasználó személyes adatainak, jelszavainak megszerzésére. A felhasználó ez ellen közvetlenül nem sokat tehet, ha a hálózati forgalmat nem titkosítják, viszont a titkosításról természetesen nem a felhasználó, hanem a hotspot üzemeltetője dönt. Másrészt a hotspot üzemeltetője, vagy ha annak nem megfelelő a védelme, akkor bármely megfelelő képzettséggel rendelkező rosszindulatú támadó hozzáfér a hotspoton keresztülmenő forgalomhoz, a csomagok tartalmához és a metaadatokhoz. Végül természetesen kérdéses a hotspot internetelérésének védettsége is, tekintettel arra, hogy titkosított WLAN-forgalom esetén is a titkosítás a felhasználó és az AP közötti rádiós szakaszra érvényes.

A jelenleg minimálisan szükséges biztonsági eljárásrend a WPA2/AES kombináció magáncélú felhasználás esetén. Ahol az eszközök támogatják, érdemes használni a WPA3-at. A WPS használata ugyan kényelmesnek tűnik, de jelentős biztonsági kockázatok hordoz.

A hotspoton keresztüli internet elérésének legbiztonságosabb módja ismeretlen biztonsági intézkedések mellett a végpontok közötti titkosítás. A végpontok közötti erős titkosításra példa a HTTPS és az SSH. Még biztonságosabb, ha VPN-t használunk. Ugyanakkor a titkosított forgalom is nyílt közegen halad keresztül, tehát a rosszindulatú felhasználók a rádiócsatorna figyelésével hozzájutnak a felhasználó forgalmi mintázatához.

3.4.2 Jogi problémák

A nyilvános hotspot üzemeltetője tulajdonképpen tekinthető internet hozzáférés szolgáltatónak is, hiszen mások számára lehetőséget nyújt arra, hogy az eszközeikkel az internetre csatlakozzanak. Ugyanakkor ez az üzemeltető/szolgáltató jogi kötelezettségét is jelenti, hogy a forgalmat a jogszabályoknak megfelelően felügyelje és a szükséges intézkedéseket megtegye például az illegális vagy jogszabálysértő tevékenységek megakadályozására. Nyilvánvalóan ez nem olyan könnyű, mint a vezetékes hozzáférési pontok esetén, ugyanakkor a nem megfelelő forgalom blokkolására itt is van lehetőség.

3.4.3 További vezetéknélküli hozzáférési megoldások

A hálózati kapacitások növekedése és ezzel együtt az egységnyi hálózati erőforrás árának csökkenése, valamint az automatizáció növekvő foka és az ezzel összefüggésbe hozható igények robbanásszerű bővülése a dolgok internetéhez kapcsolódó megoldásokra is ráirányítja a figyelmet. A tipikusan M2M (machine-to-machine) célra alkalmazott kommunikáció forgalmi mintázata jellemző: átlagosan nagyon alacsony sebesség, a kommunikáció ütemezett jellege, az energiahatékonysági szempontok miatt az üzenet küldése/vétele kivételével készenléti üzemmód/alvás. A használt hozzáférési megoldások (LoRa, NB-IoT, LTE Cat-M1) sokszor a mobilszolgáltatók infrastruktúráját használják, de például az IEEE 802.11ah éppenséggel a Wi-Fi protokollcsalád része.

3.5 Virtuális magánhálózatok

A virtuális magánhálózat[18] (Virtual Private Network, VPN) eredeti értelmében egy olyan mechanizmus, amely lehetővé teszi, hogy egy közhasználatú kommunikációs médium, például a nyilvános internet segítségével egy számítástechnikai eszköz és egy számítógépes hálózat vagy két számítógépes hálózat között olyan kapcsolatot hozzunk létre, amely a magánhálózatokra jellemző. A VPN olyan módon terjeszthető ki a magánhálózatot, amely lehetővé teszi a hálózat felhasználói számára, hogy adatokat küldjenek és fogadjanak nyilvános hálózatokon keresztül, mintha a nyilvános hálózatok eszközei közvetlenül csatlakoznának a magánhálózathoz. Amíg korábban a VPN legfontosabb jellegzetességei a megbízhatóság és a konnektivitás biztosítása voltak, mostanra sokkal nagyobb hangsúly kerül a felhasználó személyes jogainak védelmére, az adat- és a szolgáltatásbiztonságra és a továbbított forgalom védelmére.

3.5.1 A VPN működése

A VPN virtuális pont-pont kapcsolat létrehozásával jön létre a meglévő hálózatokon keresztüli alagútkezelési protokollok használatával. A magáncélú és a vállalati/szervezeti felhasználású VPN-ek esetén manapság egyaránt jellemző a forgalom titkosítása. Ugyanakkor a vállalati/szervezeti célú VPN esetén lényeges a felhasználó hitelesítése, vagyis, hogy a kiterjesztett magánhálózatot csak a jogosult felhasználók érhessék el és némely esetben a felhasználók eszköze is hitelesített kell legyen, addig a magáncélú felhasználás esetén gyakran cél a felhasználók anonimizálása és akár a forráscím és a célcím elrejtése.

A VPN kapcsán gyakran használjuk az „alagút” szót (angolul pedig a „tunnel” vagy a „tunnelling” kifejezést), ami a vállalati/szervezeti felhasználás esetén jól le is írja valóságot. A magáncélú felhasználás esetén azonban inkább egymással összekötögetett alagutakból álló szövevényes hálózatról van szó, ahol a belépési pont után az érkező csomagban kicserélik a forráscímet is. Ennek következtében, ha VPN-en keresztül böngészünk az Interneten, akkor a VPN-kiszolgáló látszik kliensként a webszerver számára és természetesen ugyanígy látják a VPN kiszolgálótól a webszerverig útba eső ISP-k is. A kliens és a VPN-kiszolgáló közötti forgalom pedig titkosítva van és az ezen az útvonalon elhelyezkedő megfigyelő semmilyen információt nem szerezhet a felkeresni kívánt webcímről. Ez jelentős védelmet nyújt a felhasználók számára, ha nem dedikált internet hozzáféréssel rendelkeznek, hanem például Wi-Fi-n keresztül kapcsolódnak a világhálóra. Manapság a webböngészés vagy levelezés esetén a böngészők és a levelező kliensek amúgy is SSL/TLS-t használnak, a titkosítással nem rendelkező honlapok aránya egyre kisebb, a mai modern böngészők legtöbb esetben csak a felhasználó kifejezett kívánságára, többszöri megerősítést kérve hajlandóak az ilyen oldalakat megnyitni. A VPN működése azonban erre nincs tekintettel, a tartalmat és immár akár a csomag fejlécét is titkosítja, ráadásul ez nemcsak a böngészésre és a levelezésre, hanem az adott csatolón (interface-en) keresztülmenő összes forgalomra vonatkozik.

Megjegyzendő, hogy egyes böngészők, mint például a Tor (https://www.torproject.org/) önmagában is célul tűzte ki a felhasználók anonimitásának biztosítását, így például a Tor egy proxy-hálózatot is működtet, amely ezt lehetővé teszi.

[18] Lásd például: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~how-a-vpn-works, https://www.proofpoint.com/us/threat-reference/vpn, https://nordvpn.com/what-is-a-vpn/, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn/#what-is-a-vpn, https://www.ibm.com/docs/en/i/7.5?topic=security-virtual-private-networking

Azt is fontos kiemelni, hogy amíg a világháló felett működő overlay szolgáltatja az anonimitást és egyébként növelheti a hálózat rendelkezésreállását, megbízhatóságát, csökkentheti a csomagvesztési arányt, ugyanakkor valószínűleg észrevehetően megnöveli a kiszolgálási késleltetést, akár a felhasználó számára kényelmetlen mértékben is. Nyilván ez a pont-pont jellegű VPN-ek esetén nem jellemző.
Harmadjára: látnunk kell, hogy az anonim és titkosított hálózati forgalom visszaélésekre és törvénytelen tevékenységre is lehetőséget nyújt, az ún. „dark web" is tulajdonképpen megfeleltethető a VPN definíciójának[19].

3.5.2 A VPN használatának előnyei

A VPN használatának legfontosabb technológiai előnyei között az alábbiakat szokták felemlíteni:

- Biztonságos titkosítás: A mai modern VPN-ek segítségével a felhasználó teljes internettel kapcsolatos tevékenysége még a nyilvános hálózaton is rejtve marad. A VPN-en továbbított adatok olvasásához titkosítási kulcsra van szükség, anélkül nagyon hosszú időre van szükség a kódolt adat visszafejtéséhez.
- Az online személyazonosság álcázása: A proxy-ként működő VPN-kiszolgálók a továbbítás közben az IP-csomagok forráscímét a sajátjaikra cserélik, így a forgalom, az igénybe vett szolgáltatás, az elfogyasztott tartalom közvetlenül nem hozható kapcsolatba az eredeti felhasználóval. Ez különösen fontos lehet azokban az országokban, ahol az internethasználat korlátozott és cenzúrázott. Ilyen helyeken a VPN-t használó internet felhasználók aránya kimondottan magas, akár 20% is lehet. Az ezen a téren liberálisabbnak tekintett országokban, például az USA-ban, Nagy-Britanniában és Németországban a VPN-felhasználók aránya 5% körül alakul, viszont növekszik.
- A felhasználó hollétének álcázása: A fentebb már leírt címcsere következtében a végső célban elhelyezkedő eszköz a szolgáltatás igénybevevőjének a VPN-kiszolgálót tekinti, így a tartalom vagy szolgáltatás igénybevételére vonatkozó földrajzi vagy szolgáltatói jellegű korlátozásokat eszerint érvényesíti. Az elmúlt időszakban a VPN alkalmazásának egyik legnagyobb hajtóereje éppen a földrajzi hozzáférési korlátozásokkal rendelkező tartalmak iránti növekvő kereslet volt. Például az olyan videostreaming szolgáltatások, mint a Netflix vagy a YouTube, bizonyos videókat csak bizonyos országokban tesznek elérhetővé. Hasonlóan az egyes sportesemények közvetítési jogainak értékesítése is országokra, földrajzi régiókra, illetve esetlegesen szolgáltatók szolgáltatási területeire érvényes. Az ilyen típusú korlátozások megkerülésére jól alkalmazhatóak a VPN-ek.

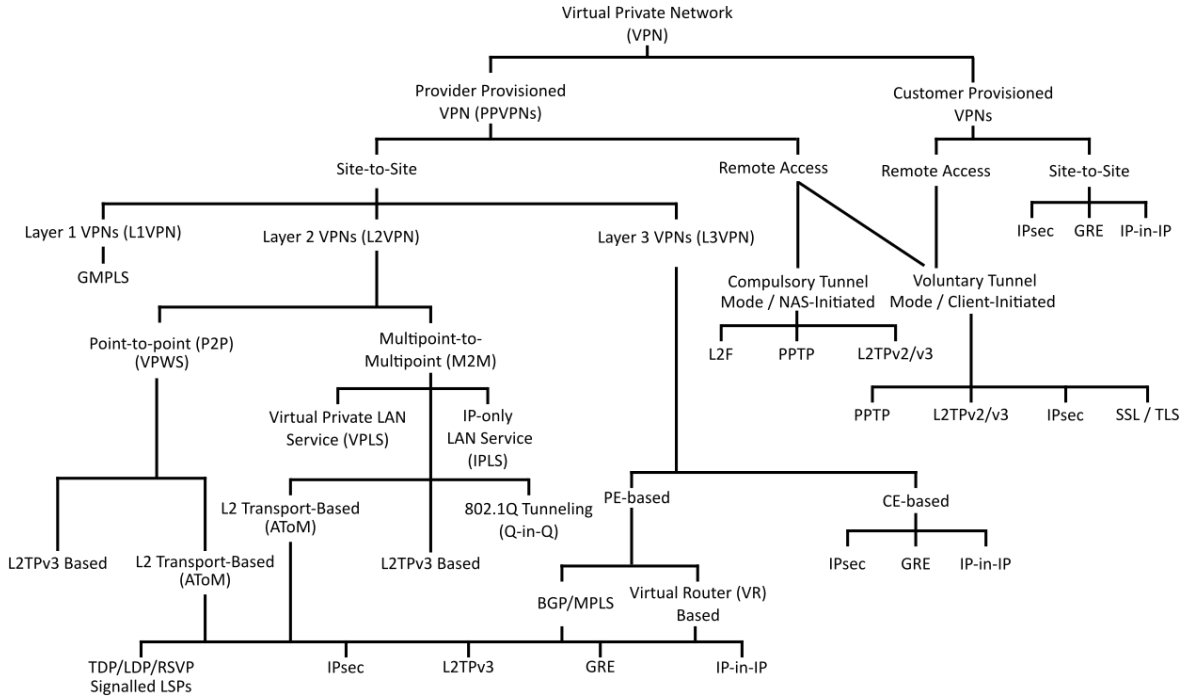
Mielőtt azt hihetnénk, hogy a VPN-ek ezen jellegzetessége szinte csakis illegális tevékenységek álcázására szolgál, gondoljuk át, hogy sok esetben ennek éppen az ellenkezője igaz: a felhasználó törvényesen jogosult az adott szolgáltatás igénybevételére vagy tartalom fogyasztására, azonban – például egy utazás során – előfordulhat, hogy az eszköze egy olyan hálózaton keresztül éri el az Internetet, amely a felhasználó jogainak és a lehetőségeinek csak egy részhalmazával rendelkezik. Ekkor a felhasználó természetes

[19] Megjegyzendő, hogy bizonyos esetekben ezt a viszonyt fordítva is értelmezik, a dark web részeként tekintenek az anonimizált forgalomra, például a Tor forgalmára.

elvárása, hogy ilyen körülmények között is az általa kifizetett szolgáltatást vagy tartalmat elérhesse.
A vállalkozások számára a fentebb bemutatott technológiai jellegű előnyök mellett nagyon fontos lehet még a nagy rugalmasság, vagyis, hogy a kapcsolat szinte bármilyen helyről biztonságosan létrehozható, illetve a költséghatékonyság, mivel a VPN használata jelentősen olcsóbb, mintha dedikált kommunikációs vonalakat alkalmaznánk a vállalkozás telephelyein lévő helyi hálózatok kiterjesztésére és egymással való összekötésére.

3.5.3 A VPN-ek típusai

A 13. ábra[20] a VPN-ek típusait igyekszik rendszerezni. Azt mindenképpen elmondhatjuk ennek alapján, hogy a VPN-ek különböző rétegbeli építőkövei meglehetősen szabadon kombinálhatóak. Ezeket a technológiákat (IPsec, PPTP, GMPLS, 802.1Q) még az 1990-es és a 2000-es években fejlesztették ki.



13. ábra A virtuális magánhálózatok típusai

Sok különböző típusú VPN létezik, de ezek 2-3 nagyobb osztályba sorolhatóak:

- Távoli hozzáférésű VPN (Remote Access VPN) – Ez egy ideiglenes kapcsolat a távolról dolgozó alkalmazott és a vállalati hálózat között. Ennek két lényegesen különböző megoldása[21] is létezik:
    - SSL VPN terminológia azt a helyzetet írja le, amikor a távolról dolgozó alkalmazott nem a vállalat által biztosított informatikai eszközt, hanem a sajátját használja[22]. Ebben az esetben a vállalatok egy SSL-VPN megoldást választanak, amelyet általában egy megfelelő hardverdobozon keresztül

[20] Forrás: Lewis, Mark (April 2006) Comparing, Designing, and Deploying VPNs, Cisco Press, p. 1043 ISBN: 1587051796, https://ptgmedia.pearsoncmg.com/images/1587051796/samplechapter/1587051796content.pdf
[21] https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn
[22] Ennek elfogadására sok vállalkozás rákényszerült a COVID-19-cel kapcsolatos lezárások és a kapcsolódó informatikai eszközhiány következtében.

valósítanak meg. Az előfeltétel általában egy HTML-5-képes böngésző, amely a cég bejelentkezési oldalának előhívására szolgál. A HTML-5 kompatibilis böngészők gyakorlatilag minden operációs rendszerhez elérhetőek. A hozzáférést felhasználónévvel és jelszóval védjük.

- Az ügyfél-szerver VPN (Client-to-Server VPN) viszont annak feleltethető meg, hogy az alkalmazott által használt számítógépet – ami ebben az esetben többnyire a vállalat tulajdona – képletesen egy hosszú kábellel közvetlenül a vállalati hálózatba kötjük. Az alkalmazottak a biztonságos kapcsolaton keresztül otthoni irodájukból csatlakozhatnak be a vállalati hálózatba és ugyanolyan lehetőségeik vannak, mintha az irodában ülnének. A VPN-kliens szoftvert azonban először telepíteni és konfigurálni kell a számítógépen, utána a számítógép minden egyes indulásakor automatikusan elindul a VPN kliens is és közvetlenül össze is kapcsolja a számítógépet a vállalati hálózattal. Innentől a számítógép teljes IP-szintű forgalma keresztülmegy a vállalati hálózaton. Az adatcsere nagyon hatékony és amennyiben például a vállalkozás IP-alapú távbeszélő szolgáltatást használ, akkor az alkalmazott által kezdeményezett VPN-en keresztül telefonálni is lehet, akár softphone alkalmazás, akár ténylegesen kézbe vehető telefonkészülék segítségével.

- Telephelyek közötti VPN (Site-to-site VPN) – Ez egy állandó kapcsolat, amely arra szolgál, hogy a vállalat fizikailag egymástól távol lévő telephelyei között titkosított összeköttetést nyújtson. Ezt tipikusan IPsec alkalmazásával érik el, csakúgy, mint az ügyfél-szerver VPN esetén is inkább azt használják[23]. A telephelyek közötti VPN-eket főként nagyvállalatok használják. A megvalósításuk bonyolult, és nem nyújtanak ugyanolyan rugalmasságot, mint például az SSL VPN-ek, azonban ezek jelentik a kommunikáció biztosításának leghatékonyabb módját a nagy szervezeti egységeken belül és ezek egységek között.
- Személyes VPN (Personal VPN) – A legtöbb fogyasztói szintű VPN személyes VPN-nek minősül, beleértve az legtöbb olyan céget, amelyek magánügyfelek számára nyújtanak VPN szolgáltatást. A technológia nagyon hasonló a távoli hozzáférésű VPN-ekhez, de ahelyett, hogy egy védett hálózathoz (például a munkahelyéhez) csatlakozna, a VPN-szolgáltató szervereihez csatlakozik adatbiztonság és a magánéletének védelme érdekében. Itt az elsődleges cél a felhasználó védelme, sok esetben személyazonosságának elfedése.

A virtuális magánhálózatok ugyanakkor nem jelentenek minden problémára univerzális megoldást és például jelentős felhasználási korlátot jelent, hogy bizonyos típusú VPN-ekben az üzenetszórás nem úgy működik, mint a helyi hálózatokban. A 2. rétegbeli alagútkezelési protokollok igyekeznek ezzel a problémával is megbirkózni. Fontos látni még azt is, hogy a VPN forgalom a nyilvános interneten keresztül halad, valamilyen szinten a nyomkövetés továbbra is lehetséges és a forgalmi profilból is számos következtetés levonható, még akkor is, ha titkosított. Természetesen ez még inkább így van, ha a felhasználó csak böngészőn keresztül kapcsolódik a VPN-hez, hiszen akkor a többi forgalma teljesen nyitott. Természetesen a VPN nem véd sem a vírusoktól, sem az egyéb internetes támadásoktól.

[23] https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn

3.6 Mit hozhat a jövő?

3.6.1 Szoftverizáció

Az Internet infrastruktúrájának jövőjét meghatározó egyik legfontosabb trend a szoftverizáció térnyerése. Ez a technológiai változás az infrastruktúra összes fentebb említett elemében megjelenik. A virtuális magánhálózatok tulajdonképpen már a kezdeti változataik létrehozásától kezdve szoftvertermékek voltak, hiszen a meglévő fizikai összeköttetések fölött ideiglenes jelleggel létrehozott vagy állandóan működő overlay hálózatok kialakítását szoftveres megoldások teszik lehetővé. A hozzáférési hálózatok esetén a helyhez kötött szolgáltatási pontok esetén az SDN, mint hálózatmenedzselési technológia egyelőre nem jut szerephez a customer edge-en túl, csak a maghálózatban, viszont a rádiós hozzáférések esetében az Open RAN koncepció egyértelműen a szoftveres komponensek mind nagyobb szerepe irányába tolja el a hálózatfejlesztést. Az Internet adatkicserélő központok esetében a szoftverizáció az elmúlt évtizedben jelent meg, több koncepció is verseng[24], de azt nem tudjuk egyértelműen, hogy jelenleg működik-e teljes értékű szoftveres IXP.

3.6.2 Biztonság

Az Internetnek magának és a rajta keresztül nyújtott szolgáltatásoknak a biztonsága a jövőben még a mostanihoz képest is sokkal jelentősebb kérdés lesz, tekintettel arra, hogy a gazdasághoz, a közlekedéshez, a kritikus rendszerekhez kapcsolódó automatizáció szintjének növekedése egyre erőteljesebb lesz. Ez nemcsak abban nyilvánul meg, hogy a nem személyi kommunikációra szolgáló internetvégpontok száma lényegesen – akár több nagyságrenddel – meghaladja az emberek által használt internetvégpontok számát, hanem abban is, hogy egy idő után az M2M és az ember-gép forgalom összessége is túlsúlyba fog kerülni. Ráadásul a sebesség és a feldolgozóképesség/számítási teljesítmény növekedése azt is jelenti, hogy a rosszindulatú vagy éppen csak véletlenül hibát okozó forgalom/szolgáltatás/jelzés feltartóztatására, a hálózati vagy adatbiztonsági problémák megakadályozására az emberi reakcióidő nem lesz elegendő – nemcsak a szükséges beavatkozás elvégzésére, hanem a döntés meghozatalára vagy akárcsak a hálózatbiztonsági rendszerek által felajánlott eljárás jóváhagyására sem. A már jelenleg is elérhető mesterséges intelligencia által vezérelt biztonsági megoldások megkerülhetetlenek lesznek a jövő hálózatában. Szerepük növekedni fog és az adatközpontok mellett az ISP maghálózataiban, a CDN-ekben és a felhőszolgáltatóknál is megjelennek.

A különböző típusú felhőszolgáltatások védelméről nyilván jelenleg is igyekeznek az üzemeltetők megfelelően gondoskodni, de ahogy egyre több nagyobb földrajzi területre kiterjedő szolgáltatás infrastruktúrája lesz felhőalapú, úgy várhatóan az ezek elleni támadások is felerősödnek és változatosabbá lesznek, megkövetelve a védelmi rendszerek erősítését is.

Ugyanakkor a Software-as-a-Service és a Database-as-a-Service felhőszolgáltatás-típusok sajátos vegyülékeként megjelenhet a Security-as-a-Service, vagyis egy olyan felhőszolgáltatás-típus, amely az Internet különböző végpontjainak – legyen azok egyéni felhasználók, vállalkozások, állami szereplők vagy non-profit csoportok, az igényeiknek és az elvárásaiknak megfelelő biztonsági szolgáltatást nyújt. Ezek a Security-aaS megoldások szintén gépi tanulási és mesterséges intelligencia alapon kell létrejöjjenek. Az adatbázisuk

[24] Például: SDX: https://people.csail.mit.edu/alizadeh/courses/6.888/papers/sdx.pdf, iSDX: https://dl.acm.org/doi/10.5555/2930611.2930612, DeSi: https://ieeexplore.ieee.org/document/9439194, SDNaaS: https://ieeexplore.ieee.org/document/9974910/

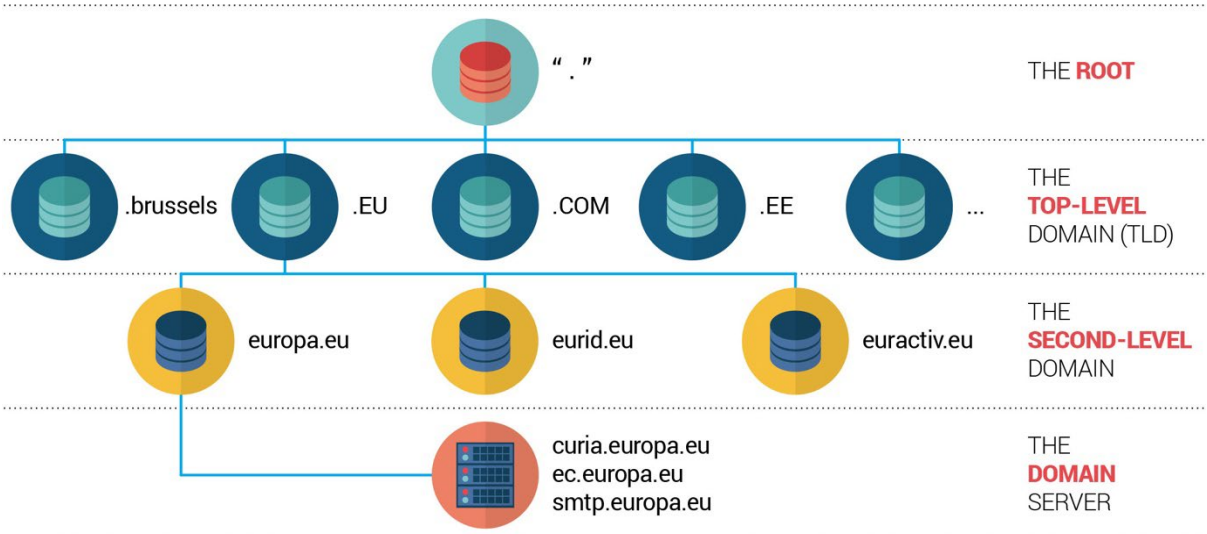
mérete, a rövid időn belül az Internet különböző részeiről származó beáramló adatmennyiség és a beavatkozási lehetőségek technológiai és nagyságrendi tekintetben is széles skálája egy nagyon hatékony rendszert eredményezhet, amely bármilyen felismert támadásra nagyon rövid időn belül reagálni tud az által felügyelt hálózaton belül.

3.6.3 Szolgáltatásminőség

A jövő internetében az emberi felhasználók által az érzékelt szolgáltatásminőség vélhetően nem sokat változik. Mostanra a piac elég nagy része számára elérhetőek olyan hozzáférési lehetőségek, amelyek a jelenlegi megjelenítők paramétereit és az emberi érzékelés jellemzőit figyelembe véve tulajdonképpen hibátlannak tekinthető felhasználó élményt nyújtanak. Az 5G-s mobilinternet rendszerek ehhez még hozzáadják az eléggé széleskörű mobilitás lehetőségét is. Nem várható azonban ugyanilyen előrelépés a szolgáltatások rendelkezésre állása tekintetében. Nyilván az előfizetők jelentős része száma ez legfeljebb kényelmi problémát jelent és ebben a tekintetben sem túlzottan lényeges, ugyanakkor az M2M kommunikáció számára ez kardinális kérdés lehet, főleg, ha kommunikálni kívánó eszközök valamilyen kritikus rendszer részei. Figyelembe véve, hogy az M2M kommunikációban az emberi adatfeldolgozási korlátok nem érvényesülnek, azt is látjuk, hogy az elvárt szolgáltatásminőség biztosítása ebben az esetben akár magasabb szinten is kell megvalósuljon, mint az emberi felhasználók tekintetében.

4 Domain Name Service

A névfeloldási szolgáltatás az IP alapú világ mai napig kiemelt jelentőségű infrastrukturális építőeleme. A szolgáltatás alacsony válaszideje hozzájárul a jó felhasználói és szolgáltatásminőséghez. A redundancia lehetősége bizonyos szinten a kezdetektől fogva adott, de a modern elvárások (felhőszolgáltatások, adatvédelem) új kihívásokat támasztanak.



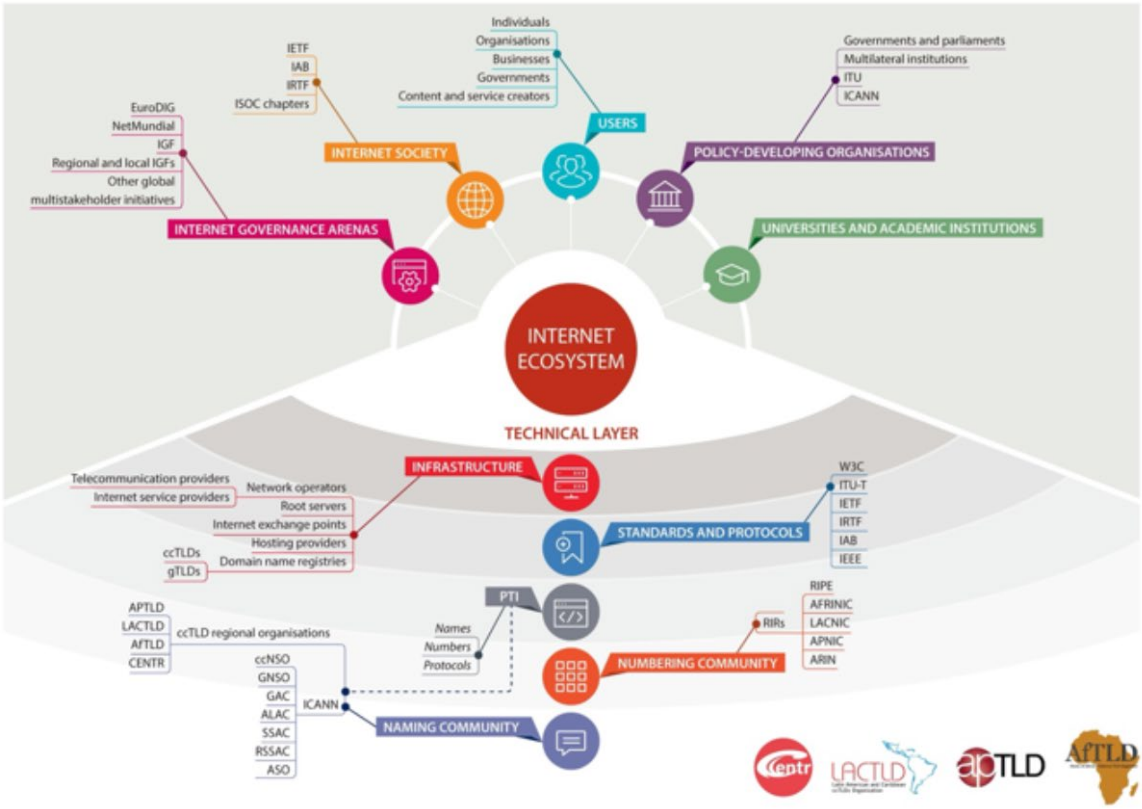
14. ábra A domain nevek strukturálódása

4.1 A DNS ökoszisztéma

A hierarchia tetején a TLD-k (Top Level Domains) állnak, amelyeket a gyökér (root) DNS szerverek ismernek. Ezek között lehetnek ccTLD-k (country code TLD) és gTLD-k (generic TLD) (lásd 14. ábra[25]). Bár a gyökér szerverek IP címei mögött minden bizonnyal redundáns és terheléselosztott csomópontok vannak, a terheléscsökkentés végett a feloldás változatos szintjein is gyorsítótárazzák a keresési eredményeket, a DNS szerverektől egészen az alkalmazási rétegig.

Ezt a hierarchiát több fontos szervezet is szabályozza és számos iparági szereplő vesz részt a fenntartásában (lásd 15. ábra). Az elnevezések szabályzásában irányadó az ICANN (Internet Corporation for Assigned Names and Numbers). A regionális internet regisztrátorok szabályozzák az IP kiosztást a régióban (pl. kontinensen) érvényes szabályok szerint, Európában például a RIPE (Réseaux IP Européens) felügyelete alatt.

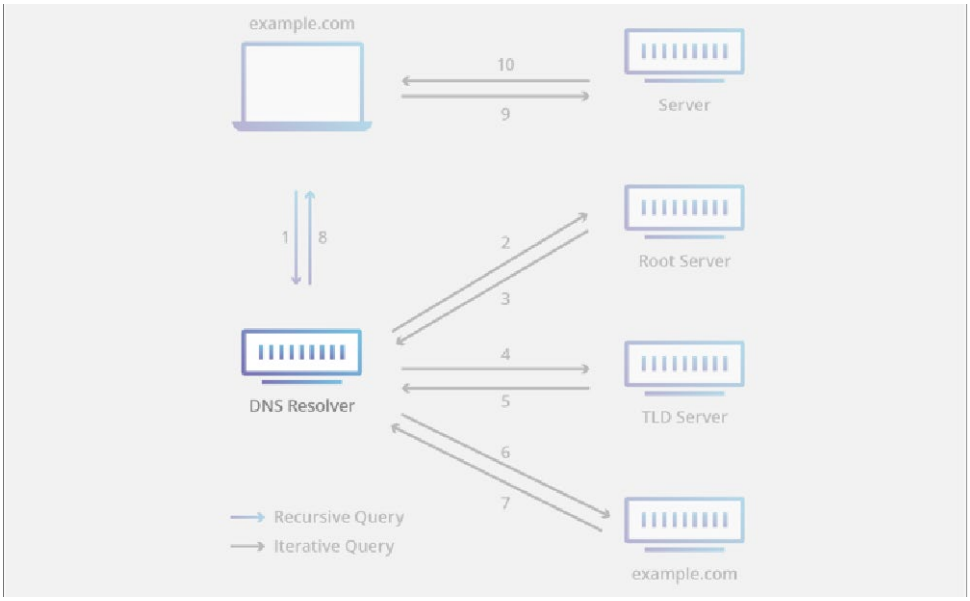
[25] https://www.centr.org/about-the-industry/item/the-dns.html



15. ábra Az internet ökoszisztémája

4.2 A névfeloldás folyamata és gyenge pontjai

Rekurzív lekérdezéskor a feloldási feladatot kvázi delegáljuk egy DNS szerver felé (lásd 16. ábra[26]). A gyorsítótárazásnak köszönhetően ez ugyan gyorsítja a folyamatot, de egyben támadási felületeket is nyithat (ld. DNS amplifikációs támadás).



[26] https://www.cloudflare.com/learning/dns/what-is-recursive-dns/

16. ábra Rekurzív és iteratív DNS feloldás

Bár a TCP is támogatott, a lekérdezések számára hagyományosan az UDP a jellemző transzport protokoll, mivel a TCP-vel ellentétben szükségtelen kapcsolatfelépítési fázis elhagyásával jelentősen lerövidül a válaszidő. Ez ugyanakkor korlátozza a kommunikációs fél azonosítását, biztonsági szempontok alapján történő ellenőrizhetőségét is.

Lekérdezéskor hagyományosan unicast típusú kommunikáció zajlik: a kliens elküldi kérését a feloldónak, amely a feldolgozás után küldi vissza neki az eredményt. Nincs ráhatásunk, hogy a feloldási folyamat során mely további feloldókhoz forduljon az első megkérdezett feloldó.

4.3 Jellemző támadástípusok

A biztonsági rések három fő csoportba sorolhatók: felhasználók (szervezetek, vállalatok, végfelhasználók), infrastruktúra szolgáltatók ellen, ill. az implementációs hiányosságok kihasználása mentén indított támadásokra. A fő ismert támadástípusokat az 1. táblázat foglalja össze aszerint, hogy azok mely ügyfélköröket érintik.

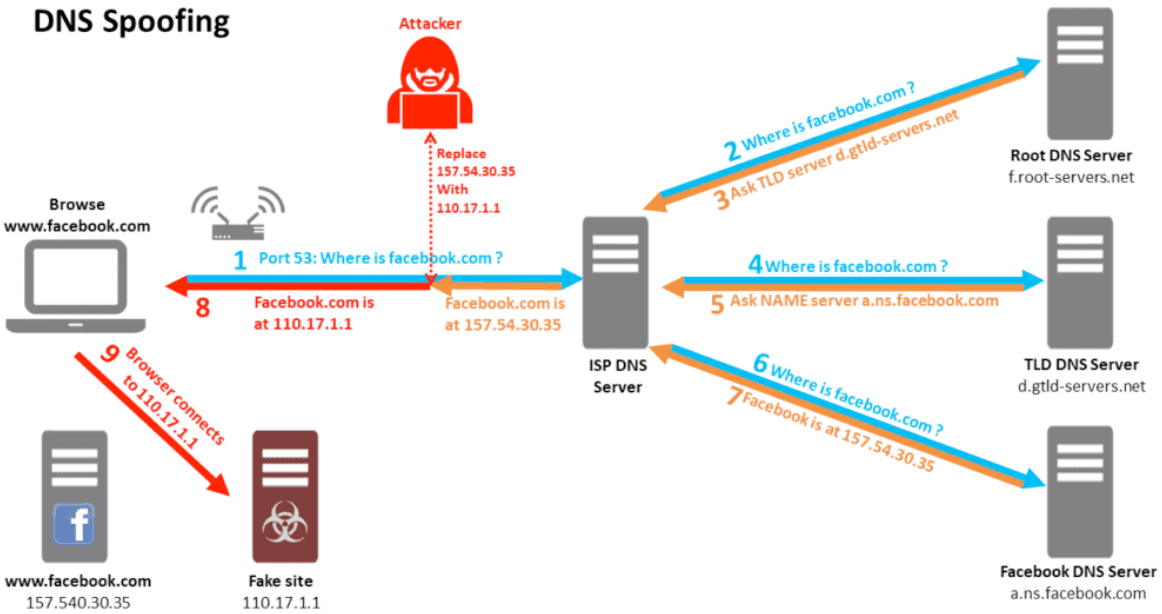
1. táblázat Az egyes sebezhetőségeknek való kitettség szereplők szerint

	Felhasználó	**Szervezet**	**ISP**	**IXP**	**IP transit**	**Felhőszolgáltató**
Lehallgatás	x	x				
Elárasztás		x	x			x
Amplifikáció	x	x	x			x
Mérgezés		x	x			x
Slamming	x	x				
Drop catching	x	x				
***squatting**	x	x				

4.3.1 Lehallgatás és eltérítés

A DNS feloldás szolgáltatás eredendően nem tartalmaz a felhasználó kilétére vonatkozó információt, de a feladó IP címét és a lekérdezés tárgyát begyűjtve bizonyos mértékben nyomon követhetővé válik. A titkosítatlan DNS lekérdezések lehallgathatók és az áldozatot rosszindulatú webhely vagy egyéb IP szolgáltatás felé terelheti a támadó (lásd 17. ábra[27]). Védekezés: végpont-végpont titkosítás.

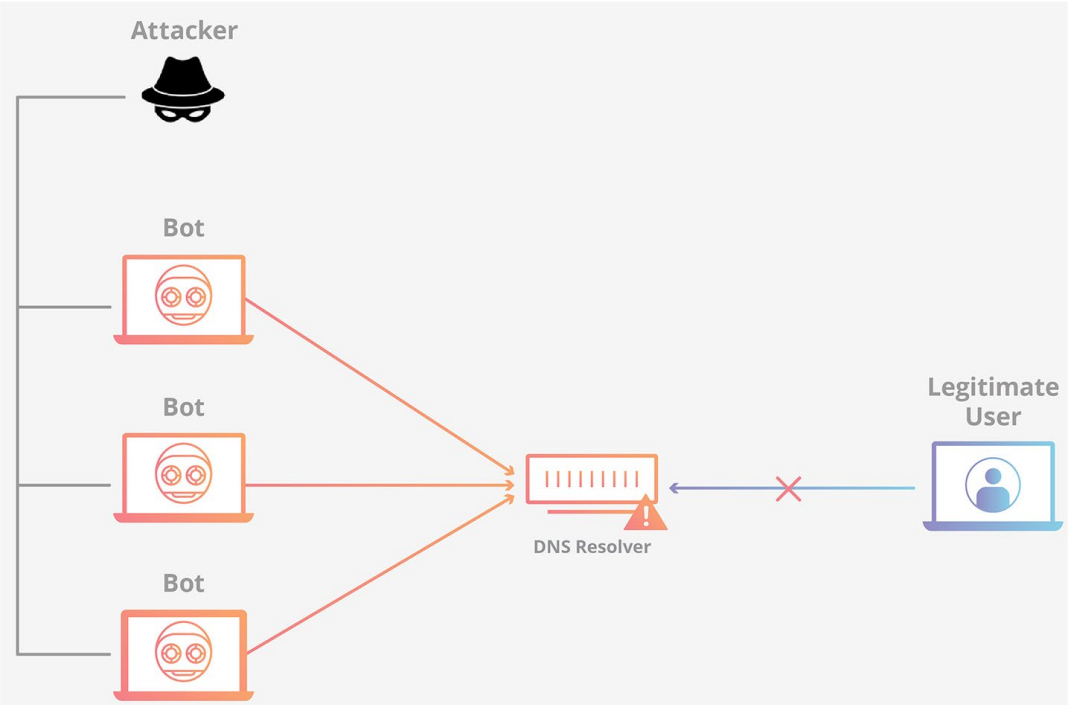
[27] https://www.3key.company/encrypted_dns



17. ábra DNS lehallgatás és eltérítés

4.3.2 DNS elárasztás

A támadó zombigépek hálózatának segítségével intéz nagy mennyiségű lekérdezést a megcélzott DNS szerver irányába (lásd 18. ábra[28]). E DDoS támadás célpontja konkrét DNS szolgáltatás, célja bizonyos domainek, pl. adott szolgáltatáshoz kapcsolódó domain nevek feloldásának ellehetetlenítése.



18. ábra A DNS elárasztásos támadás

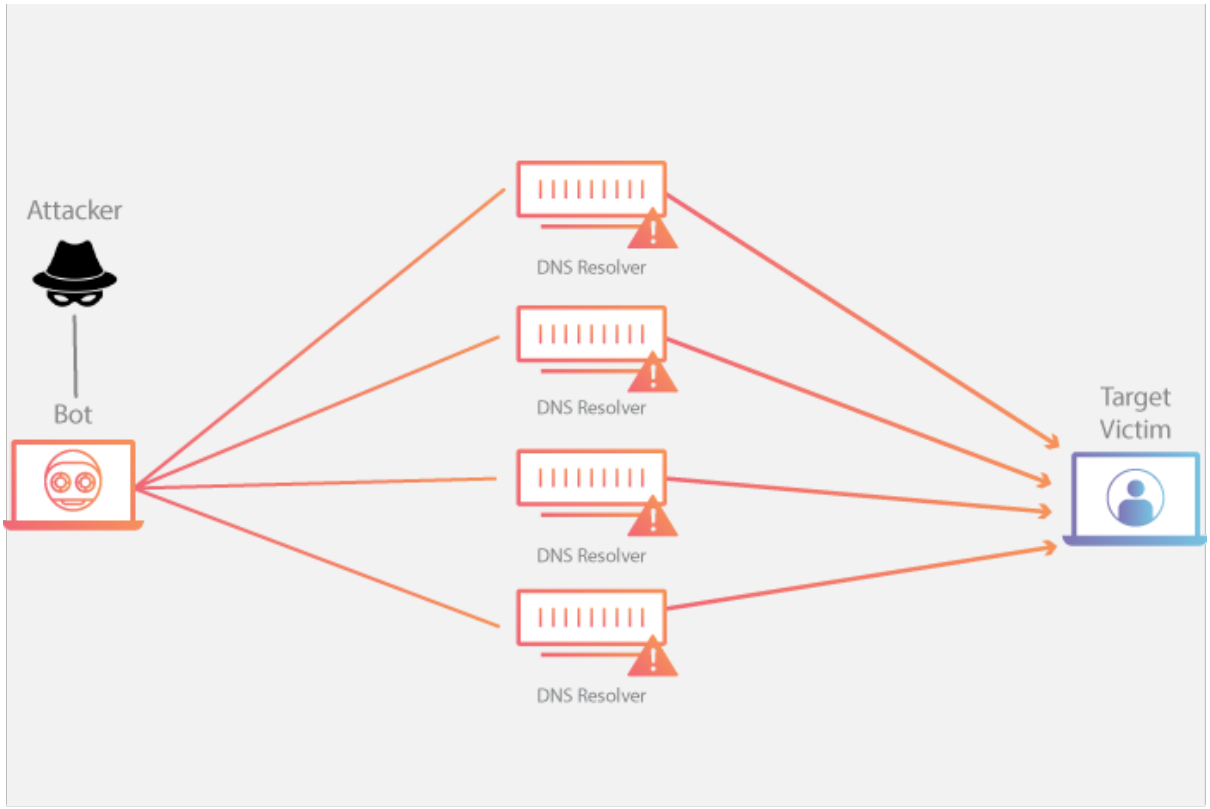
[28] https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/

Felderítését nehezíti, hogy mintázata hasonló a nagy terhelésű időszakok forgalmához, amikor szintén sok irányból történik lekérdezés rövid idő alatt. Védekezés: terheléselosztással, DDoS monitorozással.

4.3.3 DNS amplifikáció

E támadásnak csupán eszköze a DNS szolgáltatás, a célpontja egy adott IP végpont. A támadó rendszerint zombigépek hálózatát használva nagy mennyiségű DNS lekérdezést küld egy kiválasztott DNS szerver felé. A szervernek a választ egy áldozat vagy hamis IP cím felé kell majd visszaküldenie, tehát a válasz címzettje nem a kérés valódi feladója lesz (lásd 19. ábra[29]). Még jobban leterhelheti az áldozat erőforrásait, ha a válasz hosszú (nem fér el egy IP csomagban). Ez a támadástípus rekurzív lekérdezést elfogadó DNS szerverek esetén jellemző, általában rossz konfigurációs beállítás esetén.

A védekezés egyéni vagy kisvállalati szinten korlátos. A kérések feladójának ellenőrzése segíthet, ill. a nyitott (bárkinek válaszoló) DNS szerverek számának csökkentése egy másik lehetőség. Az előbbihez nem mindig adott a helyi szintű tudás. Internet szolgáltatók (Internet Service Provider, ISP) és felhőszolgáltatók viszont hatékonyabban tudnak védekezni ellene.



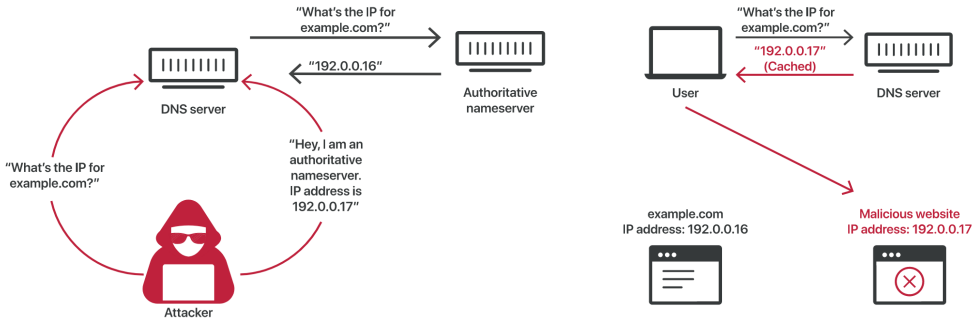
19. ábra A DNS amplifikációs támadás

4.3.4 Gyorsítótár mérgezés, DNS hamisítás

A támadás a DNS gyorsítótárazás mechanizmusára épít: Ha egy kérés eredménye nincs benne a gyorsítótárban, akkor a szerver egy irányadó (autoritatív) DNS szerverhez fordul. A

[29] https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

támadó az irányadó névszerver nevében küldi a választ, meghamisítva a gyorsítótárazandó eredményt (lásd 20. ábra[30]). A támadás kivitelezéséhez a támadónak számos dolgot ismernie kell a kéréssel kapcsolatban (kérésazonosító, kérés feladó portszáma, gyorsítótárazva van-e már a kérés, kiválasztott irányadó névszerver IP-címe) és még a tényleges válasz megérkezése előtt el kell készítenie és küldenie a mérgező csomagot. Ezért egy már kompromittált DNS szerveren valószínű a támadás kivitelezése.



20. ábra A DNS mérgezéses támadás

A támadást a felhasználókat korlátozó hatalmi szereplők előszeretettel használják tartalmak cenzúrására, tartalomhozzáférés korlátozására, hiszen a meghamisított információ a DNS szervert kérdező összes felhasználóhoz szétszóródik. Védekezni ellene a DNSSEC alkalmazásával és a DNS szerver megfelelő védelmével lehet.

4.3.5 Domainnév slamming[31]

Adathalászati technika, amely egy adott domainnév tulajdonosa ellen irányul. Például egy hamis számlát küldenek megújítási figyelmeztetésre hivatkozva, de valójában mögötte átregisztrálás történik egy másik szolgáltató felé, ami által elbitorolják az eredeti tulajdonostól az érintett domainnevet.

Egyéb esetekben pedig arról értesítik a tulajdonost, hogy a domainneve, vagy egy arra nagyon hasonlító domain regisztráció alatt van egy harmadik fél által. Egy magasabb összeg megfizetésével viszont elsőbbséget kaphat. Ez esetben a becsapott felet lopják meg.
Ez a visszaéléstípus az emberi figyelmetlenségre alapoz, ezért technológiai megoldást nehéz kínálni a védekezéshez.

4.3.6 Domainnév drop catching[32]

Ha egy domainnév előfizetése lejár egy regisztrátornál, a meghosszabbítást elszalaszthatja az ügyfél, ha nem fizet időben. Ha ekkor más is megigényli a domainnevet, az az illetőhöz kerülhet. Ez ellen a törvény védi a védjeggyel rendelkező szereplőket. Egyéb ügyfelek felé a regisztrátor abban az esetben köteles türelmi időszakot adni, ha az ICANN RAA (Registrar Accreditation Agreement) megállapodás részeként ún. megváltási türelmi időszakot (RGP)

[30] https://www.cloudflare.com/learning/dns/dns-cache-poisoning/
[31] https://icannwiki.org/Domain_Slamming
[32] https://icannwiki.org/Drop-Catching

tart fenn. Ilyenkor a lejárat után 30-90 napja van az eredeti ügyfélnek, hogy meghosszabbítsa domainneve előfizetését.

Nem tekinthető technológiai jellegű támadásnak. Az ügyfél proaktivitással tud védekezni, azaz figyeli a domainneve lejárati idejét. Ezt segítendő a regisztrátor küldhet értesítő üzenetet a lejárat közeledtéről.

4.3.7 Elgépelt doménnevek (typosquatting és cybersquatting)[33]

Előfordulhat, hogy a felhasználó félregépeli a domainnevet. A leggyakoribb elgépelt domainneveket is sok esetben foglalják le előre. Typosquattingról beszélünk akkor, ha a cél, hogy az eredeti domainnév elgépelőit kattintásnövelés és egyéb tartalmak megtekintése céljából összefogdossák. A cybersquatting ennek súlyosabb esete, amikor az eredeti domainnév mögötti szolgáltatást mímelő oldalt építenek fel adathalászati és egyéb visszaélési céllal, hogy a felhasználót megtévesztve a szolgáltatáshoz kapcsolódó adatait megszerezzék, esetleg az eredeti domainnév tulajdonosát rossz hírbe hozzák.

Védelem szempontjából fontos tényező a felhasználó ébersége, ill. a népszerű böngészők blacklistekkel igyekeznek szűrni az ilyen jellegű domainekre tévedést. A süllyesztő (sinkhole) jellegű megoldások is hatásosak ellenük.

4.4 Jelenlegi védelmi megoldások

A 2. táblázat a jelenleg alkalmazott DNS védelmi megoldásokat foglalja össze olyan szempontból, hogy azok jellemzően mely felhasználói kör védelmét látják el.

2. táblázat Alkalmazható védelmi lehetőségek szereplők szerint

	Felhasználó	Vállalat	ISP	IXP	IP transit	Felhőszolgáltató
Sinkhole	x	x				
Osztott DNS	x	x				
DNSSEC	x	x	x	x	x	x
DoX: DoH/DoT/DoQ	x	x				
DNSCrypt	x					
Anycast DNS						x
oDoH	x	x				

Az egyes védekezési módszerekről részletesebben:

- DNS süllyesztő (sinkhole)[34]: A felhasználó DNS válasz általi eltérítése ellen véd. A felhasználó DNS kéréseit átvezetik rajta. Az ismert kamu, adathalász domainnevekhez tartozó választ írja át úgy, hogy a felhasználó ne jusson el a rosszindulatú helyig.

- Osztott (split) DNS: Vállalati vagy privát környezetben alkalmazott módszer: a belső hálózat címeinek (saját zóna) feloldása eltérő módon történik, mint az azon kívülieké. Például a privát hálózat gépei más IP címen szólíthatják meg ugyanazon domainnevű

[33] https://icannwiki.org/Typosquatting, https://icannwiki.org/Cybersquatting
[34] https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole

csomópontot, mint a publikus irányból érkezők. Segít a mérgezéses támadásokat elkerülni.

- DNSSEC (Domain Name System Security Extensions)[35]: Célja a man-in-the-middle meghamisítás elleni védelem. DNS rekordok digitálisan aláírt halmazain alapul. Segítségével egy névfeloldó ellenőrizheti (pl. adott zónáról) kapott információ hitelességét. Infrastrukturálisan komplexebb implementálni az igényelt kriptográfiai infrastruktúra kapcsán.

  Kihívások: Egyes tűzfalak legfeljebb 512 bájtos UDP csomagban elhelyezett DNS üzenetet várnak. Fragmentáció alkalmazása esetén további nehézség a körülményesebb elemzés[36], ami válaszidő növeléssel jár vagy akár kapcsolódási hibák is felléphetnek a válaszok eldobása miatt[37]. Emiatt a végfelhasználói oldalon nehézkesebb lehet az alkalmazása.

- DNS over HTTP és DNS over TLS[38]: Cél a teljes kérdés/válasz kommunikáció titkosítása kliens és feloldó között. DoH esetében a DNS lekérdesek szinte teljesen belesimulnak a webböngészés csomagjai közé, a DoT viszont jellemzően eltérő portszámot alkalmaz. Inkább kiegészítik a DNSSEC-et, mint kiváltják.

  Felhasználói oldalon az elterjedését segíti, hogy az operációs rendszerek[39] és a böngészők[40] is elkezdték beépíteni a támogatásukat.

- DNS over QUIC: A megoldás szabványosítási folyamata során 2022-ben draft státuszba került[41], mint a DoH és DoT alternatívája. Ezek szűk keresztmetszete a TCP transzportréteg head-of-line-blocking problémája, vagyis az esetlegesen elvesző adat a sikeres újraküldésig feltorlasztja az utána továbbítandó adatokat is. Ez az egyre elterjedtebb mobil hozzáférés során gyakori érzetiminőség csökkentő jelenség.

- DNSCrypt[42]: Célja a lekérdezések anonimizálása. Azon felhasználók használják, akik szeretnék elrejteni adatforgalmuk DNS lekérdezéseit, amely felfedheti a látogatott webhelyeket és a fogyasztott tartalmak jellegét. Használata némi technikai felkészültséget is igényel (3rd party alkalmazás telepítése szükséges).

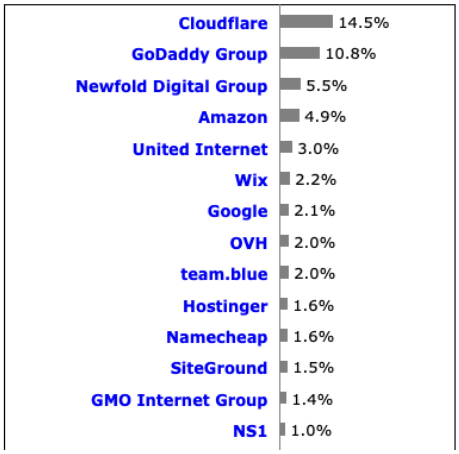
- Anycast DNS: Egy feloldó IP címe mögött egy terhelés elosztó logika van, amely biztosítja, hogy a kérdezőtől leggyorsabban elérhető feloldó válaszolja meg a kérést. Hatékony DDoS védelmi mechanizmus az elárasztásos támadással szemben.

[35] https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
[36] https://blog.apnic.net/2017/08/22/dealing-ipv6-fragmentation-dns/
[37] https://annasperotto.org/publication/papers/2014/broek-commag-2014.pdf
[38] https://www.cloudflare.com/learning/dns/dns-over-tls/
[39] Apple macOS 11 és iOS 14 felett: https://www.zdnet.com/article/apple-adds-support-for-encrypted-dns-doh-and-dot/, Microsoft Windows 10 build 19628-tól: https://blogs.windows.com/windows-insider/2020/05/13/announcing-windows-10-insider-preview-build-19628/
[40] "DNS queries from the Firefox browser are encrypted by DoH and go to either Cloudflare or NextDNS.", https://www.cloudflare.com/learning/dns/dns-over-tls/
[41] https://datatracker.ietf.org/doc/rfc9250/
[42] https://dnscrypt.info/

- oDoH[43]: Jelenleg draft státuszú szolgáltatás, a CloudFlare-nél már kipróbálható. Segítségével a kliens IP-címe rejtve marad a feloldó számára, mivel egy beékelődő proxy (amely a titkosított forgalomba nem lát bele) továbbítja a kéréseket egy köztes csomópont felé. Ez a köztes csomópont fogja a feloldót megkérdezni és a választ visszaküldeni.

4.5 Meghatározó szereplők

A 21. ábra[44] a legnagyobb DNS regisztrátorok listáját mutatja 2023. október 1-én. A CloudFlare globálisan meghatározó szereplő, elsősorban CDN, felhőbiztonsági, DDoS védelmi és DNS regisztrátori szolgáltatásokat biztosít. Ingyenes DNS feloldási szolgáltatást (1.1.1.1) is nyújt, valamint a fentebb említett oDoH-t.



21. ábra Az 1% és afölötti piaci jelenléttel bíró DNS szolgáltatók listája

További jelentős szervezetek:

- Packet Clearing House (PCH)[45]: Internet kicserélő (Internet Exchange Point, IXP, kb. 700 db kicserélési ponttal) és DNS szolgáltató (2 gyökér szerver, több, mint 400 TLD biztosítása, adaptív DNS, DNSSEC).

- Global Cyber Alliance (GCA)[46]: IT biztonsággal foglalkozó cég, többek között a Quad9[47] DNS blokkoló szolgáltatást biztosítják.

4.6 Említésre méltó jelenségek

4.6.1 BRICS

A BRICS (Brazil, Russia, India, China, South-Africa) DNS-e egy alternatív DNS szolgáltatás. Ezek az autokratikus berendezkedésű nemzetek saját névfeloldó szolgáltatást tartanak fenn, hogy az állampolgáraik tartalomhozzáférését befolyásolják. Ez nemcsak a szóban forgó országok felhasználóira kártékony, hanem az internet esetleg két- vagy több részre szakadásával

[43] https://datatracker.ietf.org/doc/html/draft-pauly-dprive-oblivious-doh-03
[44] https://w3techs.com/technologies/overview/dns_server
[45] https://www.pch.net/
[46] https://www.globalcyberalliance.org/
[47] https://www.quad9.net/

sérülhet a földrajzi redundancia elve is[48]. Ha például egy domainnév nincs regisztrálva egy ilyen alternatív DNS-ben, akkor az ottani felhasználók azt nem fogják elérni.

4.6.2 DNS4EU[49]

Az EU saját DNS szolgáltatás felépítésén dolgozik. Az EU szándéka, hogy a tagállamok IT infrastruktúrája minél kevésbé függjön a főként USÁ-ban működő tech-vállalatok által biztosított szolgáltatásoktól. Mivel a felhasználók zöme az ISP-je által kiajánlott DNS feloldót használja, a névfeloldási kérelmek jó része a fent említett szereplők szolgáltatásához fordul. Ezen kívül az EU fontos szempontként kezeli a felhasználók online térbeli biztonságát. A névfeloldási szolgáltatás fontos technológiai belépési pont lehet ehhez. Segítségével a káros, rosszindulatú szolgáltatások opcionális (felhasználó általi beleegyezéssel történő) szűrése és modern biztonsági megoldások (IPv6, DNSSEC, DoH/DoT) is könnyebben lennének elterjeszthetők.

A projektet vivő konzorciumot a Whalebone[50] nevű cseh szoftvercég vezeti és további 12 tagja van, köztük hazánkból a SZTAKI.

Biztosítani fog egy publikusan hozzáférhető felhős, terheléselosztott, alacsony késleltetésű feloldószolgáltatást, szűrési funkcióval. ISP-k és CSP-k (Communication Service Provider, vagyis telekommunikációs szolgáltatók) számára kihelyezett feloldókat is fog biztosítani, de a felhős megoldás IP-címeivel. A szolgáltatást érő támadásokról gyűjtött információkat anonimizálás után kutatási céllal felhasználják. Cél egy, a nyilvános feloldók fölött nyújtott profitorientált szolgáltatás kialakítása is.

A DNS4EU szolgáltatás a konzorcium felügyelete alatt fog állni. Az EU nem tervezi kötelezni az állampolgárait annak használatára. Bár a tagországok kormányainak és állami szerveinek valószínűleg ajánlani fogják a használatát a biztonság növelése érdekében. A konzorcium vezetője szerint a naplókban nem keletkeznek majd olyan információk, amelyek a felhasználók személyének beazonosítására vagy IP-címének visszakeresésére alkalmasak.

Bár az EU-n belül már a gyakorlatban is létezik hasonló szemléletű szolgáltatás (pl. az AdGuardé[51]), ha megvalósul, minden bizonnyal fontos szereplővé léphet elő, bár a térnyeréshez megfelelő súlyú promóció és ajánlások is szükségesek lesznek, például a nemzeti hatóságokon keresztül.

4.6.3 Szoftver gyártók

Az operációs rendszer gyártók elkezdték bevezetni a DoX támogatást, ahogy a böngésző gyártók is. A Mozilla Firefox egyre több országban (USÁ-ban már 2019 óta) teszi alapértelmezetté a böngészőjében a DoH használatát. Ez esetben egy megbízható partner (pl. CloudFlare) szolgáltatását használják a böngészőből feloldás elvégzéséhez. Ez a függés nem rejt nagy teljesítmény és megbízhatóságbeli kockázatot, mivel jellemzően jól skálázódó

[48] https://thecustomizewindows.com/2018/02/separate-dns-brics-countries-russia/
[49] https://adguard-dns.io/en/blog/dns-eu-project-secutity.html
[50] https://www.whalebone.io/, https://www.crunchbase.com/organization/whalebone-io
[51] https://adguard-dns.io/

felhőszolgáltatáson alapulnak. Adatvédelem szempontjából viszont kikerülnek a feloldott információk az ISP-k vagy a vállalati DNS szerverek hatásköréből.

Az operációs rendszerekben egyelőre alapértelmezés szerint a DHCP szolgáltatástól kapott DNS szervert használja a rendszer. A vállalati felhasználásra szánt rendszereknél minden bizonnyal még jó ideig így is marad, de a magánszféra biztonságosságának fontossága miatt az otthoni felhasználók eszközeinél a böngészőknél tapasztalható irányba fordulhatnak a trendek. A Microsoft jelentős felhő infrastruktúrával bír, ezért az otthoni használatra szánt Windows desktop verziókban alapértelmezetté válhat a saját felhőjéből kiszolgált DoX.

4.7 Mit hozhat a jövő?

A trendekből kiolvasható, hogy a fő kihívás a biztonság és privátszféra biztosítása a gyors válaszidő és magas rendelkezésre állás mellett.

4.7.1 IP levélelemek

Végfelhasználók: A felhasználók zöme nem változtat az alapértelmezett DNS beállításokon. Ezért az eszközeik és a rajtuk használt szoftverek alapértelmezett feloldási megoldásai fogják meghatározni a működést.

Vállalatok, szervezetek: A piaci szereplők legalább két irányból vannak nyomás alatt: Míg költséghatékonysági szempontok miatt egyre nyitottabbak a publikus (bár rendszerint SLA-val biztosított prémium szolgáltatásként) felhőkben nyújtott erőforrások, szolgáltatások használatára, a saját biztonságuk mégis jobban kézben tartható, ha a kritikus infrastrukturális elemek helyi felügyelet alatt maradnak.

Minél kisebb méretű egy szervezet, annál inkább jellemző, hogy ISP-je DNS feloldási szolgáltatására támaszkodik. A változásokra sem feltétlenül reagálnak azonnal, ezért a DNS feloldási mód változása leginkább a szoftverek evolúcióján keresztül várható, ami várhatóan a felhőszolgáltatók irányába terelést fog eredményezni.

4.7.2 IP adatátviteli szereplők

ISP-k és CSP-k: Mivel a végfelhasználókhoz ők vannak a legközelebb, az alacsony válaszidejű DNS feloldást még mindig ők kínálhatják a legeredményesebben. Az 5G terjedésével e szolgáltatás monitorozása még fontosabb lesz.[52] Emellett érdemes a szolgáltatási kínálatba az DNSSEC és DoX technológiák beemelésével is foglalkozniuk.

IXP: A helyi szintű feloldóktól a felhő/globális feloldás kínáló szolgáltatók irányába több ilyen jellegű forgalom várható, de nem jelentős a változás volumene.

IP tranzit: Bár a költséghatékonyság különösen fontos szempont, hiszen kiélezett verseny van a szegmensben, a névfeloldáshoz kapcsolódó forgalom nem jelentős volumenű az egyéb forgalmakhoz képest, ezért nem várható nagy változás.

[52] https://futurecio.tech/idc-telcos-are-favourite-dns-attack-targets/

Felhőszolgáltatók: Nagy kiterjedésű infrastruktúrájukkal komoly szereplők, mivel ez hatékony a terheléselosztást segít megvalósítani és biztosítani az alacsony válaszidőt (ld. anycast DNS), valamint a támadások felismerése terén is előnyben vannak.

4.8 Előrejelzés

Mivel a privátszféra biztonsága – az EU-ban különösképp – egyre fontosabb szempont, a DoX megoldások további térnyerése várható. Globális méretekben ezt az alacsony válaszidővel a globális kiterjedésű felhőszolgáltatók tudják legjobban kiszolgálni. 2021-ben indult az European DNS Resolver Policy kezdeményezés[53], amely megpróbálja közös nevezőre hozni a DNS feloldáskor keletkező személyes adatokat a GDPR-ral. A feloldás nem feltétlenül az EU-n belül következik be (ld.az említett DoX megoldásokat), ezért a megoldás nem egyszerű, ezért iparági támogatást próbálnak meg előhívni.[54]

Felhasználói végpontokon a szoftver gyártókon múlik, mikor és mely felhőszolgáltatók felé kezdik el terelni a felhasználókat. Várható, hogy az igazán nagyokra, a Google-re, Microsoftra CloudFlare-re támaszkodnak majd leginkább.

A vállalati és államigazgatási szektorban továbbra is igény lehet a szolgáltatás központi felügyeletére, ezért nem mindenki fog feltétlenül a felhőszolgáltatókra támaszkodni. Ugyanakkor külső szolgáltatóktól független teljesen biztonságos DNS feloldásra történő átálláshoz szükséges technológiai ismeretekre és infrastrukturális beruházásokra lesz szükség. Ez leginkább a nagyobb cégeknek, ill. az IT vállalatoknak áll majd rendelkezésre, a kkv szektor várhatóan sodródni fog a szoftver gyártók és felhőszolgáltatók diktálta irányba.

Az IaC (Infrastructure as Code) és DevOps paradigma megkövetelte automatizáció következtében egyre fontosabbá válik a DNS infrastruktúra globális megbízhatósága[55]. Mivel a fejlesztési és kihelyezési munkák sok helyről történhetnek egy időben, ezért a DNS frissítések gyors és stabil elterjesztése kritikus fontosságú. Ennek természetesen API oldalról is vannak követelményei.

A névfeloldási szolgáltatás konzisztenciája és megbízhatósága hálózatsemlegességi szempontból is fontos kérdés. A lekérdezések eredményének manipulációjával, meghamisításával felhasználók tömegei zárhatók el információtól és szolgáltatásoktól. Ezért a szolgáltatás felügyelete és a semlegesség biztosítása a nemzeti hírközlési hatóságok fontos feladata a jövőben.

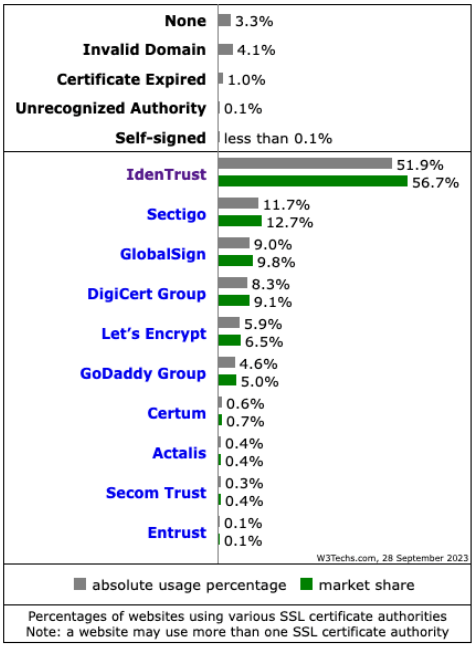
[53] https://europeanresolverpolicy.com/
[54] https://blog.apnic.net/2021/04/12/understanding-the-european-resolver-policy/
[55] https://www.digicert.com/blog/digicert-2023-security-predictions

5 Digitális tanúsítványkiadó hatóságok

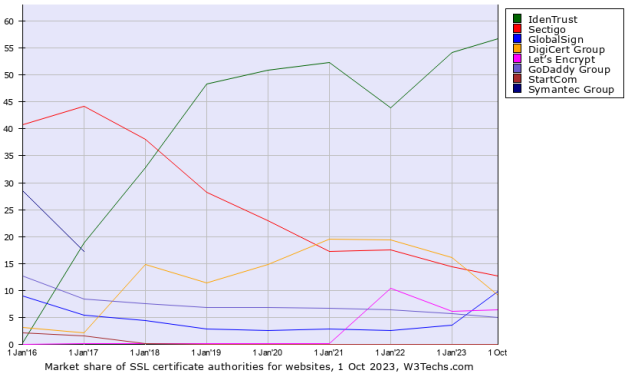
Az internetes kommunikáció protokolljai nagyban támaszkodnak a publikus kulcsú (aszimmetrikus) kriptográfiai algoritmusok és a hozzá kötődő infrastruktúra (Public Key Infrastructure, PKI) alkalmazására. A tanúsítványkiadó hatóságok (Certificate Authorities, CA-k) olyan PKI szereplők, akik digitális tanúsítványokat tárolnak, írnak alá és adnak ki. A tanúsítványok mind a továbbított vagy tárolt információ valódiságának ellenőrzéséhez, mind az átvitel vagy tárolt adat titkosításához használatosak: a privát kulcs segítségével az aláírás vagy titkosítás elvégezhető, a publikus kulcs vagy tanúsítvány segítségével pedig a szignatúra ellenőrizhető vagy a visszafejtés elvégezhető. Az elmúlt évtizedben az adatbiztonság és privát szféra védelme egyre fontosabbá vált. Ezért mára elmondható, hogy a PKI és a CA-k kritikus szereplői a területnek.

5.1 A tanúsítványkiadók piaca

A felhasználók leginkább a website-ok tanúsítványaival találkozik, még ha azok ellenőrzését a szoftverek (jellemzően a böngészők, ill. az operációs rendszer szoftver stackje) transzparensen elvégzik.



22. ábra A website-okat tanúsító CA-k piaca 2023-ban



23. ábra Az SSL tanúsítványkiadók piaca 2023-ban

A 22. ábra[56] a website-okat (domain validation, DV) tanúsító szolgáltatók piaci részesedését mutatja be. Ez a teljes tanúsítvány piac legnagyobb szegmense, 94,4%-os méretével[57]. E területen viszonylag új szereplő az IdenTrust, amely 2016-os megjelenése óta a legnagyobb növekedést produkálta, ahogy azt a 23. ábra[58] is mutatja, amelyen a szereplők piaci

[56] https://w3techs.com/technologies/overview/ssl_certificate
[57] http://web.archive.org/web/20230625223109/https://www.ssldragon.com/blog/ssl-stats/
[58] https://w3techs.com/technologies/history_overview/ssl_certificate/ms/y

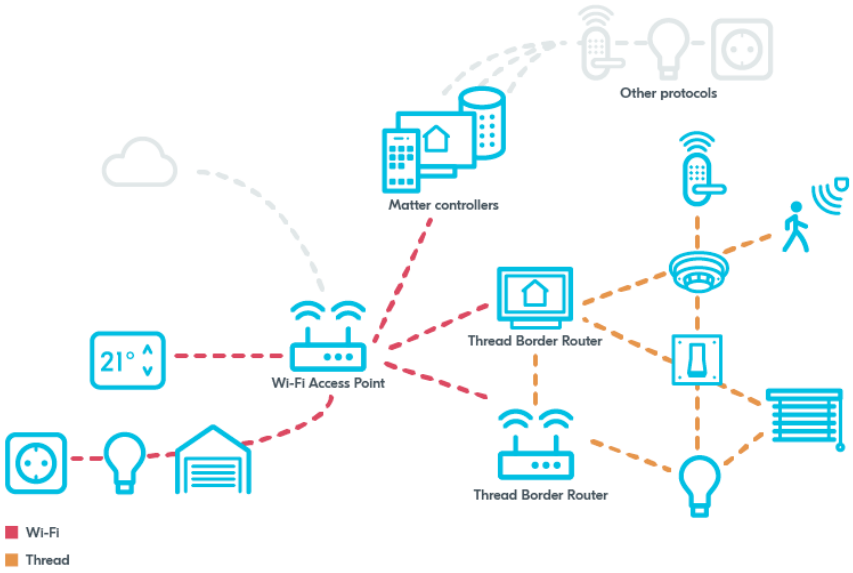
részesedésének változása látható. A szervezettanúsító (organization validation, OV) tanúsítvány piac 5,5%-os méretű, míg a kiterjesztett tanúsítványok (extended validation, EV) termékek 0,1%-nyi.

5.2 Biztonsági helyzet

Bár az SSL tanúsítványok alkalmazását a böngésző gyártók az utóbbi években határozottan kikényszerítették, egy 2022. végén végzett felmérésben a vizsgált site-ok 37,6%-a (köztük sok népszerűvel) nem kellő szintű biztonságot (nem megfelelő tanúsítvány vagy gyenge titkosító algoritmusok) alkalmaz[59]. A legújabb, TLS1.3 szabványt a webhelyek csak 58,9%-a támogatja. És az elavult SSLv2 és SSLv3 szabványokat még a site-ok közel 2%-a fogadja el.

5.3 Fejlemények a digitális tanúsítványok terén

A Matter szabvány[60]: Kezdeményezés az IoT és okosotthon eszközök összekapcsolásának segítéséhez. Komoly szereplők álltak mögé: pl. Apple, Google, Samsung, stb. A DigiCert lett az első Matter-tanúsított CA. A szabvánnyal szeretnék egységesíteni az otthoni okoseszközök menedzsmentjét. Ennek egyik pillére a biztonságos wifi kapcsolat, a WPA3/WiFi6-ra építve. Kommunikációs protokollként a Threadet választották, amely támogatja a kis teljesítményű, hálószerű (nem centralizált) adatátvitelt és segít az offline, helyi hálózatban történő adatfeldolgozás megvalósításában (lásd 24. ábra[61]).



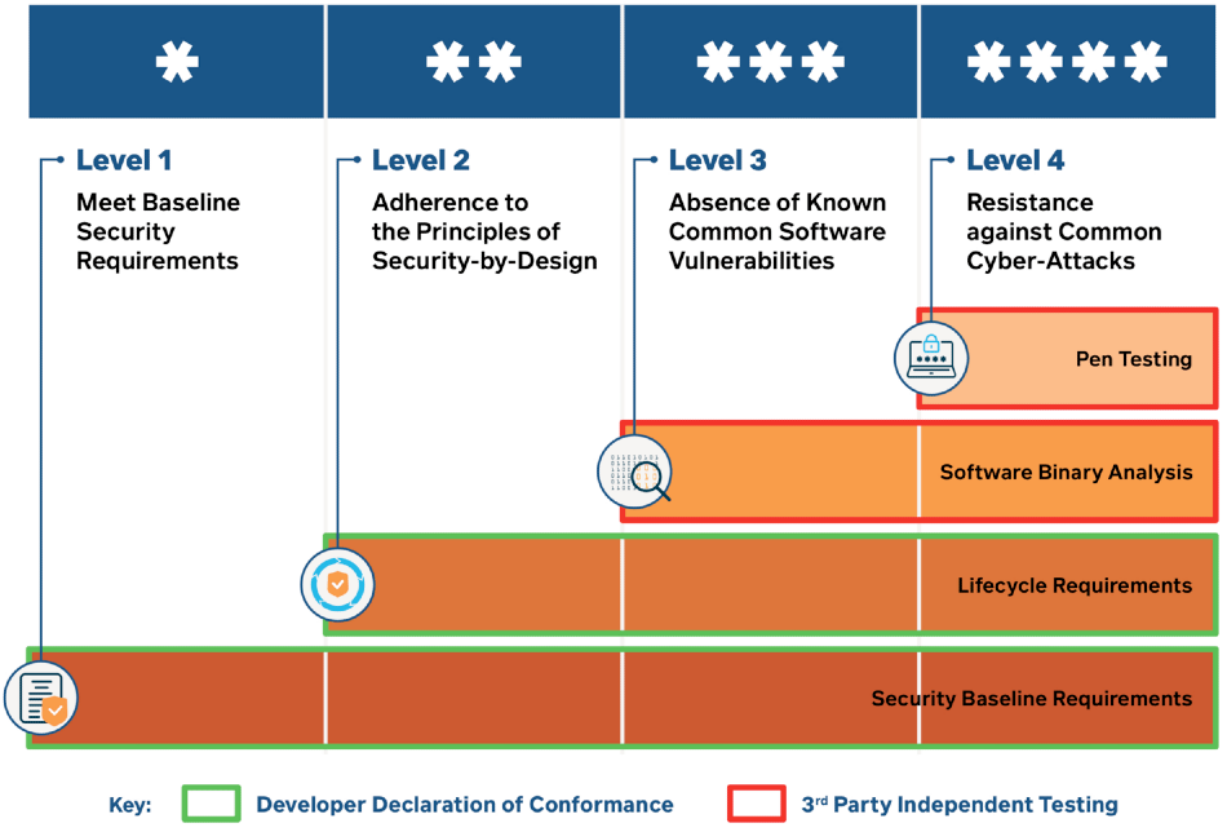
24. ábra A Matter szabványú eszközök jellemző topológiája

[59] http://web.archive.org/web/20230830115308/https://www.ssllabs.com/ssl-pulse/

[60] https://csa-iot.org/newsroom/matter-arrives/, https://www.androidpolice.com/matter-smart-home-standard-explained/

[61] https://developer.nordicsemi.com/nRF_Connect_SDK/doc/2.1.2/nrf/ug_matter_overview_network_topologies.html

IoT biztonsági címkék[62]: A kezdeményezés szeretné megkönnyíteni a tájékozódást a tengernyi IoT eszköz között. Az eszközök a legfontosabb biztonsági paramétereket leíró (milyen adatot gyűjt, milyen célra, mit kezd vele) címkéket kapnának, mint a háztartási gépek energiacímkéi azok energiafelhasználásával kapcsolatban (lásd 25. ábra[63]).



25. ábra A Szingapúrban már alkalmazott biztonsági címkék sémája

A Matter szabvány és biztonsági címke kezdeményezések várhatóan javíthatják majd az IoT eszközök biztonsága terén tapasztalt káoszt (azok pl. gyakran DDoS támadások alanyai), a rosszindulatú forgalmak csökkentése mellett. Viszont a közeljövőben nem várható, hogy minden fontos szereplőt be tudnak vonni a szabvány alá, valamint a már meglevő, a szigorú követelményeknek nem eleget tevő eszközöket rövid távon kiszorítani.

Kvantumbiztos kritptográfia (Post-Quantum Cryptography, PQC): Bár a kvantumszámítógépek mindennapos alkalmazása még távoli jövőnek tűnik, a Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology, NIST) már elkezdte a kripto-agilis algoritmusok keresését és vizsgálatát[64]. Azért is fontos ilyen algoritmusok kidolgozása, mert amint a kvantumszámítógépek szélesebb körben alkalmazhatóvá válnak, a jelenleg még kellően erős (pl. 3072 bites kulcsú RSA vagy 384 bites

[62] https://arstechnica.com/gadgets/2022/10/everything-we-know-about-the-white-houses-iot-security-labeling-effort/
[63] https://www.digicert.com/blog/iot-security-labels-by-spring-2023
[64] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

kulcsú ECC) algoritmusok gyorsan elavulttá válnak, és sok azokkal titkosított anyag gyorsabban visszafejthetővé válik.

Rövid lejáratú tanúsítványok: A Google a szervezeteket a 90-napos érvényességű tanúsítványok[65] használata felé tereli. Ez automatizálási lépéseket kíván majd az IT üzemeltetők részéről, de nyilvánvalóan javítja a webhelyek biztonságát. Várhatóan a többi szolgáltató is követni fogja az egyik legfontosabb piaci szereplőt a sűrűbb tanúsítványcsere periódusidők előírásában, bevezetésében.

Gyenge CA gyökértanúsítványok kivezetése: A Mozilla a következő években tervezi[66] a régi (kb. 15-18 éves) SSL/TLS és S/MIME gyökértanúsítványok visszavonását, mivel ezek a mai szigorú kriptográfiai követelményeknek már nem felelnek meg.

A **kódaláíró tanúsítványok**at végrehajtható állományok, meghajtóprogramok aláírására használják, így csökkentve annak a lehetőségét, hogy módosított, rosszindulatú kódot juttassanak a végfelhasználók eszközeire. Általában OV tanúsítvány segítségével történik az ellenőrzés. A CA/B fórum hatására 2023. júniusától[67] a tanúsítványok tárolására szigorúbb követelményeket írnak elő, ami sok esetben a meglevő hardverkulcs cseréjét követeli majd meg. Ez sok esetben körülményes lehet a szervezeteknél, ezért bizonyos szereplők a felhőalapú kódaláírás irányába fognak fordulni.

Új S/MIME alapkövetelmények: A CA/B fórum tagjai 2023. januárjában állapodtak meg az elektronikus levelezéssel kapcsolatos S/MIME tanúsítványok részletes iparági követelményeinek biztosításában[68], amely azóta érvénybe is lépett. A lépés a TLS és a kódaláíró tanúsítványok terén is történt lépésekkel vannak összhangban. Szabványosított tanúsítványprofilok alkalmazását jelenti, amely a különböző szoftverek közötti együttműködést javítja.

[65] https://www.globalsign.com/en/company/news-events/news/be-prepared-major-pki-changes-beginning-autumn-through-2024
[66] https://www.globalsign.com/en/company/news-events/news/be-prepared-major-pki-changes-beginning-autumn-through-2024
[67] https://cabforum.org/baseline-requirements-code-signing/
[68] https://cabforum.org/smime-br/

6 Személyközi kommunikációs megoldások

Az IP-alapú telefónia hegemóniája a kétezres évek eleje óta töretlen. A hagyományos, áramkör kapcsolt telefonhálózatok megszűnésével az IP-alapú, csomagkapcsolt hangátvitel uralja a személyközi kommunikációs megoldásos piacát mérettől és a felmerülő igényektől függetlenül. Ebben a fejezetben áttekintjük az IP-alapú hangszolgáltatások jelenlegi spektrumát, technológiai hátterét és szolgáltatásait, valamint kitekintünk a továbblépési lehetőségekre és a fejlesztési irányokra.
Az IP-alapú telefónia alkalmazási területei:

- **Privát telefonrendszerek IP-alapú hálózatok**on (pl. vállalati, irodai belső telefonrendszerek: Cisco UC, Avaya IP Office, 3CX)
- **Nyilvános kommunikációs szolgáltatások az interneten**:
    - Telefonszolgáltatás (pl. szabványos protokollokra épülő ingyenes és üzleti VoIP szoftverek és rendszerek: Ekiga, Linphone, Jitsi, 3CX, Zoiper, Ooma)
    - Üzenetküldő alkalmazások: Skype, Viber, WhatsApp, Discord, Facebook Messenger, Google Meet
    - Videókonferencia rendszerek: Teams, WebEx, Zoom
- **Hangszolgáltatás mobil távközlő hálózatokban** (VoLTE, VoWiFi, VoNR/Vo5G)

6.1 VoIP

A Voice over IP (VoIP) technológia lehetővé teszi, hogy IP-alapú hálózatokban, illetve a nyilvános interneten hang- és multimédia hívásokat bonyolítsunk le. A hívások két vagy több fél összekapcsolásával jönnek létre, mely összeköttetés lehet közvetlen IP-to-IP vagy IP-alapú telefonközpont (PBX) közreműködésével központilag vezérelt. A hagyományos telefóniához hasonlóan a VoIP rendszerek is rendelkeznek hívásvezérlő (jelzés) protokollal, amely jellemzően a széles körben elterjedt Session Initiation Protocol (SIP) vagy alternatívája a H.323. Bizonyos internetes VoIP szolgáltatások saját belső jelzési protokollt valósítanak meg, melyek – bár többnyire a SIP-ből származnak – nem kompatibilisek a szabványos SIP jelzéssel. A beszédhang és a médiatartalom átvitelére széles körben alkalmazzák a Real-time Transport Protocol-t (RTP), mely specifikus tulajdonságainak köszönhetően hatékony szállítást biztosít IP felett a médiafolyamok számára. A hanghívások egyedi követelményeket támasztanak az IP hálózattal szemben: alacsony késleltetés, késleltetés-ingadozás, valamint csomagvesztési arány. A médiacsomagok átvitelénél kulcsfontosságú a sorrendiség fenntartása, valamint a megfelelő ütemezés. Az IP hálózatok, illetve maga az IP protokoll hagyományosan nem nyújt garanciákat sem az átvitt csomagok vételi oldali helyes sorrendjére, sem az eredeti időzítési tulajdonságok fenntartására (csomagok érkezési időközére). Minden adatot, beleértve a médiaadatot is, best-effort módon továbbítanak az IP hálózatok, bárminemű garancia nélkül. Ahhoz, hogy az IP telefónia számára biztosítható legyen a megfelelő átvitelminőség, a szállítási protokollnak támogatnia kell a vételi oldali feldolgozást és dekódolást. Az RTP protokoll ennek megfelelően forrás oldalon minden kiküldött médiacsomagot egyedi szekvenciaszámmal lát el, ezzel az IP hálózaton az átvitel során bekövetkezett átrendeződéseket a vételi oldalon bizonyos korlátok között helyre lehet állítani a média dekódolása előtt. Ezen felül az RTP csomagok rendelkeznek időzítési információval is (egyedi időbélyeggel), mely támogatja a helyes ütemezést lejátszáskor. A

hálózati késleltetés ingadozását a vételi oldalon az ún. jitter-puffer alkalmazásával egyenlítik ki. Mindezek mellett fontos megjegyezni, hogy a nyilvános internet feletti hangszolgáltatások esetén mindig best-effort továbbításra számíthatunk, így a hangszolgáltatás minőségének megfelelő szintjéhez további adaptációs és korrekciós képességeket kell beépíteni a VoIP alkalmazásba. Ilyen képesség például az elasztikus vagy más szóval adaptív méretű jitter-puffer, illetve hibavédő kódolás alkalmazása a beszédhang kódolása során. A legkorszerűbb hangkódolók (pl. Opus) beépített hibavédő kódolást alkalmaznak, az Opus esetén a Forward Error Correction (FEC) algoritmust. Az adaptivitás további lehetősége, hogy hívás alatt az átvitel minőségének romlásakor a jelzésprotokoll segítségével alacsonyabb bitsebességű hangkódolóra vált a VoIP végpont (pl. szélessávú hangkódolóról keskenysávú kódolóra vált). Ezzel a csomagvesztésből kialakuló szaggatott beszéd mértéke jelentősen csökkenthető, tehát a hanghívás érzeti minőségét többé-kevésbé fenn lehet tartani. A korszerű hangkódolók (pl. AMR, AMR-WB, Opus, EVS) képesek a kimeneti média bitrátát dinamikusan hangolni, így elkerülhető az átviteli tulajdonságok romlása esetén a kodekváltás.
A nyilvános interneten működő, felhőalapú VoIP szolgáltatók jellemzően titkosítással továbbítják a teljes felhasználói forgalmat, beleértve a jelzést és a médiát. Emiatt a szolgáltatásban alkalmazott protokollok és kódolók meghatározásánál csak az általuk rendelkezésre bocsátott információkra hagyatkozhatunk.

Egy másik megközelítésben két nagy csoportra oszthatjuk a személyközi kommunikációs megoldásokat infrastrukturális szempontból:

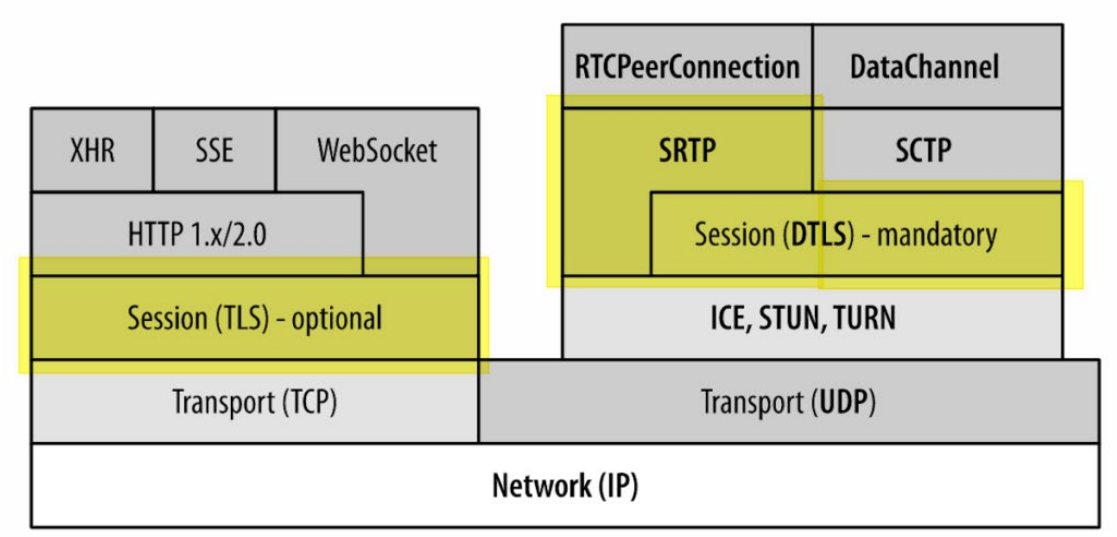
- **Menedzselt infrastruktúra** (pl. belső vállalati telefonrendszer, mobil távközlő hálózat)
- **Nem menedzselt infrastruktúra** (publikus internet)

Az első esetben a felhasználói készülékek közötti IP összeköttetést biztosító hálózat a szolgáltató üzemeltetésében van, vagy szolgáltatásminőségi megállapodást között az átviteli szolgáltatóval. Ebben az esetben a hangátvitelre vonatkozóan garanciákat várhatunk el a hálózattól. A fő kérdés az, hogy technológiailag milyen eszközök állnak egy hálózatüzemeltető rendelkezésére az átvitelminőségi, szolgáltatásminőségi garanciák megvalósításához. Az IP hálózatok best-effort átvitelét abban az esetben lehet garanciákkal kiegészíteni, ha az átmenő forgalmak a hálózat megfelelő pontjain megfelelő tulajdonságok alapján osztályozzuk és az így kialakult forgalmi osztályokhoz továbbítási prioritásokat rendelünk. Ennek megfelelően a végpontok közötti IP kapcsoló és útválasztó eszközök az előre definiált osztályokba tartozó forgalmakat már nem best-effort jelleggel, hanem prioritási sorokba rendezve fogja továbbitani. Ezzel statisztikai értelemben garanciát lehet kialakítani a csomagvesztésre és a késleltetésre kvázi függetlenül az adott összeköttetések forgalmi viszonyaitól. Így egy magas prioritású hangfolyam átvitelminőségét kevésbé fogja befolyásolni egy alacsonyabb osztály várakozási sorában kialakult torlódás.

6.2 WebRTC

A SIP-alapú VoIP technológia újgenerációs kibővítése, továbbfejlesztése a Google által kifejlesztett WebRTC projekt és API, mellyel webes böngészőkben, mindenfajta előzetes telepítés igénye nélkül nyújtható valósidejű videó- és hangkommunikációs szolgáltatás. A WebRTC megalkotásakor a valósidejű kommunikáció mellett a biztonság is nagy hangsúlyt kapott. Mivel a WebRTC technológiát a nyilvános interneten történő személyközi kommunikációhoz fejlesztették ki, a végpontok között minden esetben titkosított a jelzés és

média kommunikáció. Az implementáció nyitott, minden jelentős webböngészőben (Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Opera) elérhető integrált komponensként. A megoldás ezáltal hasznosítani tudja a böngészők erős és érett titkosítási funkcióit az átvitel során. Ez biztonsági szempontból komoly előny a korábbi tisztán SIP-alapú VoIP szolgáltatásokkal szemben, melyek gyakran gyártóspecifikus biztonsági megoldásokat alkalmaztak. Hasonlóan a klasszikus SIP-alapú VoIP megoldásokhoz, központi szerver nélkül, peer-to-peer üzemmódban is működőképes a technológia.



26. ábra WebRTC protokoll készlet

Korábban felmerült az az adatvédelmi kritika a WebRTC-vel szemben, hogy a kapcsolatfelépítési fázisban átadja a kliens lokális IP címét a másik félnek. Idő közben a WebRTC fejlesztői megtalálták a megoldást a fenti problémára, bevezették az mDNS-alapú végpontazonosítást a kommunikációs felek között. Ennek lényege, hogy a JavaScript kód nem fér hozzá a gép valódi lokális IP címeihez, mivel a böngésző kicseréli azokat véletlenszerűen generált mDNS címekre.

6.2.1 WebRTC kommunikáció címfordítással elérhető kliensek között (NAT traversal)

NAT mögötti kliensek esetén a WebRTC az ICE (Interactive Connectivity Establishment, RFC 5245) protokollt alkalmazza a médiakapcsolat kialakításához (lásd 26. ábra[69]). Az ICE protokoll összegyűjti a kliens lokális és ugró (relay, reflexív) IP címeit, melyeket SDP protokollon keresztül átküld a másik félnek. Ha mindkét fél megkapta a partner címeit, megkezdik a kapcsolódási teszteket. Ebben a fázisban a kliens médiaadatot kísérel meg továbbítani az átadott címekre, szisztematikusan végigjárva a lehetséges kapcsolódási címeket. A próbálkozása addig tart, amíg sikeres nem lesz a médiaátvitel vagy elfogynak a tesztelhető címek.

A kommunikációs végpontok közötti sikeres kommunikáció feltétele, hogy közösen elfogadott hang- és videókódolót alkalmazzanak a médiatartalom átvitelekor. A WebRTC technológiát megvalósító webböngészőkkel szemben az IETF RFC 7742 és RFC 7874 dokumentumok fogalmazzák meg a médiakódolás specifikus követelményeit (lásd 27. ábra[70]).

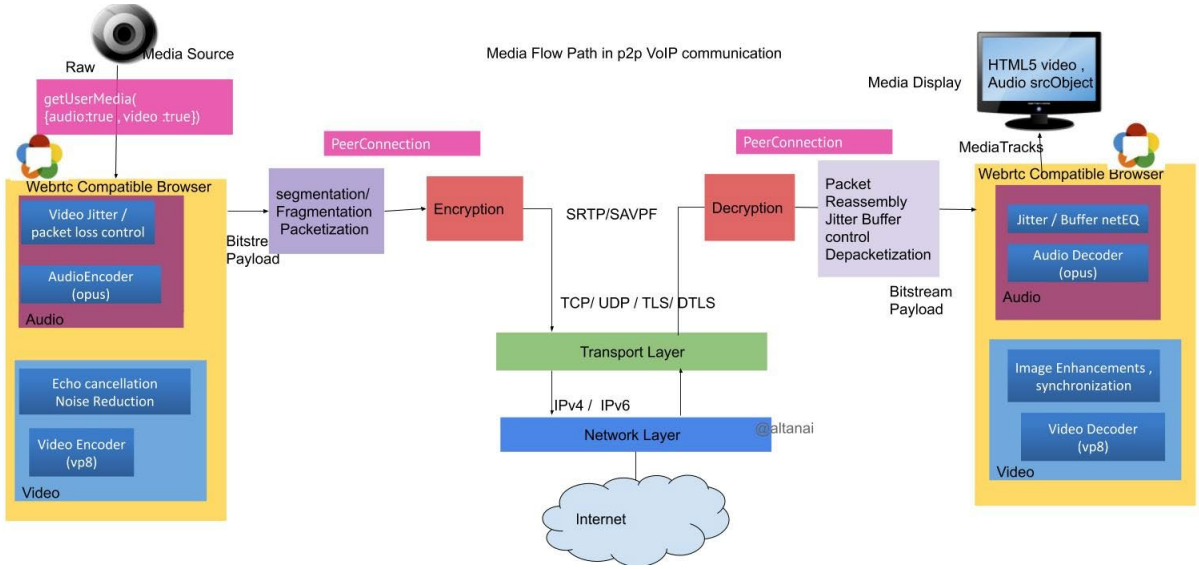
[69] https://bloggeek.me/is-webrtc-safe/

[70] https://telecom.altanai.com/2020/05/06/webrtc-audio-video-codecs/

A 3. táblázat sorolja fel, hogy a WebRTC-képes böngészőknek minimálisan mely kódolókat kell támogatniuk.

3. táblázat A WebRTC-képes böngészők számára szükséges kódolókészlet

Hangkodek	**Videókodek**
G.711 PCM (u-law és A-law)	VP8
Opus	VP9
iLBC (opcionális)	H.264 (MPEG-4 AVC)
iSAC (opcionális)	



27. ábra WebRTC végpontok közötti kommunikációs útvonal

A WebRTC technológia jellemző felhasználási esetei:

- Többrésztvevős videókonferencia
- Élő képernyőmegosztás
- Fájlmegosztás
- Beágyazott rendszerek videófunkciói
- Vásárlói ügyfélszolgálat
- Vészhelyzeti kommunikáció
- Távgyógyászat
- E-learning

A jelenleg legnépszerűbb WebRTC-alapú nyilvános kommunikációs szolgáltatások:

- Google Meet (Hangout) és Duo: videó- és hanghívások
- Facebook Live, Messenger, Instagram Live, Oculus (videó hívások VR szemüvegben), Workplace
- Discord: videójátékosok közötti valós idejű hangkommunikáció
- WhatsApp: videó- és hanghívások, üzenetek (a Facebook 2014-ben felvásárolta és integrálta számos szolgáltatásába, de jelenleg is elérhető önálló mobilapplikációként)
- Amazon Chime: videókonferencia hívások
- Snapchat: üzenetküldés
- ZenDesk: ügyfélkapcsolat

Egyértelmű tendenciaként megállapítható, hogy a WebRTC-re megjelenése óta folyamatosan növekvő számú személyközi kommunikációs szolgáltatás épül. A növekedési folyamat jelenleg is töretlenül zajlik. A fenti népszerű példákon túlmenően számos területspecifikus kommunikációs szolgáltatás használja a WebRTC technológiát az ügyfélkapcsolat, távgyógyászat, csoportmunka és e-learning területeken.
A legelterjedtebb videókonferencia rendszerek (Microsoft Teams, Cisco Webex, Zoom) opcionális lehetőséget adnak a kliensnek a WebRTC-alapú becsatlakozásra.
A komplett kommunikációs alkalmazásokon túlmenően elérhetőek olyan fejlesztői eszközök (pl. Webtrit SDK), amelyekkel egyedi igényeknek megfelelő kommunikációs alkalmazások készíthetőek.
A mobilalapú üzenetküldő alkalmazások népszerűsége mára már meghaladja a közösségi média szolgáltatásokét. Ezt a tendenciát felismerték a hirdetők is, lehetőséget látva abban, hogy olyan alkalmazáson keresztül érjék el a célközönségüket, amelyekkel napi szinten a legtöbb időt töltik.

6.2.2 Biztonsági kérdések

A WebRTC technológia a kezdetektől nagy hangsúlyt fektet a biztonságra. A teljes kommunikáció végponttól végpontig titkosított, beleértve a vezérlő és médiaadat csatornákat.
A fentiek ellenére számos biztonsági kérdést kell kezelni a kommunikáció során:

- A kamera és a mikrofon tartós hozzáférhetősége
- Akaratlanul megosztott privát információ a képernyőn (személyes és banki adatok, bizalmas dokumentumok stb.)
- Auto-answer opció használata DDoS támadáshoz
- Tűzfalak megkerülése TURN szerver használatával: jogosulatlan adatforgalmazás
- Felhasználó félrevezetése: képernyő szerint véget ért hívás a háttérben tovább küldi a felhasználó kamerájából és mikrofonjából származó valósidejű médiaadatot
- Beépített torlódásvezérlés hiánya miatt a kommunikációra felhasznált sávszélesség nincs korlátozva
- Webes böngészőkben jelenlévő klasszikus kockázatok: cross-origin resource sharing (CORS) elv helytelen használata, ismeretlen állomány letöltése a partnertől, rosszindulatú kódot tartalmazó oldalak meglátogatása

6.3 Ingyenes OTT hangszolgáltatások és mobilhálózati hangszolgáltatás

A VoIP technológia megjelenése és tömeges elterjedése óta a távközlési szolgáltatók hagyományosan számlázott hívásokból származó bevételei évről évre csökkennek. A kiesést egyéb szolgáltatások bevezetésével próbálták ellensúlyozni: internethozzáférés, IPTV és telefon integrált 3play szolgáltatásként értékesítve. Ennek ellenére létrejött egy gazdasági érdekellentét a fogyasztók és a távközlési szolgáltató között. Mivel a távközlési szolgáltató jellemzően a telefonszoltáltatás mellett internethozzáférés szolgáltató is, a kialakult helyzetet számos esetben tudatos használati korlátozásokkal próbálták megoldani. A 2000-es években nemzetközi szinten számos olyan eset látott napvilágot, amikor a szolgáltató tudatosan korlátozta bizonyos VoIP technológián alapuló ingyenes szolgáltatások elérhetőségét. Ebből a jelenségből kiindulva született meg az igény a semleges internethozzáférés jogi szabályozására. A hálózatsemlegesség jogi kereteit az Európai Unióban a 2015-ben

elfogadott Telecom Single Market (TSM) 2015/2120 rendelet adja. Ennek értelmében az internethozzáférés-szolgáltatónak mindenfajta megkülönböztetés nélkül kell kezelnie a felhasználó adatforgalmát, tekintet nélkül a felhasználóra, készülékére és az alkalmazott szolgáltatásra. Mára az OTT-alapú internetes VoIP szolgáltatások oly mértékben elterjedtek mind a lakossági, mind az üzleti felhasználók körében, hogy a hozzáférés korlátozása már nem kifizetődő a távközlési szolgáltatók számára. Ehelyett a mobilhálózaton elérhető hangszolgáltatás továbbfejlesztésével lehet versenyképes alternatívát kínálni a felhasználók felé.

6.4 Hangszolgáltatás mobil távközlő hálózatokban

6.4.1 Voice over LTE (VoLTE)

A Voice over LTE (VoLTE) egy IP-alapú csomagkapcsolt technológia, amely 4G LTE mobilhálózaton valósít meg kommunikációs szolgáltatást az IP Multimedia Subsystem (IMS) alrendszer felhasználásával. Az IP hálózat lehetővé teszi, hogy a VoLTE szolgáltatás a multimédia információt adatként továbbítsa a felhasználók között, a klasszikus áramkörkapcsolt infrastruktúra használata nélkül. Napjainkra a legtöbb mobil operátor bevezette a VoLTE szolgáltatást az LTE hálózatokban. Az IMS valójában egy önálló, az LTE hálózattól független rendszer. A két hálózat specifikus interfészeken kapcsolódik egymáshoz. Az LTE hálózat számára a hívás vezérlő és média forgalma is felhasználói forgalom. A hívásjelzés és a médiaadat előre definiált QoS prioritással kerül továbbításra az LTE hálózaton. A QoS menedzsment biztosítja, hogy torlódott rádiós és maghálózat esetén is megfelelő legyen a VoLTE szolgáltatás minősége. Tulajdonképpen az LTE hálózat megfelelő QoS menedzsment mellett összekapcsolja a felhasználói készüléket az IMS rendszerrel. Fontos megjegyezni, hogy az IMS egyéb hozzáférés-típusokat is támogat: pl. WiFi, vezetékes (lásd 28. ábra[71]).

Az IMS rendszerben a VoLTE szolgáltatáshoz felhasznált protokollok és kodekek a 4. táblázatban láthatók.

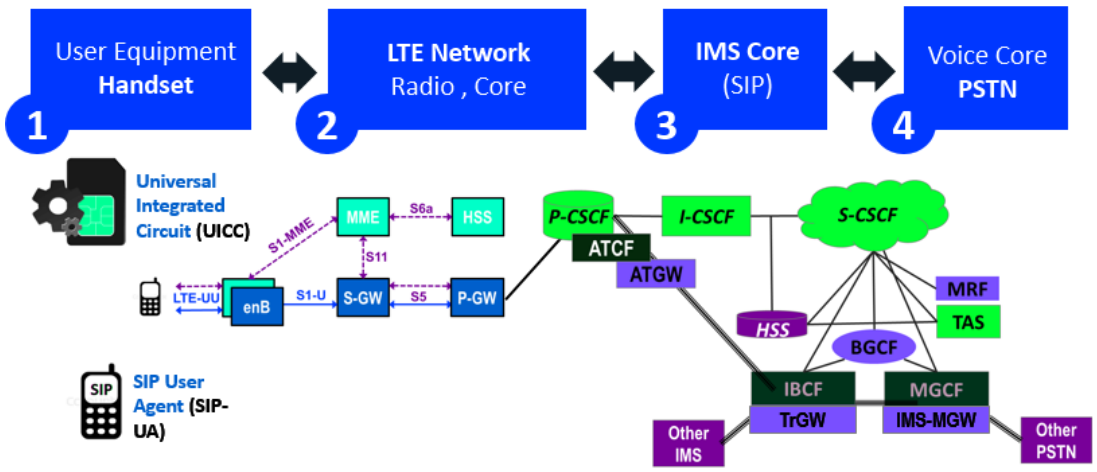
4. táblázat Az IMS rendszerben a VoLTE szolgáltatáshoz felhasznált protokollok és kodekek

Jelzés (vezérlősík)	Session Initiation Protocol (SIP), Session Description Protocol (SDP)
Média (adatsík)	Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP)
Hangkódoló	AMR-WB, AMR-NB (kompatibilitás), EVS

A VoLTE technológia előnyei az internetes OTT VoIP szolgáltatásokkal szemben:

- Menedzselt infrastruktúra végponttól végpontig
- Jobb szolgáltatásminőség
- Nagyobb megbízhatóság és rendelkezésre állás
- Egyidejű adat és hangkommunikáció (Single Radio Voice Call Continuity)
- Egyszerűbb hálózatmenedzsment

[71] https://www.telecomtutorial.info/post/volte-ims-architecture



28. ábra A VoLTE-IMS architektúra

6.4.2 5G Voice over New Radio (VoNR)

A VoNR egy 5. generációs (5G SA) mobilhálózaton megvalósított IP-alapú hangszolgáltatás, mely továbbra is az IMS alrendszerre épül. Tekinthető a VoLTE szolgáltatás továbbfejlesztésének. A felhasználói végberendezés és az IMS rendszer között az LTE helyett felhőalapú 5G rádiós és maghálózat biztosítja az összeköttetést.
A VoNR előnyei a VoLTE-val szemben:

- Gyorsabb hívásfelépítés az 5G hálózat alacsony késleltetése miatt
- Magasabb hangminőség (superwideband kódolók támogatása, f_s>16kHz, pl. EVS, Opus)
- Hatékonyabb QoS menedzsment és nagyobb átviteli kapacitás az 5G hálózaton

Ami viszont hiányzik a VoNR-ből: hívás alatt váltás korábbi, áramkörkapcsolt technológiára.
A teljes értékű 5G SA hálózatokban az IMS alrendszer is felhő alapokon kerül megvalósításra, hasonlóan az 5G maghálózathoz.

A VoLTE és a VoNR szolgáltatási konfigurációkat az 5. táblázat összegzi.

5. táblázat VoLTE és VoNR Szolgáltatási konfigurációk

VoLTE	4G: LTE RAN + LTE EPC + IMS
	5G NSA: 5G NR + LTE EPC + IMS
VoNR	5G SA: 5G NR + 5G core + IMS

6.5 A személyközi kommunikáció jövője

A lehetséges fejlődési irányok meghatározásához érdemes szétválasztani a lakossági és az üzleti célú kommunikációs szolgáltatásokat. A távközlési gyártók az IMS rendszer továbbfejlesztésében olyan lehetőségeket látnak, melyek segítségével jelentős értéknövelés valósítható meg a VoNR-alapú kommunikációs szolgáltatásokban. Az új funkciók megvalósításának az a nemtitkolt szándéka, hogy a vállalati, üzleti ügyfeleket számára vonzóbb alternatívát kínáljanak a fizetős OTT VoIP szolgáltatásokkal szemben. Ezzel párhuzamosan a WebRTC technológia további térhódításának és az 5G mobilhálózatok adatforgalmi képességeinek köszönhetően a VoIP szolgáltatások is jelentős tovább fejlődés

előtt állnak. A fentiekből megállapítható, hogy a VoLTE és VoIP technológiák közötti verseny tovább erősödik, mely verseny közvetlenül kapcsolódik ahhoz az élénk nemzetközi szakmai vitához, mely arról szól, hogy a tartalom és alkalmazás szolgáltatók (Content and Application Provider – CAP) hozzájáruljanak-e és milyen módon a mobil operátorok és internetszolgáltatók által épített és működtetett infrastruktúrák költségeihez.

Aktuális és várható jövőbeni trendek a VoIP szolgáltatásokban:

- Mesterséges intelligencia integrációja: szolgáltatásminőség biztosítása, hatékony ügyfélszolgálat
- Felhőalapú VoIP: skálázhatóság, dolgozói mobilitás
- Videókonferencia további terjedése az üzleti kommunikációban
- Specifikus üzleti alkalmazások integrációja: CRM, projekt menedzsment, marketing automatizációs megoldások
- Megnövelt biztonság
- Hangminőség és beszédérthetőség javítása
- Unified Communications: email, hang-, videó- és üzenetküldési funkciók egy platformon
- Előfizetői igényekhez hatékonyan testre szabható funkciók: egyedi hívásútvonalak, köszöntőszövegek, együttműködési képesség egyéb VoIP megoldásokkal
- Megnövelt felhasználói élmény (User Experience)

VoLTE globális előrejelzés

- Legfontosabb globális operátorok: AT&T Inc., Verizon Wireless, Vodafone Group PLC, Bharati Airtel Limited and Bell Canada
- Legnagyobb piac: Észak Amerika
- Leggyorsabban növekvő piac: Kelet Ázsia
- Várható globális növekedés: 50,3% CAGR (2023-2028)[72]

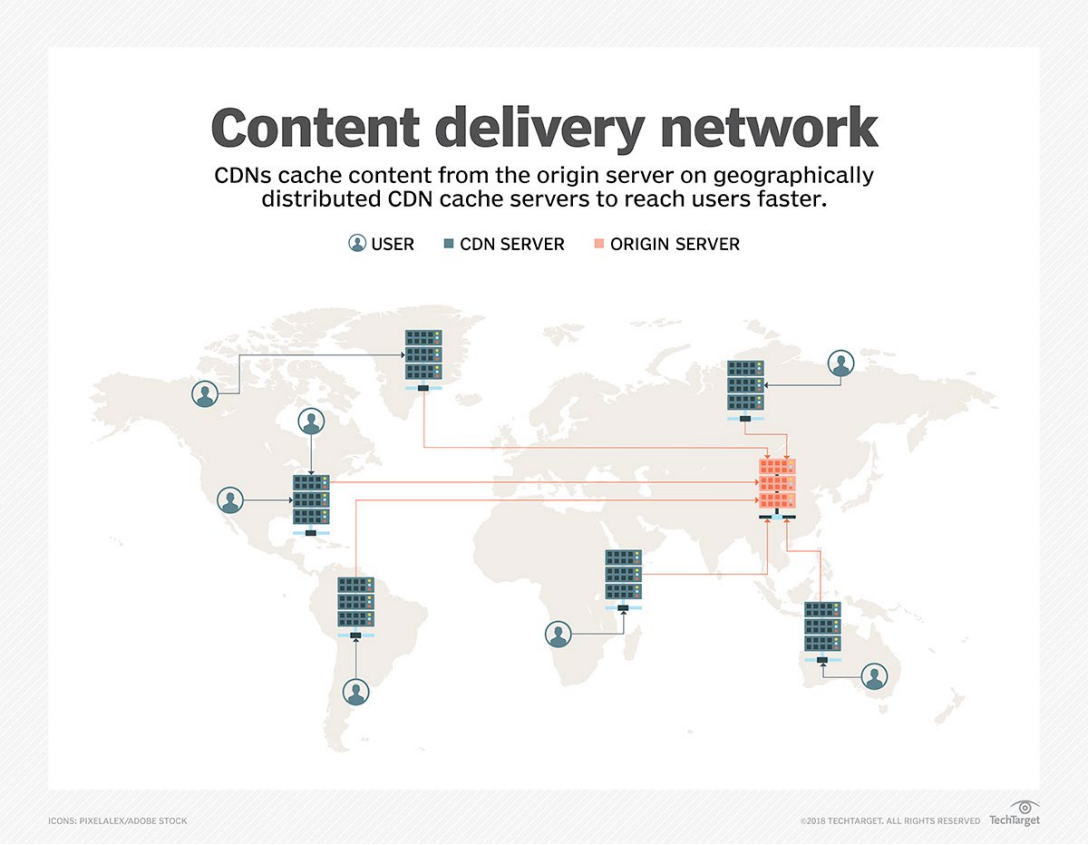
[72] https://www.mordorintelligence.com/industry-reports/voice-over-lte-market

7 Tartalmak gyorsítótárazása

Az online szolgáltatások felhasználói élményéhez hozzájárul a kapcsolódó tartalmak betöltési ideje. A gyorsítótárazás az útvonal több pontján is végezhető. A következő fejezetek a tartalomszolgáltatókkal együttműködő átfedőhálózatokkal, valamint a webszerveren implementálható gyorsítótárazási lehetőségekkel foglalkoznak.

7.1 Tartalomszolgáltató hálózatok[73]

A tartalom betöltési ideje jelentősen csökkenthető, ha olyan adatközpontból szolgálható ki a kérés, amely a felhasználóhoz képest kis késleltetéssel és viszonylag nagy átviteli sebességgel elérhető. A Content Delivery Network (CDN) szolgáltatók olyan átfedő hálózatokat képeznek, amelyek képesek gyorsítótárazni az elsősorban publikus, nagy tömegek által letöltött tartalmakat (lásd 29. ábra[74]). A pozitív hatás nemcsak a felhasználó oldalán jelentkezik a jobb felhasználói élményben, hanem a szolgáltató számára is kedvezőbb, ha ezáltal csökkentheti a szolgáltatásához kapcsolódó közvetlen adatforgalmi volument.

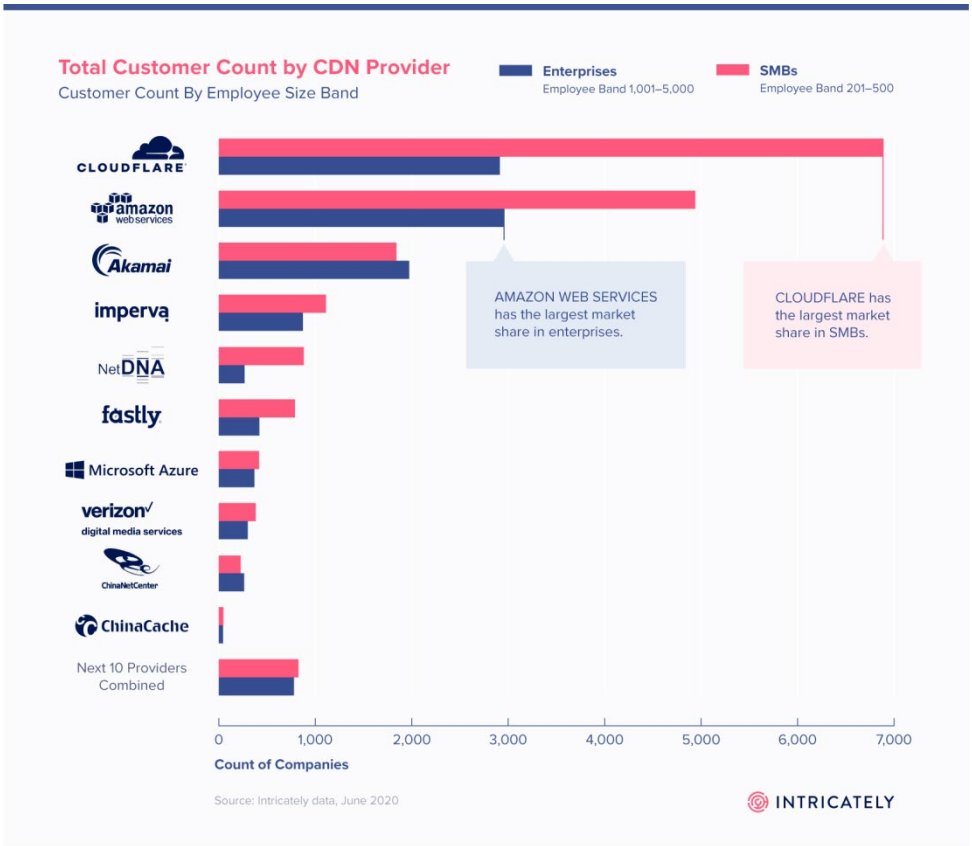


29. ábra A globális CDN hálózat architektúrája

[73] https://w3techs.com/technologies/overview/content_delivery
[74] https://www.techtarget.com/searchnetworking/definition/CDN-content-delivery-network

7.1.1 Legfontosabb szereplők és teljesítménymutatóik

Az igazán jelentős szolgáltatók globális hálózattal és sok adatközpontban vannak jelen. Az ügyfelek számát tekintve 10 legnagyobb CDN szolgáltatót a 30. ábra[75] mutatja be. Nem véletlen, hogy a szereplők egy része felhőszolgáltatóként is jelen van a piacon.



30. ábra A legtöbb ügyféllel rendelkező CDN szolgáltatók 2020. júniusában

Az egyes CDN típusok és szolgáltatók közötti választás az alkalmazás architekturális igényein, az elérni kívánt felhasználói körön és a szolgáltatás költségigényén múlik. A piacvezető a legszélesebb tartalomkészítői réteg számára nyújt jó ár/érték arányú szolgáltatást. Egy újonnan belépő tartalomkészítőnek viszont már az induláskor és később is mérlegelnie kell, hogy adott az adott tartalom forgalmi volumene mellett mely CDN-t érdemes választania. Nem minden esetben lesz számára optimális választás a piacvezető szolgáltatása.

A CDN szolgáltatás mérése felhasználói statisztikák alapján történhet és a medián HTTP válaszidő alapján célszerű rangsorolni (lásd 31. ábra[76]).

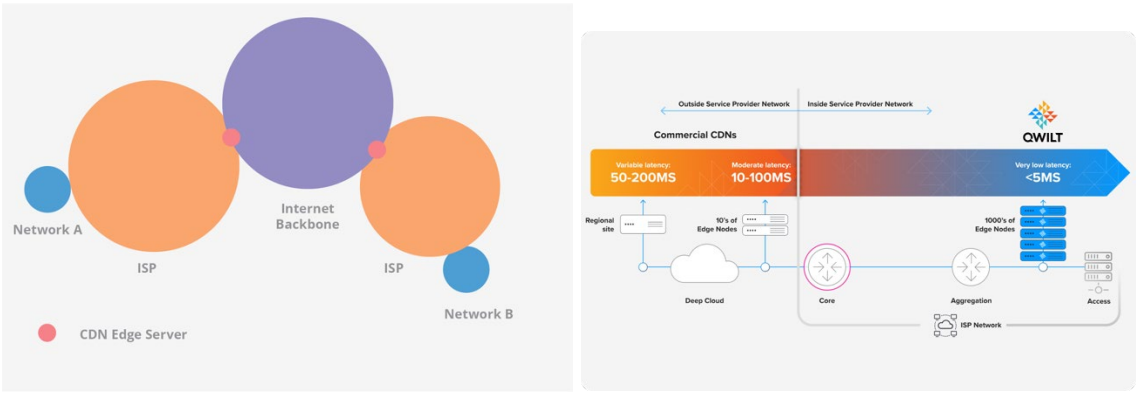
[75] https://blog.intricately.com/cdn-industry-trends-market-share-customer-size
[76] https://www.cdnperf.com/

31. ábra CDN szolgáltatások rangsorolása válaszidő alapján, magyarországi lekérdezések mintái alapján, 2023. október 2-i állapot

7.1.2 CDN kategóriák

A publikus tartalomszolgáltatók széleskörű szolgáltatást nyújtanak különféle online tartalmak kiszolgálására (hírportálok tartalma, website-ok (pl. javascript) építőelemei, stb.). A publikus CDN szolgáltatókon túl további CDN hálózatok is léteznek. A fejezet ezeket foglalja össze.

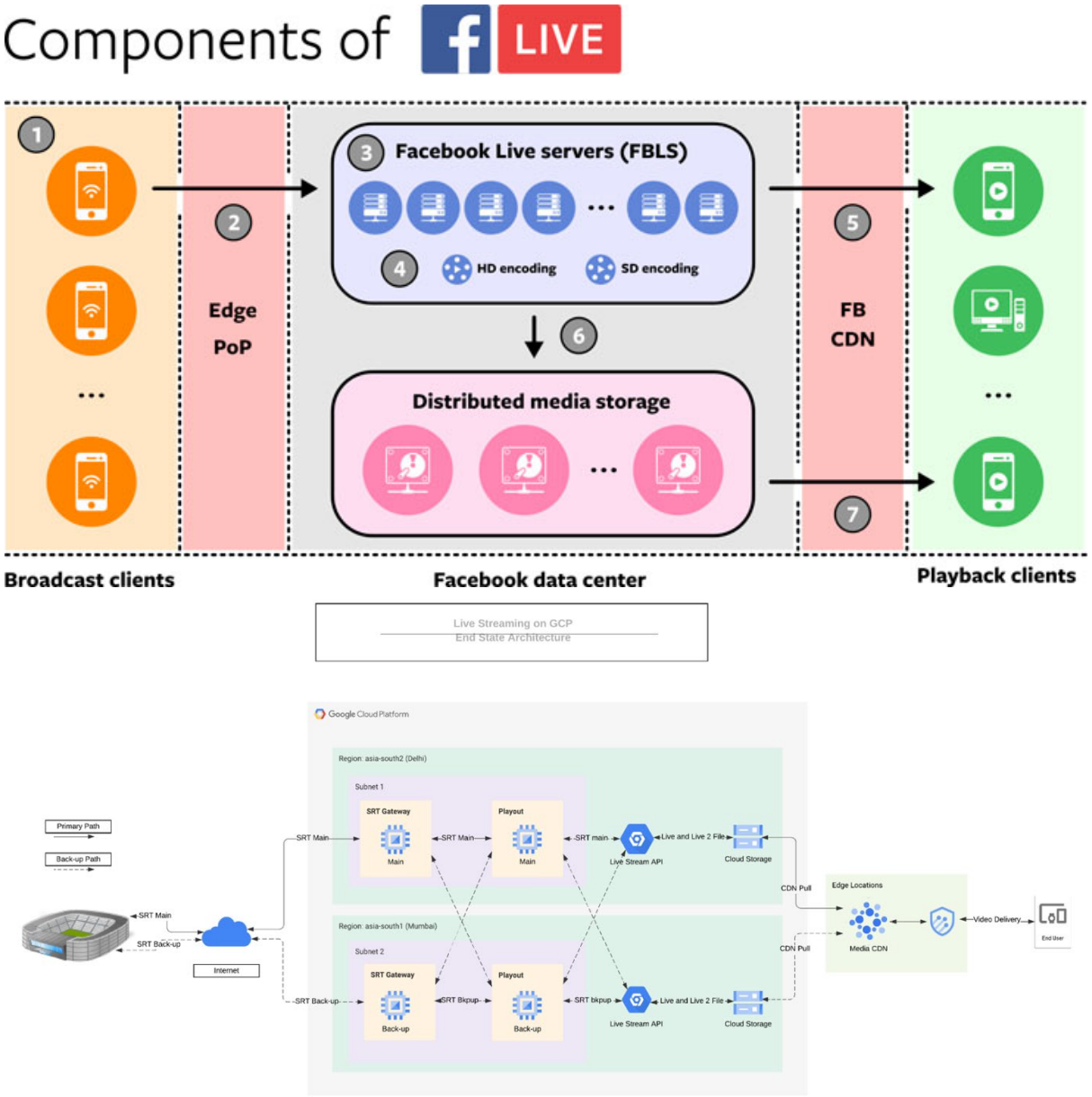
Edge CDN: Nagyobb ISP-knél, CSP-knél CDN csomópontokat helyeznek ki, hogy a tartalom a végfelhasználókhoz minél közelebb váljon elérhetővé. Előnyei a tovább csökkentett elérési idő és kisebb szolgáltatón kívüli adatforgalom (lásd 32. ábra[77]).



32. ábra A CDN edge szerverek helye és a kiszolgálás előnye

[77] https://www.cloudflare.com/learning/cdn/glossary/edge-server/ és https://www.airtel.in/business/b2b/edge-cdn

Privát CDN: A publikus CDN-eket egy CDN operátor üzemelteti és jellemzően forgalmi volumen alapján számlázzák a szolgáltatást az egyéb szolgáltatók felé. Ha ez a forgalmi volumen nagyon megugrik, a CDN szolgáltatás költsége is elszállhat. Ezért, ha nagy mennyiségű tartalmat kell eljuttatni a fogyasztókhoz (pl. videóstream), akkor gazdaságosabb lehet a privát CDN kiépítése. Ehhez természetesen be kell ruházni hardver és szoftver tekintetében is, de hosszú távon megtérülhet.

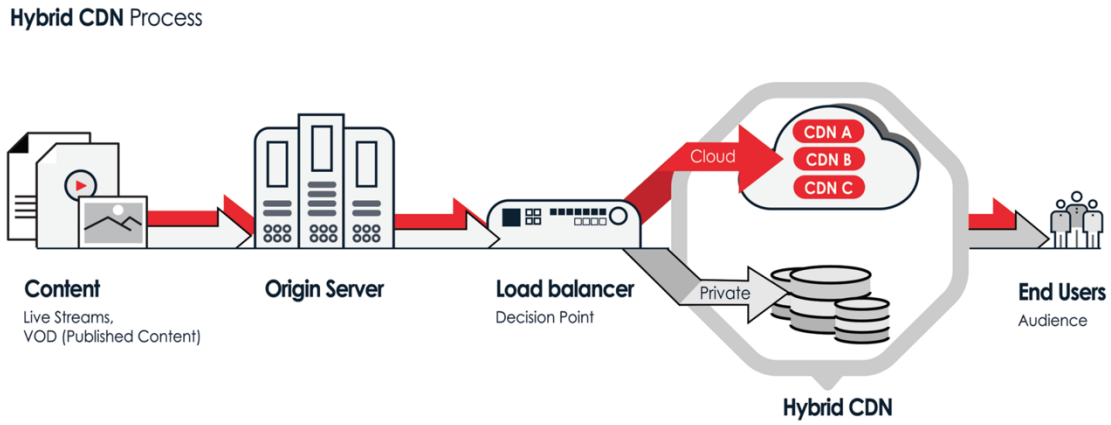


33. ábra A Facebook Live és a Google/Youtube Live Streams streaming CDN architektúrája

A Meta és a Google is saját terjesztőhálózatot alkalmaz, többek között az élő közvetítések továbbításához is. Természetesen ez esetekben a feladatot még összetettebbé teszi az élő

forrásból történő közvetítés. A kódolt tartalom osztott tárhelyekre kerül, onnan pedig média CDN-ek segítségével történik a továbbítás (lásd 33. ábra[78]).

Multi vagy hibrid CDN[79]: A gyakorlatban sok szolgáltató többféle CDN megoldást használ egyidejűleg. Például a szöveges vagy képi tartalmakat publikus CDN segítségével, míg a videó tartalmakat saját, privát infrastruktúra vagy privát CDN segítségével juttatja el a fogyasztókhoz. Hasonló megoldást szemléltet a 34. ábra[80] is. Ezzel az architektúrával javíthatja a skálázhatóságot, diverzifikálja a szolgáltatásoktól való függést és költséget is lehet optimalizálni.

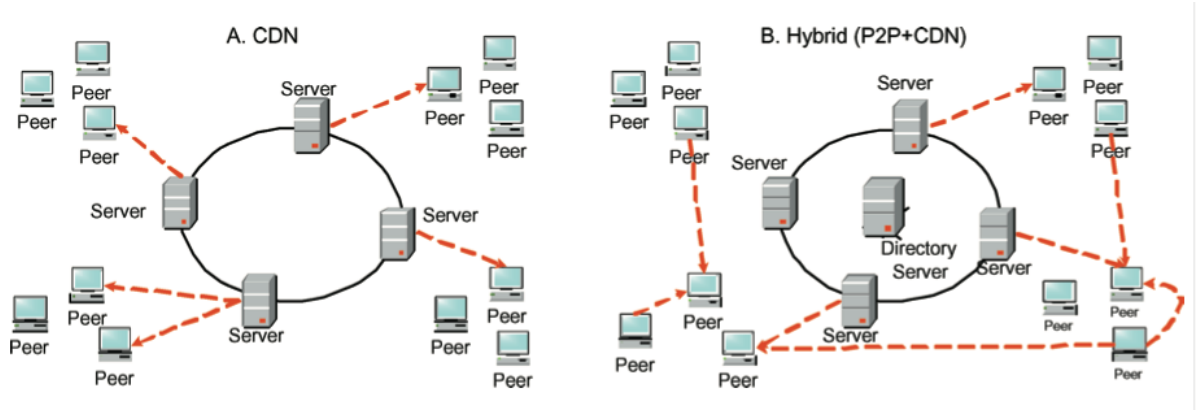


34. ábra A hibrid CDN architektúra felépítése

Peer-to-peer CDN: A hagyományos kliens-szerver megoldással szemben az adott tartalmi elemeket itt a lekérő kliensek további kliensek számára is továbbadhatják. A kliensek számával így elviekben jobban tud skálázódni a szolgáltatás, és ezáltal a fenntartási költségek is csökkenthetők. Különösen hatékony igény szerinti videó (video on demand, VoD) tartalmak esetén. A működésük alapja rendszerint valamilyen, a bittorrenthez hasonló elosztott blokkátviteli megoldás. Igazán hatékonyan hibrid formában tud működni: a tartalmak „korai" elterjesztéséért CDN hálózat felel és a kliensek később már egymástól is képesek lesznek tölteni a tartalom darabjait. Architekturális elrendezését a hagyományos CDN-ekhez képest a 35. ábra[81] mutatja be. Működésük ezáltal összetettebb is, ezért a magas szolgáltatásminőséghez jól felépített modell kell. Ezzel együtt nehezebb is a kézben tartása. Ráadásul az ISP-k peer-to-peer jellegű forgalom lassítása is ronthatja a helyzetet.[82] A Proactive network Provider Participation for P2P (P4P) megközelítés a P2P csomópontok regionális csoportosítását segíti, amely segíti az azok közti kapcsolódást és alacsony késleltetést, valamint az ISP hálózatából kifelé irányuló forgalmat is minimalizálhatja.

[78] https://engineering.fb.com/2018/02/12/production-engineering/how-production-engineers-support-global-events-on-facebook/ és https://cloud.google.com/blog/products/networking/hosting-successful-live-events-with-google-cloud
[79] https://www.mlytics.com/blog/ultimate-video-streaming-solution/
[80] https://www.linkedin.com/pulse/what-private-cdn-how-can-help-ott-industry-serkan-sevim
[81] https://www2.cs.sfu.ca/~mhefeeda/Papers/tomccap05.pdf
[82] https://medium.com/@ppio/the-importance-of-p2p-for-content-delivery-and-why-ppio-offers-the-best-solution-f75cee2b4fe

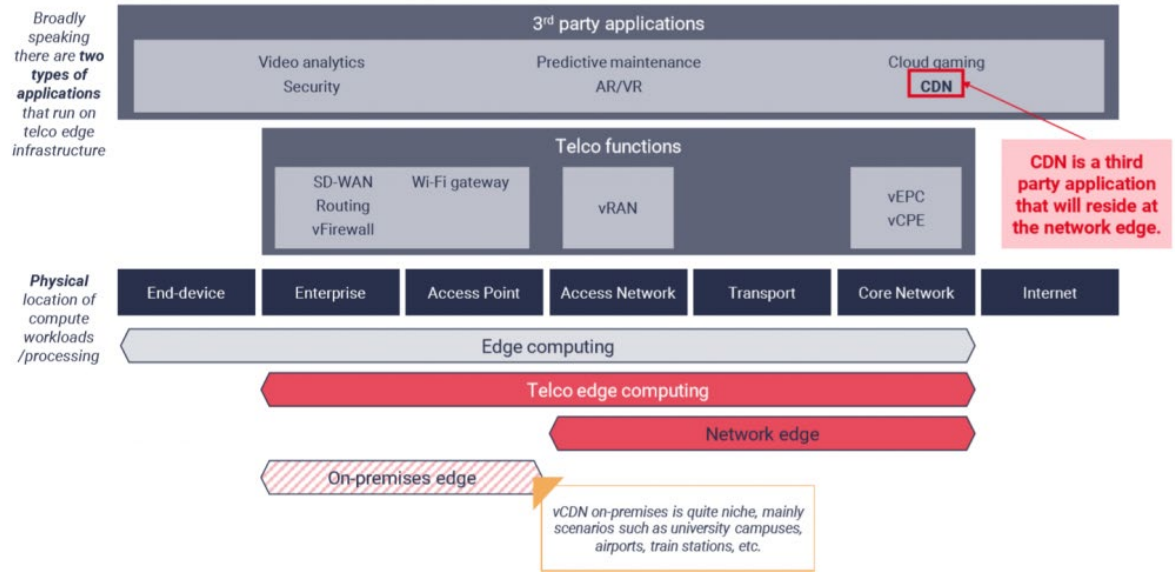
Kifejezett szolgáltatásként nem létezik, de privát CDN-ekben minden bizonnyal alkalmazzák a technológiát.



35. ábra A hagyományos CDN és hibrid CDN+P2P architektúrák összehasonlítása

Az Interplanetary File System (IPFS)[83] tekinthető egyfajta CDN-alternatívaként, mivel egy decentralizált P2P HTTP kiszolgálást valósít meg, de az átviteli teljesítmény nem elsődleges fókusz, ezért a CDN-ekkel valószínűleg egy ideig nem is lesz versenyképes.

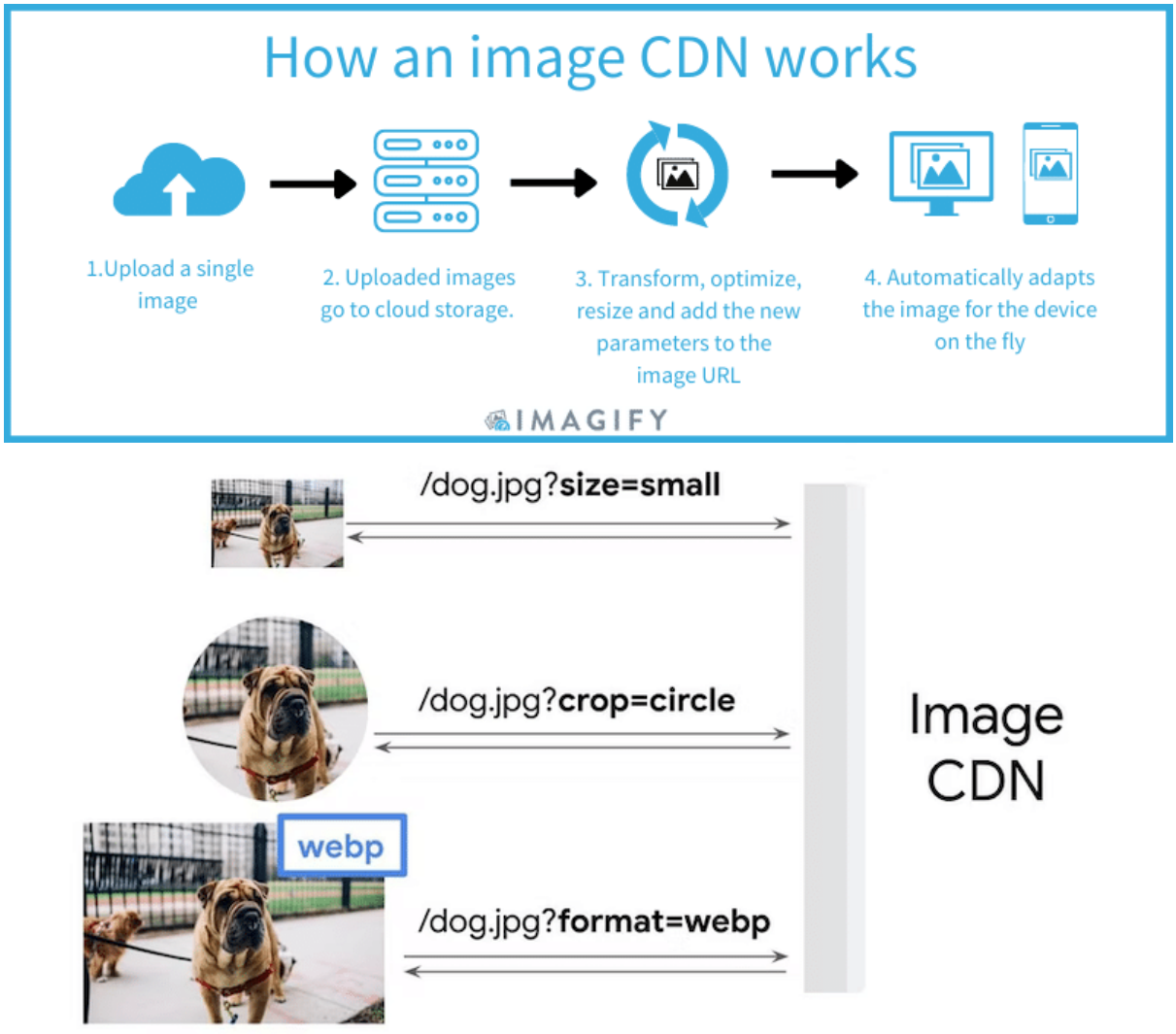
Virtuális CDN (vCDN): A hálózati funkciók virtualizációjához hasonlóan a CDN szolgáltatás is virtualizálható. Ily módon az edge CDN-hez hasonlóan a végfelhasználó közelébe vihető, akár szoftvermodulként is elhelyezhető. Jelentősége a Mobile Edge Communication (MEC) területén nagy, ahol a hálózat peremén új alkalmazásként jelenhet meg, mint ahogy a 36. ábra[84] bemutatja. Ott egy CSP szolgáltatásai felett nyújtott harmadik fél alkalmazásai között jelenik meg.



36. ábra Virtuális CDN szolgáltatás a hálózat peremén

[83] https://ipfs.tech/
[84] https://stlpartners.com/articles/edge-computing/cdn-what-is-edge-cdn-and-virtual-cdn-vcdn/

Média CDN (pl. képekhez: image CDN)[85]: Nem feltétlenül külön CDN hálózat, hanem jellemzően egy szolgáltatás a meglevő CDN hálózaton. A különböző felhasználói eszközökre különböző felbontásban vagy kódolással célszerű eljuttatni a médiatartalmakat (leginkább a képeket). Ehhez sokszor átkódolásra van szükség. Ezt a feladatot végzi el, az API nyújtotta esetleges egyéb képtranszformációs feladatokon keresztül, ahogy a 37. ábra[86] szemlélteti.



37. ábra A képi CDN architektúrája és működése egy példán keresztül

Természetesen létezik audiovizuális (A/V) tartalmak terjesztésére is ilyen jellegű szolgáltatás[87].

7.1.3 Technológiai kihívások

A CDN-ek alapvetően kvázi statikus (vagyis elsősorban geográfiai régió alapján különböző) tartalom gyorsítótárazásában jók, de napjainkban sok oldal tartalmát teljesen dinamikusan

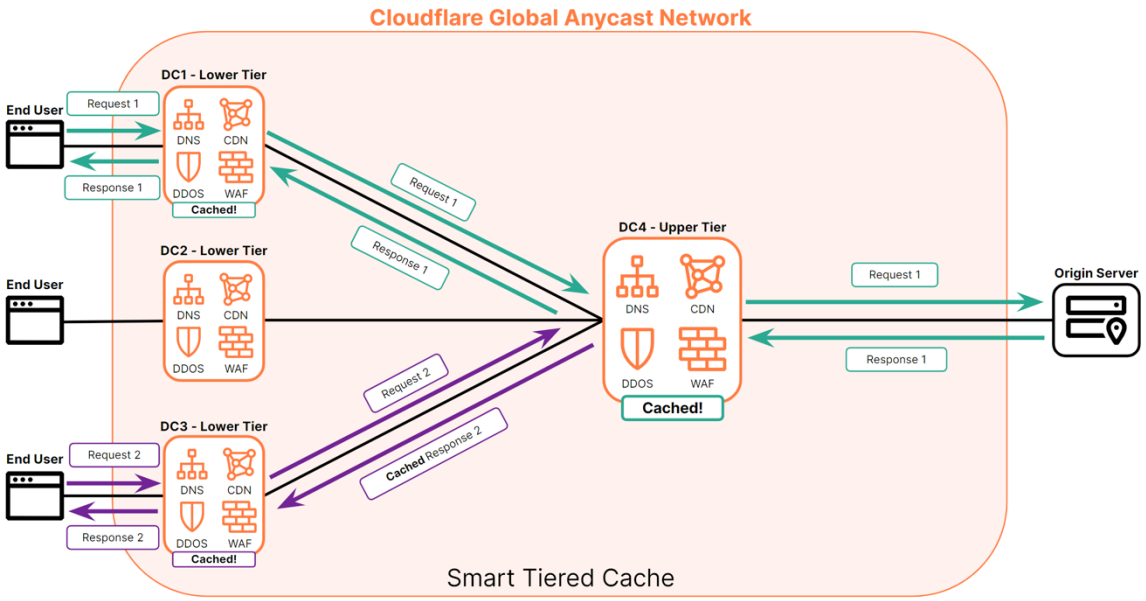
[85] https://blog.scaleflex.com/top-10-image-cdns-in-2023/
[86] https://imagify.io/blog/what-is-an-image-cdn/
[87] https://www.dacast.com/blog/content-delivery-network-cdn-providers-live-streaming/

állítják elő. Az Edge Side Includes (ESI)-t már 2001-ben eljuttatták a W3C-hez[88], az Akamai pl. implementálta, de azóta sem fogadták el. Ennek okai valószínűleg a korlátozott képességei, komplexitása és relatív lassúsága[89].

A CloudFlare a RailGun weboptimalizálóját kínálta a dinamikus tartalmak CDN-es kiszolgálására. Mivel az infrastruktúrája (mind a hálózat méretét, mind hardver és szoftver erőforrásait tekintve) sokkal kiterjedtebb és fejletteb lett, így a RailGun szolgáltatás alkalmazása már nem indokolt, karbantartása felesleges erőforrásokat von el, így kivonja azt[90].

A hatékony, alacsony késleltetésű kiszolgálás azon is múlik, hogy a kliens kérése valóban a tőle leggyorsabban elérhető adatközponthoz és kiszolgálóhoz jut-e el. Az első lépés a klienstől induló DNS lekérdezés. A hagyományosan 512 bájtban limitált DNS hasznos adatteher méret miatt a kliens nem tud a lekérdezésben elhelyezni erre vonatkozó információt. Az EDNS0 kiterjesztés lehetővé teszi ennek túllépését. A kliensnek saját IP címét adatvédelmi okokból nem célszerű felfednie, így az a DNS lekérdezésében saját IP alhálózatát is elhelyezheti[91]. A szabvány úgy lett kidolgozva, hogy visszafele kompatibilis legyen az EDNS-t nem támogató feloldókkal is.

Az alacsony késleltetés elérését célozza a globális anycast hálózati architektúra alkalmazása is, amelyet a CloudFlare használ. Ennek sémáját az 38. ábra[92] mutatja be. Olyan hálózati útvonalválasztási módszer dolgozik mögötte, amelynél egy adott IP cím mögött több csomópont is lehet. A kliens a tartalmat irányába a leggyorsabban kiszolgálni képes szerverrel fog kommunikálni. Ezt a kiválasztást a felhő globális architektúrája transzparensen biztosítja.



[88] https://www.w3.org/TR/esi-lang/
[89] https://www.keycdn.com/support/edge-side-includes
[90] https://blog.cloudflare.com/deprecating-railgun/
[91] https://engineering.salesforce.com/why-is-edns-important-for-content-delivery-85f5690744ba/
[92] https://developers.cloudflare.com/reference-architecture/cdn-reference-architecture/

38. ábra A CloudFlare globális anycast hálózatának sémája

7.1.4 Biztonsági kérdések

A CDN-ek adatokat is gyűjtenek a kiszolgált végfelhasználókkal kapcsolatban. Globális kiterjedésű hálózatuk révén nagy mennyiségű adatról van szó, az összegyűjtött adatokat igyekeznek is értékesíteni. Az EU-ban érvényben levő szigorú adatvédelmi szabályzások korlátozzák ezt, pl. az IP cím már személyes adatnak minősül. A weboldalak jellemzően valamilyen hozzájárulás kezelő szolgáltatást alkalmaznak, hogy a felhasználó engedélyét kérjék ehhez. Viszont ezek megjelenítéséhez is rendszerint scriptek, betűtípusok, képek szükségesek, amelyeket szintén a CDN-ekről kellene betölteni. 2021-ben a CookieBot nevű hozzájáruláskezelőről derült ki, hogy nem akadályozta meg, hogy a felhasználók IP címei eljussanak az Akamai CDN-hez, ami GDPR sértésnek bizonyult.

Megszokott, hogy a weboldalakon alkalmazott javascript kódokat CDN-eken keresztül kapja a végpont. Hogy a weboldal készítője bizonyos lehessen abban, hogy valóban a megfelelő kódot töltötte le a kliens, a kód Subresource Integrity (SRI) ellenőrzőösszegét (hash) is megadhatja. Így az ezt támogató böngésző a hash-t leellenőrizheti, bár az optimális működés érdekében a hash-eket a weboldal karbantartójának naprakészen kell tartania. A HTTP referer fejléc használata viszont adatszivárgást okozhat, mivel összekapcsolható a meglátogatott oldal, a felhasználó IP-címe és böngésző ujjlenyomatával, vagy akár a fizetést lebonyolító szolgáltatóval is, ha az ahhoz szükséges scriptet egy online fizetés előtt töltik be[93].

Természetesen egy publikus CDN szolgáltatót is érhet DDoS támadás, vagy egyéb technikai okból is felléphet szolgáltatáskiesés. Ezek ellen védhet egy megfelelően felépített multi CDN háttér. A másik lehetőség, ha a szolgáltatás elé fordított proxy-t tesznek. Ez megoldható a CloudFlare, Fastly stb. szolgáltatók ilyen típusú szolgáltatásával, ami sok esetben olcsóbb is lehet a CDN szolgáltatás használatánál.

7.1.5 Trendek

Information-centric networking (ICN)[94]: Új paradigma, ami során a jövőben a csomópontok közötti kommunikáció helyett arra kellene törekedni, hogy az útvonal eszközei transzparens módon képesek legyenek az információ tárolására, függetlenül annak típusától. Jelenleg az IRTF ICNRG munkacsoport[95] foglalkozik a témával, talán a távolabbi jövőben jelenhetnek meg a konkrét implementációk.

Content-centric Networking (CCN)[96]: Egyfajta ICN megközelítés. Minden hálózati csomópont célszerűen rendelkezzen információ tárolási lehetőséggel, képességgel is. Így nem feltétlenül lenne szükség az információt lehívni az azt koncentráltan tároló adatközpontokból, hanem akár jóval közelebbről is elérhető lenne. IP csomópontok elérése helyett nevesített adatcsomagokat (interest packets) tárolnának az egyes csomópontok és ezek nevére történő

[93] https://httptoolkit.com/blog/public-cdn-risks/
[94] https://www.tandfonline.com/doi/full/10.1080/23311916.2023.2210000
[95] https://irtf.org/icnrg
[96] https://www.cablelabs.com/wp-content/uploads/2016/02/Content-Delivery-with-Content-Centric-Networking-Feb-2016.pdf

hivatkozással volnának lehívhatók. Implementáció is készült (ugyan nem proof-of-concept szintű), a kódbázist a Cisco szerezte meg. Az utóbbi években nem történtek jelentős fejlemények, így várhatóan egyelőre nem alakítja át a tartalomszolgáltató hálózatok világát.

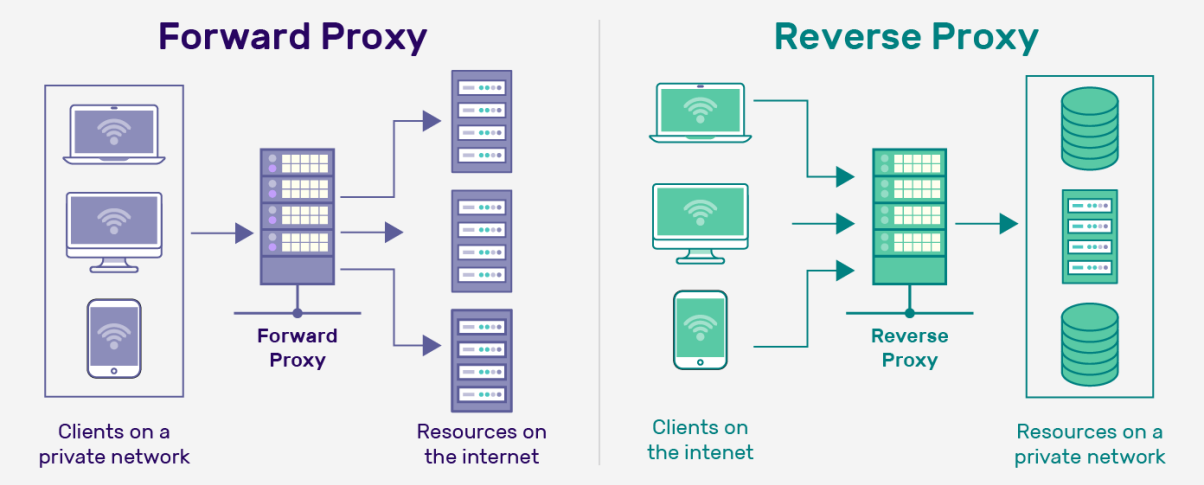
Szövetségi CDN és Open Caching[97]: Még 2011-ben indult egy Operator Carrier Exchange (OCX) kezdeményezés, amely ISP-k hálózatára épített CDN-ben gondolkodott. Később a StreamingMedia indított egy Open Caching szövetséget, hogy a szolgáltatók összekapcsolhassák a gyorsítótáraikat. Ezáltal (jellemzően a) streamelhető tartalmak az ISP-knél gyorsítótárazódnának és csökkenthető lenne a hagyományos CDN szolgáltatókra való támaszkodás. Bár vannak jelentős partnerek, a gyenge aktivitás miatt nem tűnik olyan kezdeményezésnek, amely a hagyományos CDN-ek pozíciójára veszélyes.

Központból a peremre[98]: A hagyományos, globális CDN-ek rendszerint IXP szolgáltatási pontokban (Point of Presence, PoP) vannak elhelyezve és alapvetően a peeringre építenek, hiszen hiába építenének kiterjedt hálózatot, a végfelhasználóhoz egyelőre mégiscsak az ISP-ken és a CSP-ken keresztül lehet eljuttatni a tartalmat. Az adatközponti jelenlétre természetesen továbbra is szükség lesz, de erősödik az igény, hogy a végfelhasználóhoz közel kellene vinni a gyorsítótárazás lehetőségét a jobb felhasználói élmény érdekében (pl. 5G alacsony késleltetési követelmények) és a peering forgalom csökkentéséhez. Ez a folyamat az ISP-knek kedvez, mivel az „utolsó mérföld” paramétereire jobban rálátnak és nagyobb hatást tudnak gyakorolni, pl. QoS méréssel és visszacsatolással. Ezért a CDN szolgáltatónak érdemes lehet elébe menni és megoldásokat kínálni az edge-en történő gyorsítótárazásra is, mielőtt az ISP-k lépnek[99].

7.2 Fordított proxy-k[100]

A CDN-eken túl a statikus tartalmi elemek másik jellemző gyorsítótárazási módszere a fordított proxy-k alkalmazása. Ez a szolgáltatás egyfajta előtétet képez a backend webalkalmazás előtt a külvilág felé (lásd 39. ábra[101]). A gyorsítótárazás mellett terheléselosztási, SSL/TLS végződtetési és biztonsági védelmi funkciói is lehetnek. Számos nyílt forrású szoftver elérhető, amely tud ilyen funkciót is megvalósítani (Nginx, Apache, Traefik Proxy), de számos felhőszolgáltató is nyújt ilyen szolgáltatást.

[97] https://opencaching.svta.org/what-is-open-caching/, https://www.streamingmediablog.com/2011/06/telco-and-carriers-forming-new-federated-cdn-group-called-ocx-operator-carrier-exchange.html
[98] https://www.ixcellerate.com/cdn-trends-in-2021/, https://www.azion.com/en/blog/edge-computing-evolution-of-cdn/
[99] https://www.telecomreviewna.com/articles/reports-and-coverage/5185-telcos-and-isps-to-play-a-critical-role-in-the-cdn-ecosystem
[100] https://w3techs.com/technologies/overview/proxy
[101] https://securityboulevard.com/2023/04/what-is-reverse-proxy-how-does-it-works-and-what-are-its-benefits/



39. ábra A "hagyományos" és a fordított proxy-k működése közötti különbség

7.2.1 Biztonsági kérdések

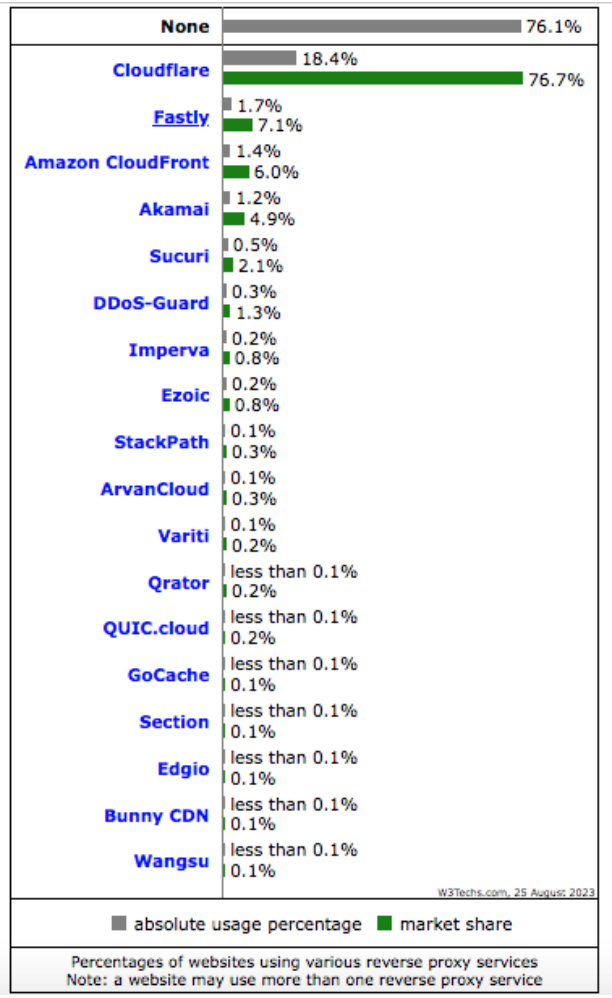
Mint a külvilággal közvetlen kapcsolatot tartó komponens, kompromittálódása a kiszolgált webes szolgáltatásokat veszélyeztetheti. Ezért ugyanúgy karban kell tartani, mint magukat a backendeket. Ellenkező esetben az alábbi problémák forrása lehet:

- Titkosítás végződtetése esetén a backendek irányába folyó titkosítatlan forgalomhoz is hozzáfér, és szenzitív adatok szerezhetők meg tőle.
- Sokszor a védett hálózati szegmensekhez közvetlenül tud kapcsolódni. Ha nem alkalmaznak egyéb (pl. DNS alapú) terheléselosztást, akkor kizárólagos meghibásodási pont lehet: az összes kiszolgált webalkalmazás kompromittálódik vagy elérhetetlen lesz.
- Ha a backendet nem, de a proxy-t valamilyen felhőszolgáltató biztosítja, az további biztonsági és függőségi kérdéseket vet fel.

7.2.2 Fő piaci szereplők

Az 40. ábra[102] azt mutatja meg, mely szolgáltatók és milyen arányban biztosítanak fordított proxy szolgáltatást a weboldalak számára. Látható, hogy CDN-ek és felhőszolgáltatók is jelen vannak ezen a piacon. A webhelyek 76,1%-a nem használ ilyen jellegű szolgáltatást, és a legnagyobb szereplő CloudFlare a site-ok 18,4%-ának biztosít fordított proxy-zást, ami ennek a piacnak a 76,7%-a.

[102] https://w3techs.com/technologies/overview/proxy



40. ábra Milyen fordított proxy-t alkalmaznak a website-ok, 2023. augusztusában

7.3 Tartalomadaptációs proxy-k

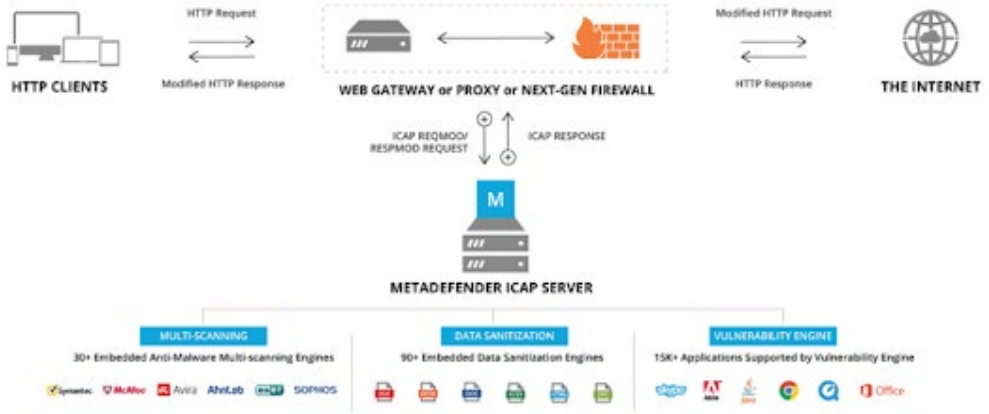
Ezek a végfelhasználóhoz közeli proxy-k nem csak továbbító és gyorsítótárazó funkciót látnak el, hanem a lekért tartalommal kapcsolatos vizsgálatokat és szűrést (pl. víruskeresés), esetleg módosítást (komplex tartalomszűrés, nyelvi fordítás, A/V transzkódolás) végezhetnek. Ezek a vizsgálatok erőforrásigényesebbek, ezért valamilyen interfész segítségével kapcsolják a hagyományos proxy-khoz (pl. Squid[103]). A tartalomadaptációs proxy-kat jellemzően vállalati környezetben alkalmazzák valamilyen enterprise kategóriás tűzfal megoldással együtt.

Internet Content Adaptation Protocol (ICAP, RFC3507, nem keverendő össze az Internet Caching Acceleration Protocol-lal): HTTP-szerű protokoll, amely a transzparens proxy-k működését hivatott kiterjeszteni oly módon, hogy a proxy a hozzá érkező kéréseket egy ICAP szerverhez továbbítsa. Az ICAP szerver (pl. CheckPoint Security Gateway[104], stb.) az üzeneteket módosíthatja, hogy végül a HTTP kliens vagy az eredeti vagy egy módosított tartalmat kapjon vissza. Rendszerint vírusvédelemre és finomabb tartalomszűrésre

[103] https://wiki.squid-cache.org/SquidFaq/ContentAdaptation

[104] https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/ICAP.htm

használatos (lásd 41. ábra[105]). Alkalmazható nyílt forráskódú proxy szerverekkel (pl. Squid), ami ilyenkor ICAP kliensként funkcionál. A protokoll absztrakciója kapcsán jelent meg az eCAP[106] szoftver interfész, amely segíti a lekért tartalom vizsgálatát kiszervezni külső komponensekhez, de alkalmazása nem terjedt el különösebben.



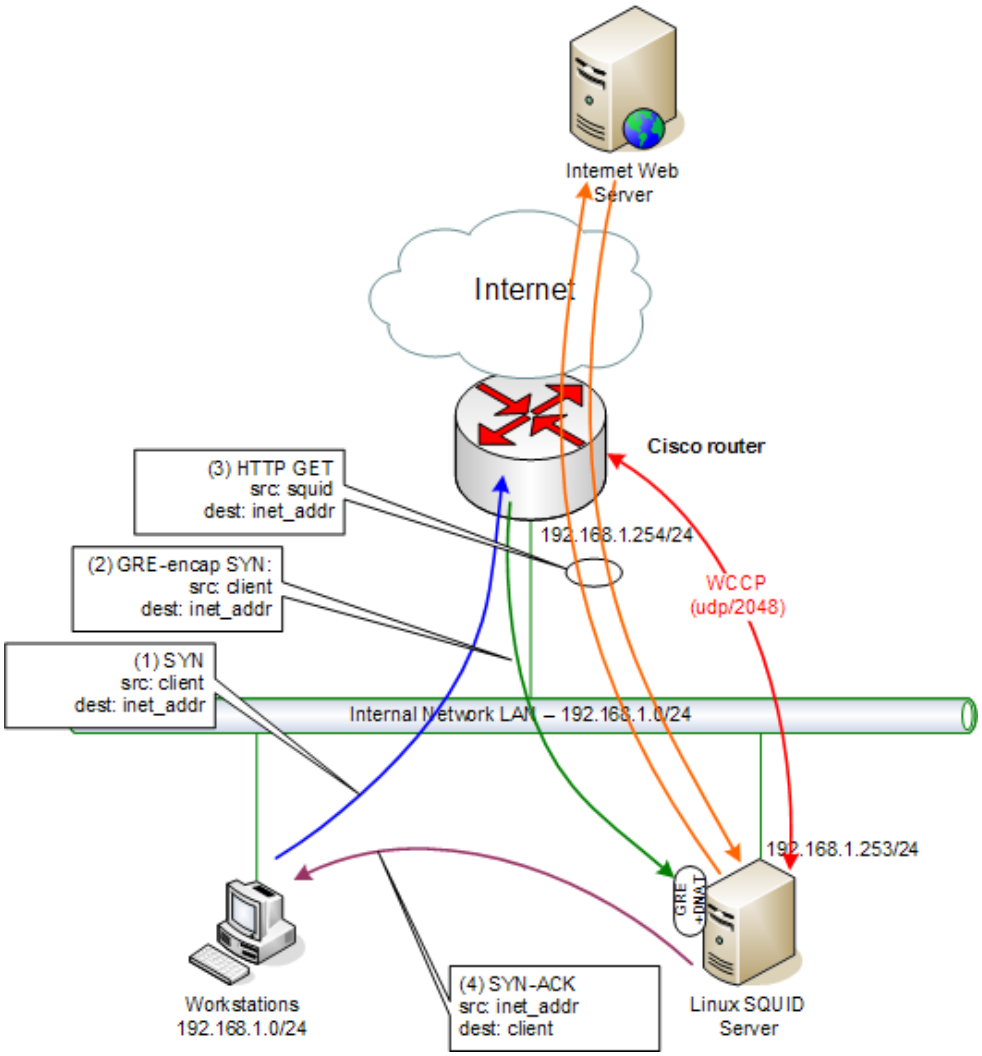
41. ábra Tartalomszűrés az ICAP protokollon keresztül

A felhő számítástechnika által biztosított nagy számítási kapacitás lehetőséget nyitott a ICAP szerverek felhőben történő üzemeltetésére. Ez a terület a Data Loss Prevention (DLP) megoldások közé tartozik[107]. A Microsoft a Defender elérhetővé tette szolgáltatását a Cloud Appok számára az ICAP-on keresztül[108], az Oracle is biztosít hasonló típusú malware elleni védelmet az SaaS (Software as a Service) szolgáltatások számára[109]. Ez újabb lehetőség a vállalati rendszerek felhőbe emeléséhez, így a tartalomadaptációs proxy-k felhőbe költözése a jövőben is folytatódik majd.

7.4 Egyéb gyorsítótárazás

Transzparens proxy: Leginkább szervezeti infrastruktúrában használják. Az átjárónál elkapják a webes forgalmat és egy helyi web proxy-n keresztül szolgálják ki. A kliens gépen nem kell konfigurációt módosítani. Mivel a HTTPS kapcsolatokba nem tud a proxy beavatkozni, ezért a kliens vele kell kiépítse a TLS kapcsolatot. Ehhez már szükség van a kliens oldalon is a proxy tanúsítványára, de központilag konfigurált kliens gépek esetén ez a tanúsítvány egyszerűen elterjeszthető a klienseken. A Cisco saját megoldást dolgozott ki Web Cache Communication Protocol (WCCP) néven[110]. Ez esetben a proxy irányába GRE alagutat épít ki, így kliens számára IP szinten is teljesen transzparensnek tűnik (lásd 42. ábra[111]).

[105] https://www.kareemccie.com/2023/05/what-is-icap-protocol.html
[106] https://www.e-cap.org/
[107] https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
[108] https://learn.microsoft.com/hu-hu/defender-cloud-apps/icap-stunnel
[109] https://blogs.oracle.com/cloudsecurity/post/using-icap-to-scale-anti-malware-protection-for-saas-services
[110] https://networklessons.com/cisco/ccie-routing-switching-written/cisco-wccp-squid-transparent-proxy
[111] https://crypt.gen.nz/papers/cisco_squid_wccp/



42. ábra Kommunikációs folyamat a WCCP-vel megvalósított transzparens proxy-n keresztül

Keresőmotorok gyorsítótárazása: A keresőmotorokat széles rétegek használják és óriási mennyiségű webes tartalmat szűrnek át rendszeresen. Ezek a szolgáltatások saját belső gyorsítótárazást alkalmaznak. Egyes szolgáltatók elérhetővé teszik a gyorsítótárukban levő korábbi változatokat. A funkció hasznos lehet akkor, ha a keresett webhely éppen nem elérhető, de bűnügyek felderítésében is segíthet. Például a Google a *cache:* előtag megadásával keres elő egy korábbi változatot. Mivel a keresőmotorok fő szolgáltatása nem az archívumképzés, ezért nem jellemző, hogy a felhasználó megadhatja, mikori tartalmat szeretne látni.

Sajnos nem internetes alapszolgáltatás az archívumképzés, de léteznek kifejezetten ezt az űrt betöltő szolgáltatások is[112]. A legismertebb talán a Wayback Machine[113], amely a számára ismert (felhasználók által is kérelmezhető) webhelyekről különböző időpontokban pillanatfelvételeket készít. Sajnos azonban ezek a szolgáltatások (amelyek általában adományokból vagy alapítványok biztosította bevételekből üzemelnek) nem képesek pótolni azt, hogy a könyvtárakhoz hasonlóan az internetes tartalmak archívumai decentralizáltan és könnyen hozzáférhetőek maradjanak. Továbbá ezek az archiváló szolgáltatások a dinamikus

[112] https://startupstash.com/internet-archive-alternatives/
[113] https://web.archive.org/

kiszolgáláson (pl. AJAX, aszinkron Javascript és XML) keresztül elérhető funkciókat nem is képesek maradéktalanul eltárolni, így képességeik is korlátozottak.

Kliens oldali gyorsítótárazás: Ezt a funkciót jellemzően a végfelhasználói szoftver (jellemzően web böngésző) végzi. A mechanizmus ezáltal implementáció függő, ugyanakkor egyénileg is konfigurálható. A cél leginkább a felhasználói élmény javítása azáltal, hogy a rendszeresen megjelenített tartalmakat a csomópont nem tölti le újra és újra a hálózatról. További, bár marginálisabb igény az offline üzemmódban is történő korlátozott működés. Ennek megvalósítását szolgálta a 2014-ben elfogadott HTML5 cache manifest[114]. Azóta megjelentek a progresszív web jellegű alkalmazások, amelyek a böngésző offline gyorsítótárába képesek helyezni azokat az objektumokat (pl. a felhasználói felület elemei), amelyek működéséhez nem kell hálózat. Továbbá nemcsak a már lekért objektumokat tárolhatja ebben a tárban, hanem az alkalmazás előre is lekérhet oda objektumok. Ennek következtében a HTML5 cache manifest támogatása mára kikerült a böngészőkből.

7.5 DSA vonatkozások

Az EU DSA szabályozása alapján az EU-ban létesített vagy azon belül is szolgáltatóknak a végfelhasználók számára is átlátható feltételek és közösségi irányelvek mellett kell a szolgáltatásukat nyújtaniuk.[115] Emellett biztosítaniuk kell az illegális tartalmak azonnali eltávolítását is. A csak továbbítást vagy gyorsítótárazást végző szolgáltatók közül a legalább 45 millió/hó felhasználót kiszolgálókra további szigorúbb kritériumok is vonatkoznak, pl. jelentkéskészítési kötelezettség különféle mutatók tekintetében. Ezek azonban a számukra technológiai kötöttséget nem jelentenek, tehát nem várható, hogy a területen átrendezné a piaci viszonyokat.

[114] https://html.spec.whatwg.org/multipage/browsers.html#offline
[115] https://www.transatlantic-lawyer.com/what-is-the-new-eu-digital-services-act-and-what-does-it-mean-for-you/

8 Felhőalapú számítástechnika

A felhő fogalom jelentése meglehetősen tág, nehezen körülhatárolható. A területen a cél elsősorban az, hogy bárhonnan és bármikor elérhető alkalmazásokat nyújthassanak a szolgáltatók egy kiterjedt és nagy teljesítményű infrastruktúra segítségével. Ehhez adatközpontokban koncentrált erőforrásokat építenek ki, ahol átfogó virtualizációs modell mentén építkeznek az infrastruktúrától az alkalmazási rétegig. A vállalati adatközpontokhoz képest a felhő adatközpontokban az a jellemző, hogy kevesebb aktív eszközön halad át a forgalom a szerverek között. A köztes kapcsolatok nagy sebességűek, továbbá a háttértár és az adathálózat szerves egységet alkot.

Egy új szolgáltatás indulásához szükséges szoftver és hardver erőforrásokat a leggyorsabban és leghatékonyabban a felhőszolgáltatók tudják biztosítani. A legismertebbek a publikus felhőszolgáltatások, de több dedikált felhőinfrastruktúra épült a népszerű szolgáltatások (pl. Facebook/Meta) kiszolgálására is.

8.1 Jellemző adatközponti infrastruktúra

Az adatközpontok osztályozása négy kategóriába (tier-be) történik. A szintek számozása a legalacsonyabb 1-es szinttől a 4-esig terjed, amit az 6. táblázat[116] foglal össze.

6. táblázat Az adatközpontok osztályozása

PARAMÉTEREK	TIER 1	TIER 2	TIER 3	TIER 4
Garantált folyamatos üzemidő	99,671%	99,741%	99,982%	99,995%
Évenkénti leállási idő	<28,8 óra	<22 óra	<1,6 óra	<26,3 perc
Komponensek redundanciája	Nincs	Részleges tápellátási és hűtési redundancia (részleges N+1)	Teljes N+1	Hibatűrő (2N vagy 2N+1)
Párhuzamos karbantarthatóság	Nincs	Nincs	Részleges	Van
Árkategória	$	$$	$$$	$$$$
Feldarabolás	Nincs	Nincs	Nincs	Van
Személyzet	Nincs	Egy műszak	Legalább két műszak	24/7/365
Jellemző ügyfélkör	Kis cégek és startupok egyszerű igényekkel	Kkv-k	Növekvő és nagy cégek	Állami szervek és nagyvállalatok

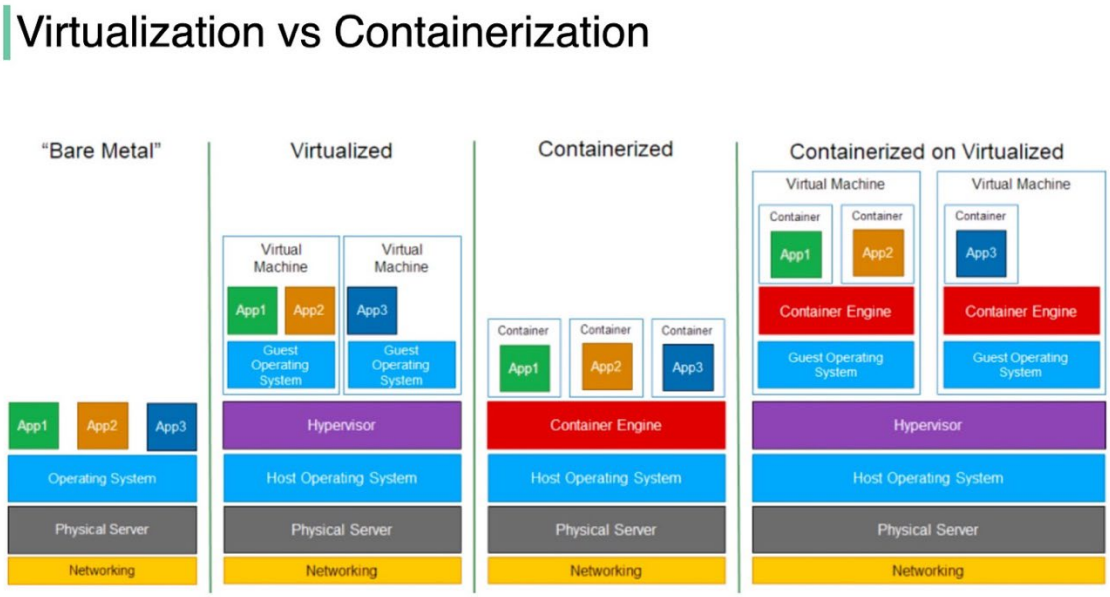
[116] forrás: https://phoenixnap.com/blog/data-center-tiers-classification

PARAMÉTEREK	TIER 1	TIER 2	TIER 3	TIER 4
Elsősorban miért választják ezt a szintet	Elérhető ár	Jó ár/teljesítmény arány	Jó egyensúly a nagy teljesítmény és a megfizethetőség között	A hibatűrő létesítmény megfelelő a folyamatos nagy terhelés és számításigényű feladatokhoz

8.1.1 Virtualizációs lehetőségek

Hardvervirtualizáció: A virtualizáció kezdetben legnépszerűbb lehetősége a teljes operációs rendszer és alkalmazási réteg régi hardverről új hardverre történő költöztetése volt. Az adatközpontokban elhelyezett nagy tárolókapacitás és memóriával jól bővíthető szerverek lehetővé tették, hogy az oda átköltöztetett (vendég operációs rendszer, OS) rendszerek virtuális gépek formájában hatékonyabban osztozzanak az erőforrásokon (a 43. ábra[117] Virtualized oszlopa), valamint a vendég OS rendszerek transzparens költöztetését, akár leállításuk nélkül. Az ipari vezető szereplő ezen a téren VMware.

Konténeralapú virtualizáció: DevOps és mikroszolgáltatás szemlélet hatására terjedő megoldás (docker swarm, kubernetes). A konténerek jellemzően egy-egy folyamatot szolgálnak ki, de közös, a gazdagép operációs rendszere által biztosított funkciók segítségével virtualizált hardver és szoftver erőforrásokon osztoznak (a 43. ábra Containerized oszlopa). Hatalmas előnye, hogy a konténerek képfájlok alapján gyorsan hozhatók létre és szüntethetők meg, ami a hardver virtualizációhoz képest dinamikus életciklus kezelést és erőforrás elosztást tesz lehetővé. Térnyerése továbbra is folytatódik, hiszen hatékonyabban támogatja az egyre komplexebb szolgáltatások kis építőelemekből történő felépítését.



43. ábra Virtualizációs és konténerizációs lehetőségek

[117] https://blog.bytebytego.com/p/what-are-the-differences-between

Nem feltétlenül a leghatékonyabb, de a hardver virtualizáció és a konténerizáció keverhető is. Ez esetben a virtuális gépekből alkotott erőforrásokon futnak a konténerizációs környezetek (mint a 43. ábra Containerized on Virtualized oszlopa esetében).

8.2 Publikus felhők

Üzleti céllal létrehozott szolgáltatások, amelyeknél bárki előfizetheti és használhatja az ott kínált erőforrásokat. Továbbá a leggyakrabban használt szoftverkörnyezeteket és technológiákat is igénybe lehet rajtuk venni. A fejlesztő, megrendelő rendszerint a felhasznált erőforrásokért fizet.

Előnyök:

- Azonnali indulás lehetősége, mivel nem szükséges hardver és szoftver eszközöket vásárolni.
- Egy szolgáltatás életciklusa kezdetén rendszerint kevés felhasználóval, forgalommal, így viszonylag kis erőforrás igénnyel bír. A szolgáltatás népszerűsödése során az erőforrásigénye is növekszik, amihez jó skálázódási lehetőségeket biztosítanak a felhőszolgáltatók.
- Az adatközpontokban fejlett támadásvédelmi módszereket alkalmaznak, így az esetleges támadások gyorsabban elháríthatók, hatékonyabban kezelhetők. Ezáltal a szolgáltatáskiesési idő is csökken.
- A hardver és szoftverkörnyezet karbantartásáról a szolgáltató gondoskodik. Az alkalmazásfejlesztő a saját szoftverének fejlesztésére koncentrálhat.

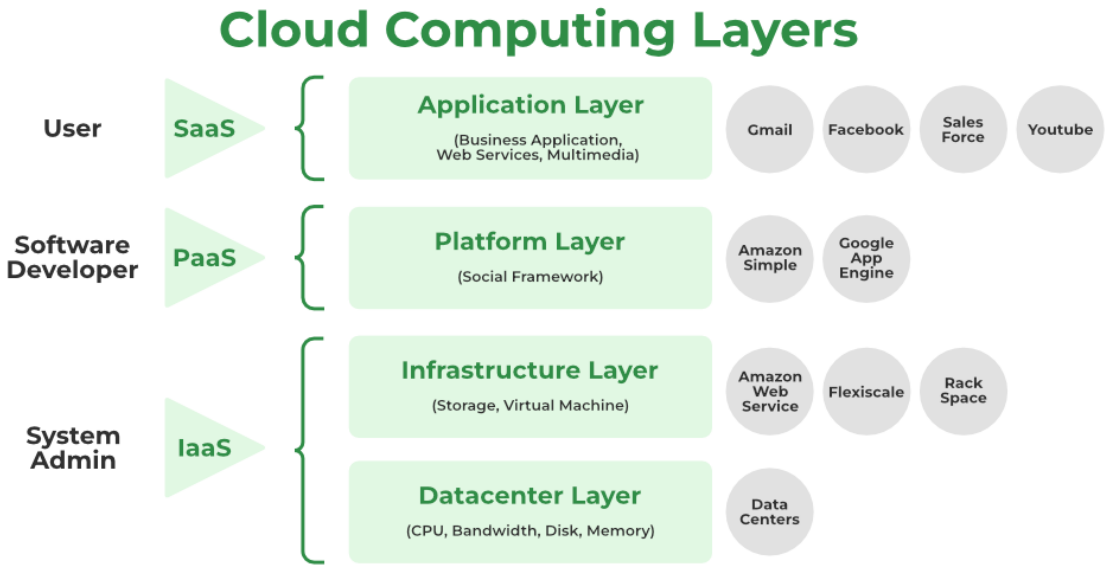
Hátrányok:

- Felhőszolgáltató váltása esetén a szolgáltatás és az adatok migrálása körülményes lehet. Ez megnehezíti a leválást és az alternatívához költözést.

8.2.1 Jellemző szolgáltatásrétegek

A rétegek nevezéke és halmaza folyamatosan változik, ahogy új technológiák, paradigmák jelennek meg az adatközponti informatikában. A legjellemzőbb rétegeket a 44. ábra[118] mutatja be.

[118] https://www.geeksforgeeks.org/layered-architecture-of-cloud/



44. ábra A felhőben jellemző szolgáltatásrétegek

IaaS (Infrastructure as a Service): Alacsonyabb rétegbeli szolgáltatások: Számítási, tárolási és hálózati kapacitás és szolgáltatások (pl. tűzfal és terheléselosztó). Ilyen az Amazon EC2 és S3, a Rackspace, a Google Compute Engine és a Microsoft Azure.

PaaS (Platform as a Service): Alkalmazási réteghez kötődő szolgáltatások: AI/ML, adatbáziskezelők, alkalmazások, API-k. Például: AWS Elastic Beanstalk, Microsoft Azure, Google App Engine.

SaaS (Software as a Service): Felhő alapú szoftvertermékek. Használatuk nagy előnye, hogy karbantartásukért és az erőforrásokért a szolgáltató felel.

NaaS (Network as a Service): Hálózati szolgáltatások, pl. CDN.

DaaS (Data as a Service): Adatgyűjtő és elemző szolgáltatás. Manapság rengetegen gyűjtenek szenzorokból és egyéb forrásokból, sokszor rendkívül nagy mennyiségű adatot. Ezek elemzése is erőforrásigényes, amit a felhőben egyszerűbb lehet elvégezni.

ITaaS (IT as a Service): Az adatközpontok szoftver-definiált absztrakciója. A virtualizáció újabb rétege, amely mentén az adatközpont erőforrásait virtualizált szolgáltatásként lehet továbbadni. Egyelőre nem bír igazi jelentőséggel.

8.2.2 Meghatározó szereplők

A 2023. nyarán a vezető tíz legjelentősebb felhőszolgáltatót a 7. táblázat[119] foglalja össze.

7. táblázat A legjelentősebb felhőszolgáltatók

#	Szolgáltató	Régiók száma	Elérhetőségi zónák száma
1	Amazon Web Services (AWS)	26	84
2	Microsoft Azure	60	116

[119] https://dgtlinfra.com/top-10-cloud-service-providers-2022/

#	Szolgáltató	Régiók száma	Elérhetőségi zónák száma
3	Google Cloud Platform (GCP)	34	103
4	Alibaba Cloud	27	84
5	Oracle Cloud	38	46
6	IBM Cloud (Kyndryl)	11	29
7	Tencent Cloud	21	65
8	OVHcloud	13	33
9	DigitalOcean	8	14
10	Linode (Akamai)	11	11

8.3 Privát felhők

Jellemzően ipari szereplők, multinacionális nagyvállalatok, államigazgatási szervek és népszerű tartalomszolgáltatást fejlesztők döntenek úgy, hogy saját IT szolgáltatásaiknak legalább egy részét (jellemzően a szenzitívebb adatokat érintőt és a vállalat napi működése szempontjából kritikusakat) saját maguk által épített és felügyelt adatközpontokkal biztosítják. Emellett költséghatékonysági, megbízhatósági (bizalmatlansági) szempontok is terelhetik őket efelé.

Ha egy szolgáltatás (pl. Facebook/Meta) nagyon népszerű és hatalmas felhasználói tábort kell elérni, akkor gazdaságosabb lehet dedikált infrastruktúra kiépítésére. Bár előfordul, hogy az erőforrások egy részét bizonyos módokon (pl. API hívásokon keresztül) elérhetővé teszi külső szereplők számára is, de alapvető célja kiszolgálni azt, amiért kiépítették.

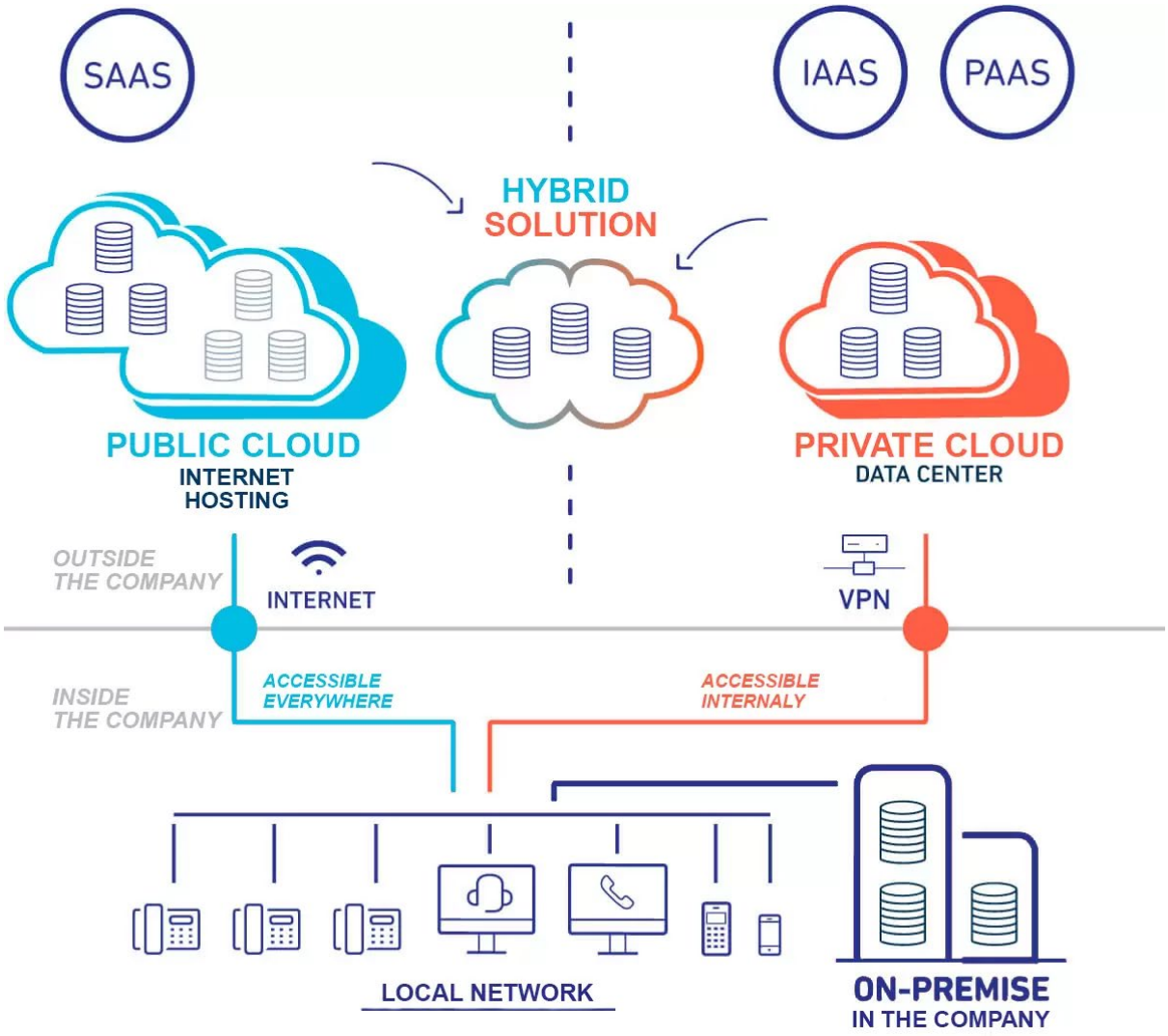
Az ipari szereplők számára a privát felhő jellemzően a külvilágtól elzárt vagy szigorúan ellenőrzött interfészen keresztül nyitott csak, hiszen a termelés minél megbízhatóbb kiszolgálásra a cél.

Publikus felhő fölött is kiépíthető privát felhő, ilyenkor virtualizált privát felhőről beszélünk (pl. az Amazon Virtual Private Cloud szolgáltatása).

8.4 Multi és hibrid felhők[120]

Ha kizárólag egy adott felhőszolgáltatóra támaszkodunk, az kiszolgáltatott állapotot jelent. Ezért sokan több felhőszolgáltatóra is építik a szolgáltatásukat, ahogyan azt a 45. ábra[121] példáján láthatjuk.

[120] https://www.techtarget.com/searchcloudcomputing/definition/hybrid-cloud
[121] https://www.iasparliament.com/current-affairs/hybrid-cloud-and-the-remote-reality



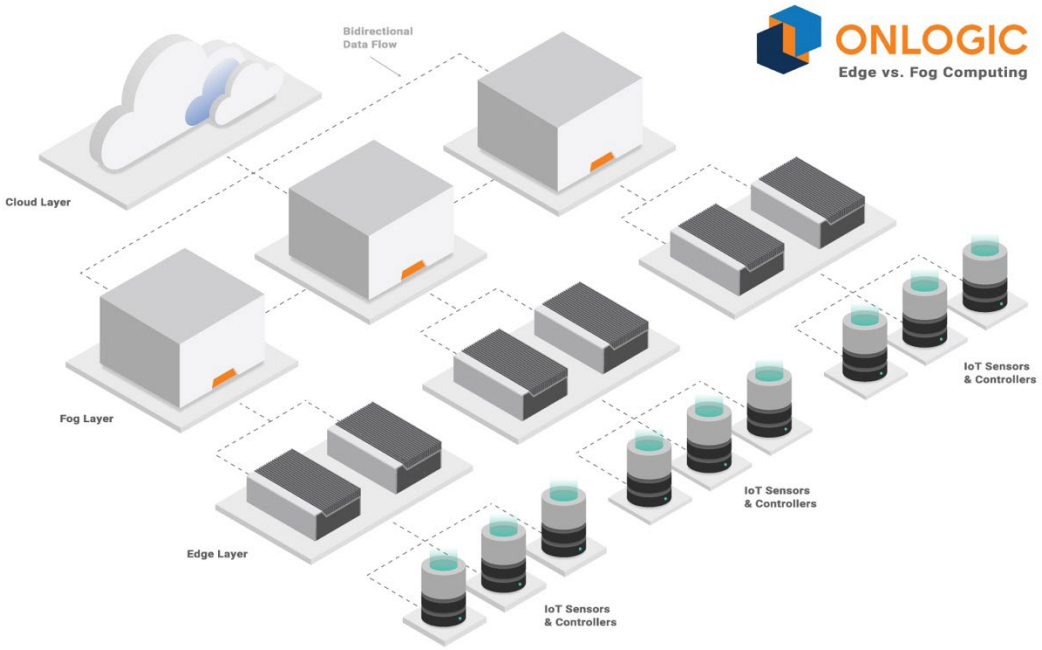
45. ábra Hibrid felhő megoldásra épített vállalati infrastruktúra

Mind a publikus, mind a privát felhő használatának lehetnek bizonyos hátrányai (pl. egy vállalat IT infrastruktúrájának működtetése szempontjából). Ilyen hátrányok pl. a publikus felhők használati költségei, az azzal való tervezés, valamint biztonsági vonatkozásai (hol találhatók valójában az adatok, mivel jár az átmeneti szolgáltatáskiesés). Ugyanakkor a privát felhők hardver és szoftver elemeit is karban kell tartani és valószínűbb a meghibásodásból fakadó leállás. Ha ez a privát felhő nem egyszerű helyi erőforrásteremben, hanem egy magas rendelkezésre állású adatközpontban található, csökkenthetők az előbbi veszélyek.

A hibrid felhőre épülő IT infrastruktúra komplex, kompatibilitási kérdéseket vet fel az interfészeknél, az adatkezelés hiányosságai miatt adatszivárgás történhet, a hozzáférés szabályzást is összetett módon kell meghatározni és a WAN (Wide Area Network) kapcsolat is kritikus a nem lokális adatközpontok irányába. Ezért az ilyen infrastruktúra tervezése és implementációja szakértelmet igényel. Ugyan számos szolgáltató biztosít hibrid felhő menedzsment eszközöket, de ezeket is integrálni kell a szervezet IT eszközkészletébe.

8.5 Perem számítástechnika/köd számítástechnika

Egyre fontosabbá váló irány, hogy az erőforrások egy részét érdemes közelebb vinni az ügyfelekhez és a végpontokhoz, mivel így csökkenthető az elérési idő. Ráadásul rengeteg adat keletkezik a végpontokon is. Ha az adatfeldolgozás vagy előfeldolgozás a forráshoz közelebb zajlik, csökken a felfelé irányuló adatforgalom is, ill. a helyi tárolókból gyorsabban férhető hozzá. A 46. ábra[122] további rétegeket mutat be a végeszközök és a felhő között: a köd (fog) réteg nagyobb teljesítményű, de közelebbi (pl. regionális) elhelyezkedésű infrastruktúrát takar. A perem (edge) réteg lehet fizikai, ez esetben jellemzően helyi, a végberendezésekhez képest nagyobb erőforrást koncentrál. Ezeket az eszközöket nem feltétlenül helyezik klimatizált adatközpontokba vagy erőforrástermekbe. Továbbá nem is kell feltétlenül kizárólag nagy teljesítményű hardverekből létrehozott infrastruktúrát érteni alatta, mert a végponti eszközök teljesítményének növekedésével tulajdonképpen egyben feldolgozó és tároló eszközök is lehetnek, vagyis egyre több erőforrás jelentkezik a hálózat határán, amely határ egyben el is mosódik. Ezáltal a perem réteg logikai is réteg is lehet.



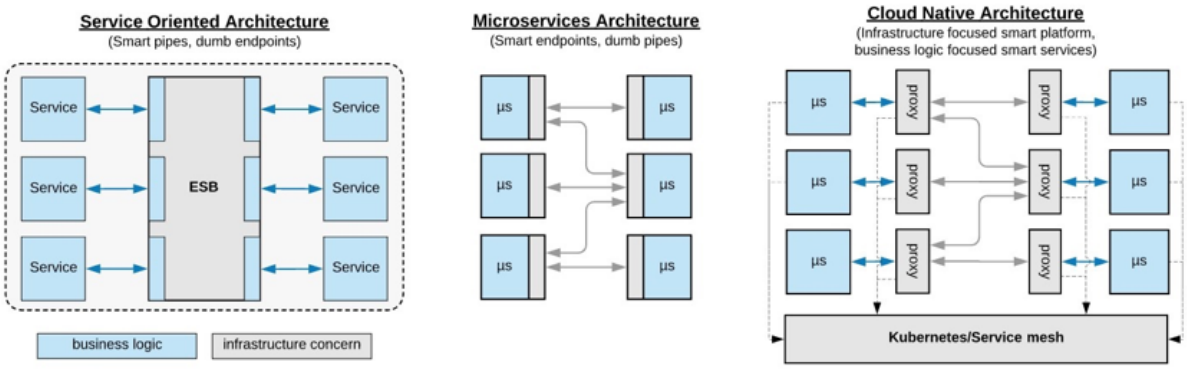
46. ábra Köztes rétegek a szenzorokról a felhőig

8.6 Lényeges trendek[123]

8.6.1 Felhőnatív alkalmazások

Egyre népszerűbb paradigma, hogy az új alkalmazások a felhős környezetet alapjainkál fogva natívan támogassák, a mikroszolgáltatás szemléletre és a konténerizációra nagyban építve. Így a ma meghatározó DevOps (Development and Operations), CI/DI (Continuous Integration/Continuous Delivery) fejlesztési, kihelyezési folyamatokhoz sokkal jobban illeszkednek és mélyen kihasználhatók a felhős környezet nyújtotta előnyök: jó skálázódás, széleskörű elérhetőség, könnyű migrálhatóság, frissíthetőség és magas rendelkezésre állás.

[122] https://www.onlogic.com/company/io-hub/fog-computing-vs-edge-computing/
[123] https://www.simplilearn.com/trends-in-cloud-computing-article



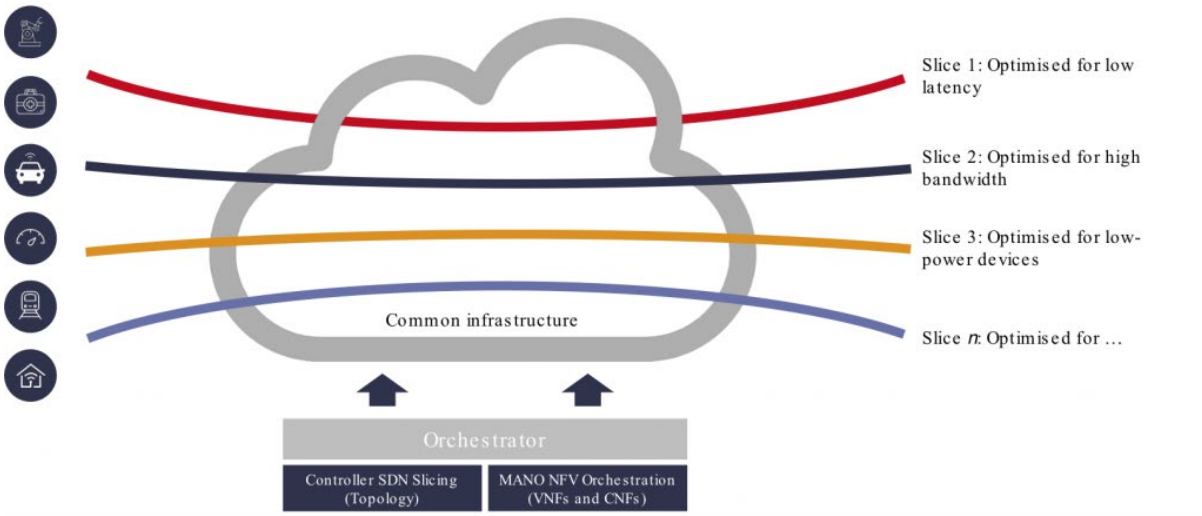
47. ábra A közelmúlt alkalmazásfejlesztési paradigmái a felhőnatív szemléleti

A 47. ábra[124] bemutatja a szolgáltatásfókuszú (service oriented application, SOA) és nagyvállalati szolgáltatáskör (enterprise service bus, ESB) paradigma szerinti alkalmazásfejlesztés evolúcióját. A monolit rendszerű szolgáltatásokat leváltották a mikroszolgáltatások, amelyek kezdetben közvetlenül egymással kommunikáltak. Itt még a szolgáltatások aránylag komplexek voltak, mert nekik kellett tudniuk, mely más szolgáltatásokhoz kell fordulniuk. A mai tendeknek megfelelően konténerizált környezetben a szolgáltatás komponensek tovább egyszerűsödtek a jó skálázódás és gyors fejlesztés érdekében, az adatkommunikációt pedig a környezet e célú komponensei valósítják meg.

8.6.2 Hálózati szoftverizáció[125]

A felhőnatív alkalmazások terjedését és a hálózatszeletelés (5G terminológiában network slicing) megvalósítását segítő folyamat. A nagy gyártói rendszereket moduláris funkciókat biztosító vendorok termékei jelennek meg (szétbontás). Ezek a virtualizáció segítségével adatközpontokban aggregált erőforrásokkal lesznek kiszolgálhatók. Mivel nagy mennyiségű építőelem, funkció jelenik meg, ezeket automatizálási eszközökkel kell menedzselni. Ennek fontos eszközei a modern fejlesztési paradigmák (pl. DevSecOps) ill. az AI/ML.

[124] https://www.alibabacloud.com/blog/how-cloud-native-is-reshaping-enterprise-it-architectures_595962
[125] https://developer.orange.com/blog/network-softwarization-what-is-it-all-about/



48. ábra Hálózatszeletelés a különböző felhasználási körök kiszolgálása érdekében

A rádiós spektrum jobb kihasználása és az 5G igényelte komplex szolgáltatáskör kiszolgálása érdekében alkalmazzák a hálózatszeletelés technikáját. A rendelkezésre álló spektrumot (és a maghálózatot) ezért virtuálisan több részre osztják aszerint, hogy milyen specifikus igényeket kell kiszolgálni vele (lásd 48. ábra[126]). Ezáltal például alacsony késleltetési idő biztosítható az azt igénylő ügyfél és alkalmazáskör számára. A felosztás dinamikusan változtatható.

8.6.3 Gépi tanulás és mesterséges intelligencia alkalmazása

A mesterséges intelligencia (artificial intelligence, AI, magyarul csak MI) és gépi tanulás (machine learning, ML) alkalmazása egyre több területre szivárog be, ezért a Google, Amazon és Microsoft, akik nemcsak a felhőszolgáltatás, hanem az MI területén és erős innovátorok abban érdekeltek, hogy a felhőikben ezek a képességek megjelenjenek és kiaknázhatóak legyenek. Ez növelheti a piaci pozícióikat, a többi szereplő pedig kénytelen lesz nyitni irányukba.

8.6.4 Adatkinyerés és feldolgozás

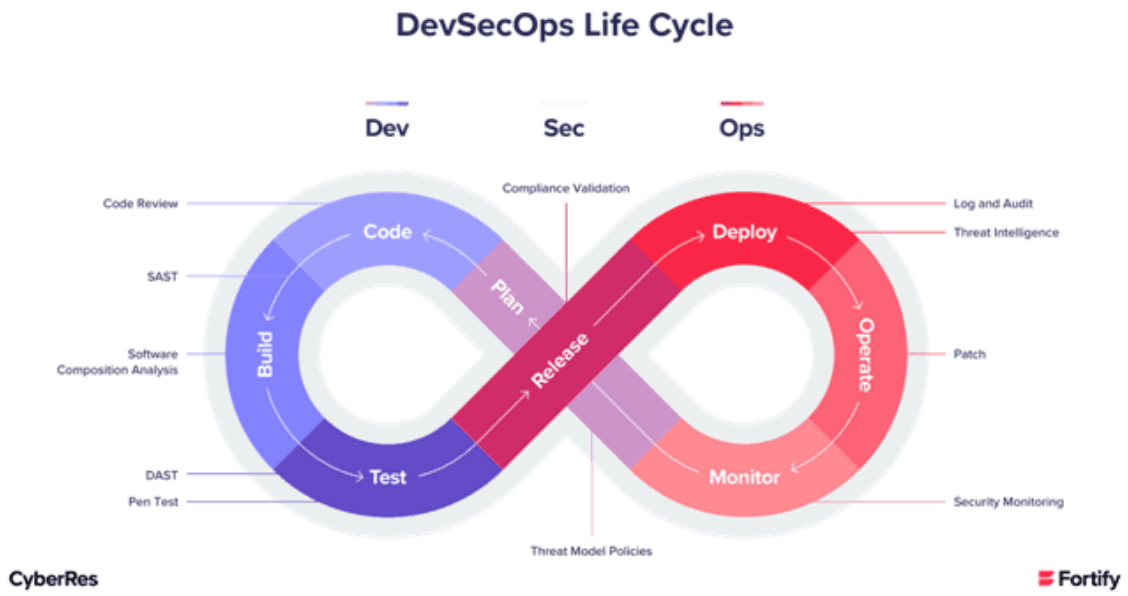
Az IoT eszközökből és felhasználói szokásokból nyert folyamatosan növekvő adatmennyiség feldolgozása, valamint az MI alkalmazása egyre több (pl. GPU) erőforrást igényel. Ez az alkalmazott hardverrel szemben támasztott követelményekben is jelentkezhet. A Facebook/Metánál már régóta ismert, hogy saját igényeikhez fejleszt hardvert és infrastruktúrát, valamint saját felhőjét is ennek szemléletében építi[127].

8.6.5 Biztonság, Dev/Sec/Ops

Ahogy egyre komplexebb szolgáltalások és egyre több adat koncentrálódik a felhőszolgáltatóknál, a biztonság kérdése is felértékelődik. A vezető szolgáltatók már most rendelkeznek elosztott túlterheléses (distributed denial of service, DDoS) védelemmel, terheléselosztási és nagy rendelkezésre állást biztosító funkciókkal. Emellett az adatok védelme is egyre fontosabb szempont lesz. A fejlesztői oldalról az DevOps gyakorlat

[126] https://stlpartners.com/articles/private-cellular/5g-network-slicing/
[127] https://about.fb.com/news/2023/05/metas-infrastructure-for-ai/

biztonsági szempontokat is magába foglaló továbbgondolásai (DevSecOps, DevOpsSec, SecDevOps) segíthetik a megfelelő adatkezelést. Van különbség a prioritásokban, de mindnél megjelenik a biztonsági szempontok érvényesítése oly módon, hogy az incidensek megelőzése mindinkább cél. Ehhez már a fejlesztéshez időben korán (akár még a konkrét fejlesztést megelőzően, tervezési fázisban (lásd 49. ábra[128]) megtörténik a szolgáltatás vagy modul sebezhetőségekkel szembeni ellenállóképességének vizsgálata.

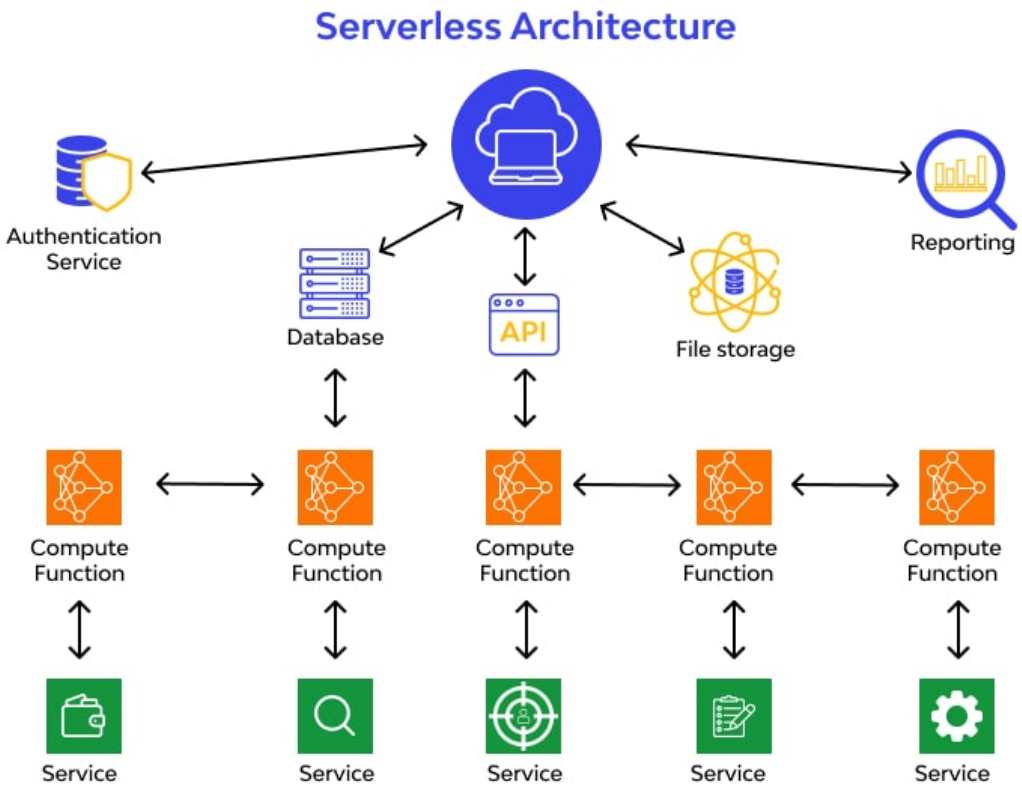


49. ábra A DevSecOps fejlesztési ciklus: fókuszban a biztonság

8.6.6 Szerver nélküli számítástechika/FaaS[129]

Az alkalmazásfejlesztők munkáját megkönnyíti, ha az infrastruktúrától minél inkább függetlenül tudják készíteni a kódot. A Function as a Service (FaaS) a mikroszolgáltatás fejlesztés egyik alapköve. Segítségével jól skálázódó rendszerek építhetőek anélkül, hogy ezzel a fejlesztőnek explicit módon foglalkoznia kellene. Az absztrakció módját a 50. ábra[130] mutatja be: generikus számítási funkciók (compute function) képezik a (mikro)szolgáltatások és a konkrétabb hardverek és API-k közötti hídat. Mint minden absztrakciónak, ennek is hátránya, hogy a mögöttes működést jobban elrejti és a lokális működtetést és tesztelést megnehezíti. Ugyan továbbra is fizikai szerverek látják el a feladatokat, de ez a réteg még jobban fedve marad a fejlesztő elől, miközben a szolgáltatás forgalmának növekedésével tovább tud skálázódni. A fejlesztéshez szükséges időt is rövidíti.

[128] https://www.microfocus.com/en-us/what-is/devsecops
[129] https://www.cloudflare.com/learning/serverless/what-is-serverless/
[130] https://www.wallarm.com/what/what-is-serverless-architecture

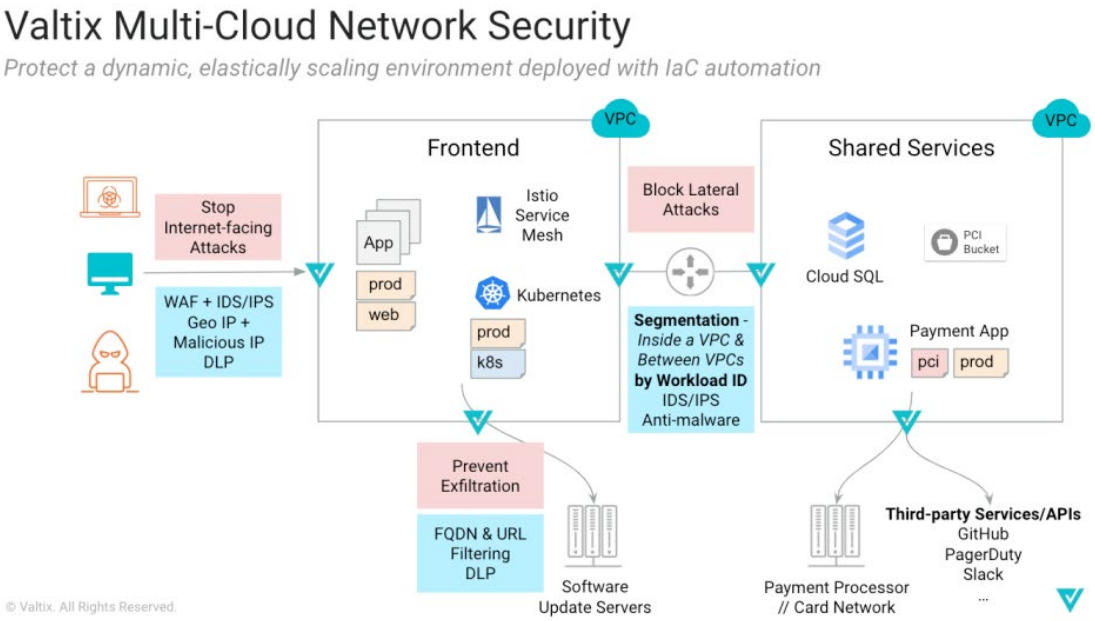


50. ábra Szerver nélküli architektúra: szerverek továbbra is léteznek, de jobban elrejti őket az absztrakció

8.6.7 A multifelhő népszerűsödése

Ha komplex szolgáltatásokra épül egy rendszer, akkor nem biztos, hogy egy adott felhőszolgáltató vagy infrastruktúratípus minden részét optimálisan kiszolgálja, akár erőforrás, akár költségoldalról. Ezeket több lábra támaszkodva többféle szolgáltató, vagy eltérő felhőtípus (elsősorban publikus és privát felhő kombinációjával) tudja kiszolgálni. Ez újfajta biztonsági kihívásokat is támaszt, ahogy arra a 51. ábra[131] is rávilágít. Míg a végpontok irányából jellemzően eleve védik a szolgáltatásokat, ügyelni kell az adatszivárgásra és a felhőkön párhuzamosan futó szolgáltatások közötti vízszintes támadásra: ha az egyik felhőben kompromittálódik egy komponens, az átterjedhet a másik felhőbe is.

[131] https://valtix.com/resources/what-is-multi-cloud-security/



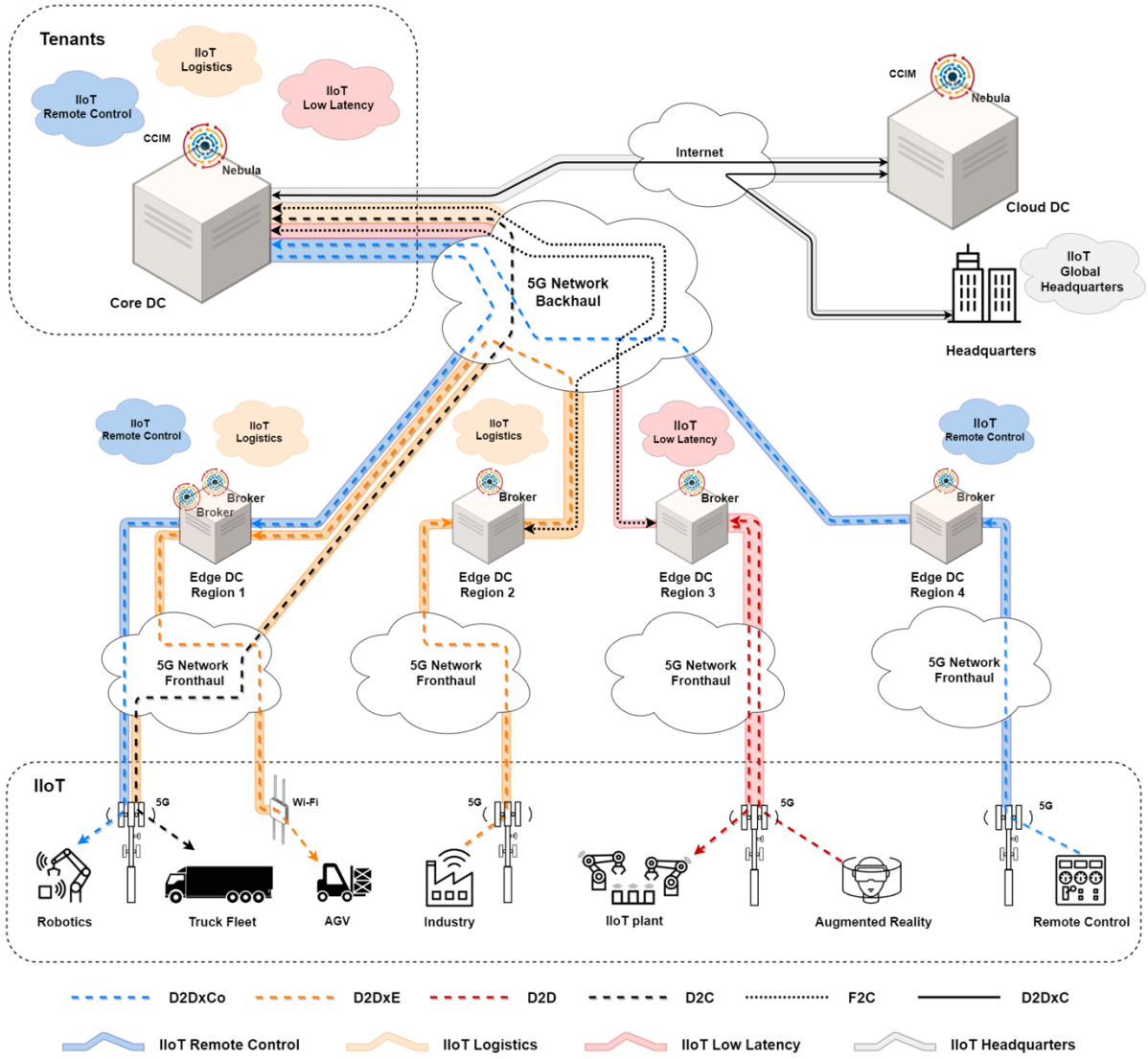
51. ábra Többfelhős architektúra és biztonsági kihívásai

8.6.8 Ipari felhők[132]

Az Ipar 5.0 célja a gyártási folyamatok automatizált és optimalizált támogatása, implementálása. Ennek fontos pillére az 5G és a mesterséges intelligencia alkalmazása. A gyártói rendszerek üzemeltetése rendszerint privát, campusokon épített adatközpontokkal, ill. peremfelhővel szolgálható ki. A magas rendelkezésre állás (ami a publikus szolgáltatóknál már elérhető) is fontos követelmény, ezért ezek fejlesztésekor erre is koncentrálni kell. További igény az egymástól függetlenül működő gyártói kapacitások interakciója, az 5G által igért magas szolgáltatásszint garanciái mellett, ahogy ezt a 52. ábra[133] is bemutatja.

[132] https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en

[133] Cabrini, Fábio Henrique, et al. "Enabling the industrial Internet of Things to cloud continuum in a real city environment." *Sensors* 21.22 (2021): 7707.

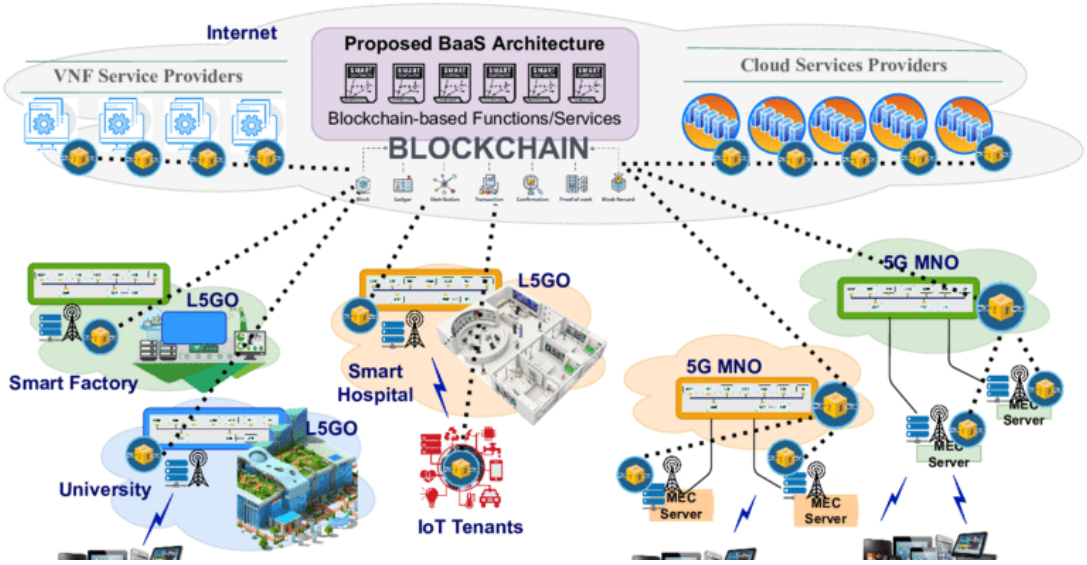


52. ábra Az ipari szereplőket kiszolgáló 5G felhő alapú architektúrák együttműködése

8.6.9 Blokklánc/BaaS

A blokklánc az Ipar 5.0 fontos technológiája lesz, de a publikus szolgáltatásoknál és publikus felhőkben is népszerűsödik. A vezető felhőszolgáltatók már most is nyújtanak Blockchain as a Service (BaaS) szolgáltatást[134], így a meglevő és készülő felhőnatív szolgáltatásba könnyebben integrálható a blokklánc technológia használata (lásd 53. ábra[135]). Praktikus lehetőség a teljesen felügyelt blokklánc üzemeltetés[136]. Azon ügyfelek, cégek számára, akik kicsik ahhoz, hogy IT szakember gárdát tartsanak a szolgáltatásaik teljeskörű üzemeltetéséhez, a felhőben futó szolgáltatásaikhoz folyamatos felügyeletre fizethetnek elő.

[134] https://www.investopedia.com/terms/b/blockchainasaservice-baas.asp
[135] Weerasinghe, Nisita, et al. "A novel blockchain-as-a-service (BaaS) platform for local 5G operators." *IEEE Open Journal of the Communications Society* 2 (2021): 575-601.
[136] https://www.helixstorm.com/blog/types-of-managed-hosting-and-how-to-choose-one/



53. ábra A BaaS alkalmazási lehetőségei

8.7 Kihívások

Biztonság: Mivel a felhőbe költözés aktuális trend, ezért az adatközpontok egyre inkább célpontjai a támadásoknak. A legjellemzőbb támadás az elosztott túlterheléses (DDoS) támadás. Ez alatt a szolgáltatás elérhetőségét veszélyeztető, nagy erőforrást lekötő és emiatt nehezen elhárítható támadások összességét értjük. A COVID-19 óta az adatközponti támadások száma egyre nő. Míg korábban jellemzően inkább az adatközponton kívülről érkeztek a támadások, folyamatosan növekszik az adatközponton belülről végrehajtott, változatos összetételű (többvektoros) támadások gyakorisága. A bérelhető virtuális gépek és a koncentrált erőforrások segítségével végrehajtott támadásokat nagyon költségesen lehet felismerni és elhárítani. Ez ma az egyik legfontosabb kihívás[137]. A nagyok előnye, hogy számos monitorozási ponton nyerhetnek mintát a támadások felismerésére, ugyanakkor az erőforrásaik bősége miatt gyakrabban is válnak célponttá. Emellett az adatközpontokban tárolt adatmennyiség is védelemre szorul, amit az EU-ban érvényes szigorú adatkezelési szabályok még kritikusabbá tesznek.

Költséghatékonyság: Az erőforrásigény váratlan növekedése komoly költségvonzatot jelenthet felhő alapú IT infrastruktúra használata esetén. Az erőforráshasználat monitorozása és optimalizálása segíthet a tervezésben, előrejelzésében. A szolgáltatóknak érdemes segíteniük ezt, így az esetlegesen hezitáló ügyfeleket is magukhoz tudják csábítani.

Integráció: A létező üzleti szolgáltatáskörök „felhősítése" mindig kihívást jelent, hiszen már létező rendszerekkel kell folyamatos együttműködést biztosítani. Ez magába foglalja a már meglevő és folyamatosan gyarapodó (régi és új rendszerekből egyaránt származó) adatvagyon bevonását is egy egységesítő struktúrába. Mivel nagy a pénzügyi felelősség és az üzleti lehetőség is ezen a téren – eközben univerzális recept és megoldás nem létezik és

[137] https://www.datacenterfrontier.com/sponsored/article/21545878/a10-why-ddos-is-more-dangerous-for-cloud-and-data-center-providers

aligha készíthető –, megjelentek olyan eszközök, amelyek az integrációs folyamatot bizonyos szintig mégiscsak segítik.

Szolgáltatófüggőség, nyílt forráskód: Egy szolgáltatáskör vagy konkrét szolgáltatás felhőszolgáltatóhoz történő költöztetése a tőle való függőséget eredményezi. Amennyiben az általa nyújtott specifikus API-khoz és felhőszolgáltatásokhoz köti magát, megnehezíti az esetleges felhőváltást. Mivel a legtöbb esetben a számlázás erőforrásfelhasználáshoz kötött, könnyen eljöhet a váltás szükségessége. Ez a függés a multi és hibrid felhős építkezéssel csökkenthető. További függetlenedési lehetőség a nyílt forráskódra történő építkezés. Többféle kezdeményezés látott napvilágot, keretrendszerek ill. PaaS formájában.

8.7.1 Ökológiai szempontok, ESG

Két környezetvédelmi szempontból is problémás a nagy adatközpontok üzemeltetése: a hardver üzeméhez és az erőforrástermek légkondícionáláshoz felhasznált energiából származó üvegházgáz kibocsájtás, valamint a hardverelemek folyamatos amortizációjából származó elektronikai hulladék. A felhőszolgáltatók folyamatosan érdekeltek abban, hogy energiafelhasználásuk egyre hatékonyabb legyen. Ezt az utóbbi időszak energiaválsága is erősítette. A COVID-19 kapcsán bekövetkező ellátási láncok megszakadása pedig kényszerítette őket a hatékonyabb hardver újrahasznosításra is[138].

A zöld felhőszámítástechnika[139] (Green Cloud Computing) kezdeményezés az energiafelhasználás és az okozott környezeti hatások minimalizálását célozza meg. A kritikus szolgáltatások szempontjából azért lehet lényeges, mert segíthet a megbízhatóságot, elérhetőséget biztosítani. A nagy szolgáltatók hozzáállása lényeges lehet az érvényesülését illetően[140]. Igéretek szintjén az Amazon, a Microsoft és Google már mutatnak szándékot.

8.8 Internetes webtárhely szolgáltatás

Bár a felhőszolgáltatók népszerűek webtárhely szolgáltatóként is, kisebb forgalmú website-ok kiszolgálására a hagyományos, technikai webszolgáltatást (webhosting) szokták igénybe venni. Az ezt kiszolgáló szerverek rendszerint szintén adatközpontokban vannak elhelyezve, de dedikáltan webszerverként működnek. A komolyabb szolgáltatóknak ugyancsak több helyszínen vagy régióban van adatközpontja. A legnagyobb ilyen jellegű szereplő a GoDaddy[141], aminek három kontinensen 9 adatközpontja van, több mint 37000 szerverrel.

[138] https://bluexp.netapp.com/blog/cvo-blg-the-future-of-cloud-computing-5-trends-you-must-know-about

[139] https://www.techrxiv.org/articles/preprint/Green_Cloud_Computing_Current_trends_and_future_prospects_for_intelligent_computing_environments/23681460

[140] https://www.simplilearn.com/green-cloud-computing-article

[141] https://webhostingadvices.com/godaddy-data-center-server-location/

54. ábra Webtárhely szolgáltatások típusai, előnyeikkel és hátrányaikkal

Többféle webhosting megoldás létezik: virtuális host, virtuális privát szerver (Virtual Private Server, VPS), felhő alapú és dedikált hardverrel biztosított. Ezekről a 54. ábra[142] ad átfogó képet. Az első megoldás olcsóbb, hiszen itt általában csak tárhelyterületet, adatbázishozzáférést és egy korlátozott beállítófelületet kap a megrendelő.

A költségesebb, VPS típusú szolgáltatás esetében az ügyfélnek nagyobb kontrollja van az erőforrások terén, rendszerint komolyabb adminisztrációs felülettel. Bár a hardveren itt is osztoznak a kiszolgált website-ok, a jobb erőforrás monitoring nagyobb rendelkezésre álláshoz és teljesítményhez segíthet.

A még drágább dedikált webhosting esetében a hardvert ugyan a szolgáltató biztosítja, de erőforrás tekintetében nem kell osztozni. Ez biztonsági és teljesítmény szempontból is előnyös.

A felhőszolgáltatók nagy előnye a skálázhatóság és a még jobb globális elérhetőség.

8.8.1 Összevetés a felhő alapú kiszolgálással

- Egyedül a dedikált hardveres kiszolgálás biztosít fizikai hozzáférést, ilyet a felhőszolgáltatók nem szoktak adni.
- Teljesítmény tekintetében a felhőszolgáltatók nagyobb adatközpontjaik miatt nagyobb merítésből gazdálkodhatnak. Ez a nagy időszaki terhelésű site-ok kiszolgálására is alkalmasabb.
- Míg a hagyományos webtárhely szolgáltatók nem minden esetben rendelkeznek több adatközponttal, a felhőszolgáltatók viszont igen, emiatt a katasztrófák és támadások ellen is jobban védettek, hiszen ugyanazon adatok több adatközpontban is megtalálhatók.
- Mivel az erőforrások virtuálisan kezeltek, még ugyanazon adatközponton belüli hardver meghibásodás esetén is transzparens módon migrálják a szolgáltatásokat az elérhető csomópontokra, rendszerint szolgáltatáskiesés nélkül.
- Költségek tekintetében a webtárhely szolgáltatók fix előfizetési díjért kínálják a szolgáltatást, valamilyen maximális forgalmi és erőforrás korláttal. A felhőszolgáltatók az igénybe vett erőforrás után számláznak.

8.8.2 Jelentős szereplők

A 2023. nyarán piaci részesedésük szerint vezető (nem felhős) webtárhely szolgáltatókat a 8. táblázat[143] foglalja össze.

8. táblázat Jelentős webtárhely szolgáltatók

Webtárhely szolgáltató	Piaci részesedés (%)
GoDaddy	30%
Hostinger	17%
Bluehost	14%
HostGator	9%
SiteGround	8%

[142] https://www.rackbank.com/blog/which-type-of-hosting-to-choose/
[143] https://www.wp-tweaks.com/web-hosting-market-share-report/

Webtárhely szolgáltató	Piaci részesedés (%)
A2 Hosting	4%
InMotion Hosting	3%
Minden egyéb	15%

8.8.3 A webtárhely szolgáltatás jövője

Egyre több website költözhet felhőszolgáltatókhoz, mivel azok dinamikusan fejlődnek és számos előnyt kínálnak. Ezek közül a legfontosabb a skálázódás lehetősége, amely az 5G térhódításával várható megnövekvő forgalmi és tárolási, számítási igény miatt lehet szükség. A kisebb ügyfelek számára azonban továbbra is alternatívák maradnak a nem-felhős szolgáltatók, mivel ők a fix előfizetési díjas konstrukciókat preferálják. Számukra fontosabb a tervezhető kiadás, mint a felhős webkiszolgálás nyújtotta többletszolgáltatások.

8.9 EU DSA vonatkozások[144]

Az EU-ban bevezetett DSA szabályozások vonatkoznak mind a felhő, mind a hagyományos tárhelyszolgáltatókra. Ez a gyakorlatban azt jelenti, hogy hatékony intézkedési munkafolyamattal kell rendelkezzenek a tartalmakkal kapcsolatban:

- A felhasználó tájékoztatása eltávolított tartalom esetén, indoklással.
- Illegális tartalom bejelentésének lehetősége.
- Bűnüldöző hatóságok felé történő adatszolgáltatás.

A vezető felhőszolgáltatók már léptek ez irányban. A szabályozás célpontjai a széles körű szolgáltatást nyújtó szereplők, ezért a rajtuk kiszolgált, számtalan kis ügyfél által biztosított webszolgáltatás fejlesztőjének nincs közvetlen teendője emiatt.

[144] https://www.allenovery.com/en-gb/global/news-and-insights/digital-services-act/layer-two-providers-of-hosting-services, https://www.utopiaanalytics.com/article/digital-services-act-dsa-effects-on-businesses-in-the-eu

9 5. generációs mobilhálózatok

Az 5G vagy ötödik generáció a cellás mobilhálózatok legújabb generációja, mely jelentős előrelépést jelent a korábbi 4G technológiához képest a sebesség, a kapacitás, a késleltetés és a támogatható alkalmazások köre tekintetében. A korszerű virtualizációs technológiák, a mikroszolgáltatás architektúra és a hiperautomatizáció együttesen alakítják az újgenerációs mobilhálózatok által nyújtott képességeket.

9.1 5G hálózatok kulcsképességei

- Alacsony késleltetés
- Nagy áteresztőképesség: spektrumhatékonyság, „beamforming", „massive MIMO"
- Magas csomópontszám hatékony kezelése: IoT/M2M kommunikáció
- Megnövelt hálózati intelligencia: „hálózati szeletelés", „felhőalapú erőforrásfoglalás"
- Nagy megbízhatóság a kritikus alkalmazások számára
- Rugalmas telepítési modellek

9.2 5G NSA vs SA

Jelenleg kétféle 5G telepítéssel találkozhatunk. Az első ún. non-stand alone (NSA) konfiguráció esetén a meglévő LTE hálózatba építjük be az 5G hálózati komponenseket (gyorsan kivitelezhető barnamezős telepítések), jellemzően egy 5. generációs rádiós hozzáférési hálózatot kapcsolnak össze a meglévő LTE EPC maghálózattal. Ebben az esetben az új technológia előnyei csak korlátozottan érhetőek el (pl. számolhatunk áteresztőképesség növekedéssel, de az ultra alacsony késleltetés ebben az esetben nem valósítható meg). A teljes jelzésforgalom LTE-alapú, a felhasználói adatok átviteléhez viszont rendelkezésre áll az 5G rádiós spektrum, amely teljesítménynövekedést hoz a meglévő LTE hálózatba. Tehát az 5G NSA hálózatok átviteli kapacitásnövekedésben nyújtanak előrelépést a meglévő LTE telepítésekhez képest. Ennek megfelelően az 5G NSA hálózatokat átmeneti megoldásnak tekinthetjük a teljesen önálló, ún. stand-alone (SA) 5G hálózatok felé, melyek végponttól végpontig biztosítják az 5. generációs mobilhálózati összeköttetést. Az 5G technológia képessége SA hálózati konfiguráció esetén aknázhatóak ki maradéktalanul. Az alacsony késleltetést követelő felhasználási esetek (pl. ipari IoT, autonóm járművek) elsősorban 5G SA hálózaton alapulnak. Az 5G SA hálózatok magasfokú virtualizációjának köszönhetően a legnagyobb felhőszolgáltatók az utóbbi pár évben érdeklődést mutatnak a távközlési piac irányába. A hyperscaler szolgáltatók rendelkeznek jelenleg a legmagasabb színvonalú felhő technológiával, így a jövő 5G hálózatainak telepítésében és üzemeltetésében potenciálisan komoly szereplővél válhatnak.

9.3 Felhőalapú maghálózat (Cloud Core)

A felhőalapú maghálózat az 5. generációs kommunikációs hálózatok kulcsfontosságú eleme. A 5G technológia karakterisztikus jellemzői (lásd fentebb) a felhő architektúra felhasználásával biztosíthatóak fenntartható és skálázható módon. A felhő architektúrákról részletesen a 7. fejezetben írunk.

9.4 Felhőalapú rádiós hozzáférési hálózat (Cloud RAN vagy C-RAN)

A hagyományos RAN architektúrában minden bázisállomás (eNodeB) egy önálló entitás, saját alapsávi feldolgozó egységgel (BBU) és rádiófrekvenciás (RF) egységgel. Ez a konstrukció bonyolult és költséges lehet, különösen sűrű telepítések esetén.
A fentiekkel szemben a Cloud RAN technológia központosítja az alapsávi feldolgozást, mely a RAN alapsávi szoftver és a RAN alapsávi hardver szétválasztásán alapul. A RAN alapsáv szoftvere általános célú szerverhardveren futtatható cloud-native eszközök és folyamatok felhasználásval. Ez a szétválasztás nagyfokú rugalmasságot biztosít a RAN szoftver telepítésében: telepíthető a RAN hardverre közvetlenül, a CSP adatközpontjába, vagy akár egy publikus felhő infrastruktúrába. A szétválasztott és központosított architektúrával a rádiós hálózatok telepítése és üzemeltetése is jelentősen megváltozik. A felhőbe kerülnek olyan funkciók, mint a moduláció és demoduláció, és hibajavítás. A központosításnak költségcsökkentő hatása is van, hiszen jelentősen csökkenthető az egy bázisállomásra eső bekerülési és üzemeltetési költség. Az 5. generációs kommunikációs hálózatok szempontjából talán a legfontosabb újdonsága a felhőalapú rádiós hálózatoknak az erőforrások hatékony menedzsmentje a központosításnak köszönhetően. Lehetővé válik az erőforrások dinamikus, igény szerinti kiosztása, miáltal csúcsidőszakokban is biztosítható az alacsony torlódás és a megfelelő QoS szint. Az 5G felhasználási esetek (virtuális valóság, autonóm járművek, ipari IoT) szempontjából kulcsfontosságú az alacsony átviteli késleltetés és a nagy áteresztőképesség. Az adaptív erőforrásallokációval a C-RAN is hozzájárul ezen kritériumok teljesüléséhez. A menedzsment feladatok központosításával nagyobb rálátást kapunk a hálózati infrastruktúrára, tovább növelhető a hálózatba épített intelligencia szintje, illetve a lehetőség nyílik szofisztikáltabb optimalizálási algoritmusok használatára. Nem utolsó szempontként a hálózati skálázhatósága is jelentősen növekszik akorábbi technológiákhoz képest. A C-RAN technológia alkalmazása nélkül nem lennének kiaknázhatóak azok a megnövelt képességek, melyeket egy 5G hálózat nyújtani képes mind teljesítményben, mind funkcióban.

9.5 Open RAN koncepció

Az Open RAN egy hálózati architektúra és technológiai koncepció, amelynek célja a RAN összetevőinek szétbontása és szabványosítása, amely magában foglalja az alapsávi egységet (BBU) és a rádióegységet (RU). Fontos továbblépés, hogy az O-RAN kiterjeszti a C-RAN-ban megjelenő szétválasztás koncepcióját a szabványosítás igényével. Ez a megközelítés nagyobb rugalmasságot, interoperabilitást és innovációt tesz lehetővé a vezeték nélküli hálózatok tervezésében és telepítésében.
Kulcs megkülönböztető tulajdonságok:

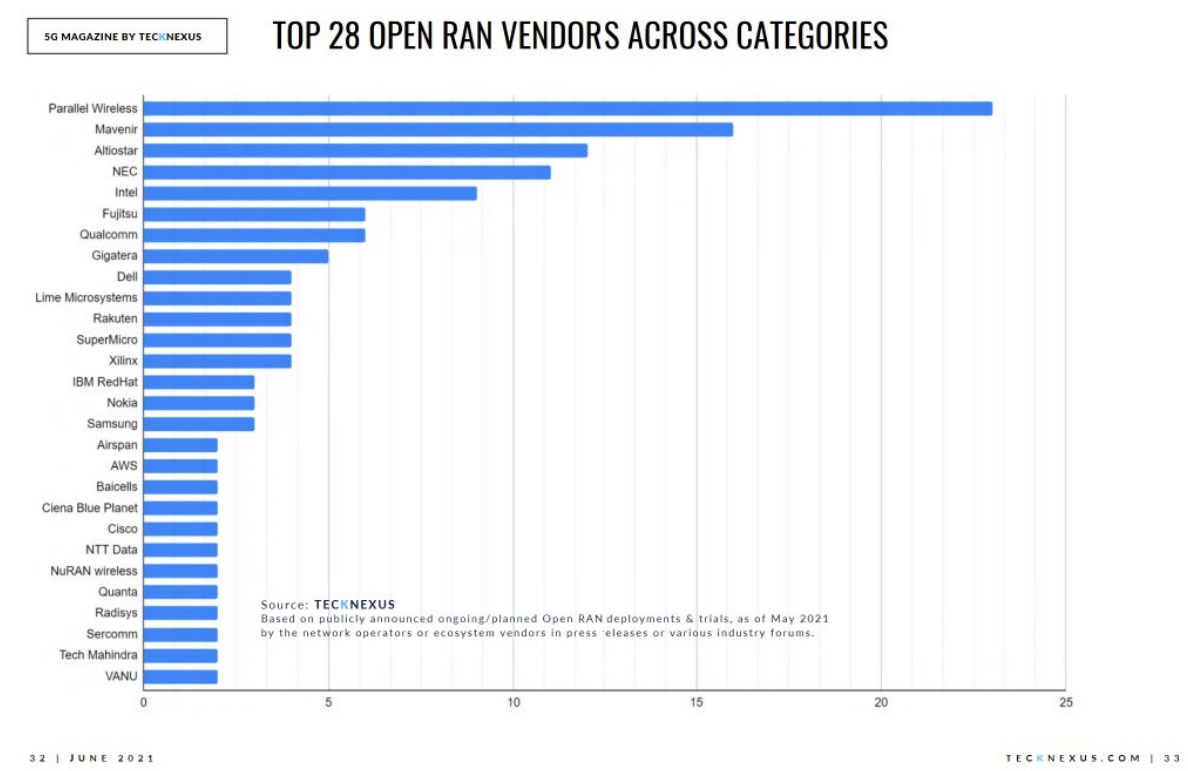
- Több-beszállítós ökoszisztéma: Az Open RAN egy több gyártóból álló ökoszisztémát hoz létre, ahol a szolgáltatók rugalmasan választhatják ki a különböző beszállítóktól származó alkatrészeket. Ez a verseny több innovációhoz és költséghatékonyabb megoldásokhoz vezethet.
- Interoperabilitási teszt: Az Open RAN kezdeményezések gyakran tartalmaznak interoperabilitási tesztelést annak biztosítására, hogy a különböző gyártók összetevői hatékonyan működjenek együtt. Ez segít garantálni a kompatibilitást és a megbízhatóságot.
- Alacsonyabb teljes tulajdonlási költség (TCO): Azáltal, hogy nagyobb szállítói versenyt és interoperabilitást tesz lehetővé, az Open RAN képes csökkenteni a RAN-

berendezések telepítésének és karbantartásának költségeit, ami végső soron alacsonyabb TCO-hoz vezet a hálózatüzemeltetők számára.

- Különféle felhasználási esetek támogatása: Az O-RAN különösen előnyös lehet olyan esetekben, ahol speciális követelményekre vagy speciális konfigurációkra van szükség, például magánhálózatokban, vidéki telepítésekben vagy ipari IoT-alkalmazásokban.

9.5.1 Az Open RAN támogatása

- Legfontosabb gyártók: Parallel Wireless, Nokia, Ericsson, Samsung, NEC, Fujitsu, Mavenir, Xilinx, Intel, Qualcomm (lásd 55. ábra[145])
- Legfontosabb operátorok: AT&T, Chine Mobile, Deutsche Telekom, DoCoMo, Orange, Vodafone



55. ábra A top 28 legfontosabb Open RAN gyártó

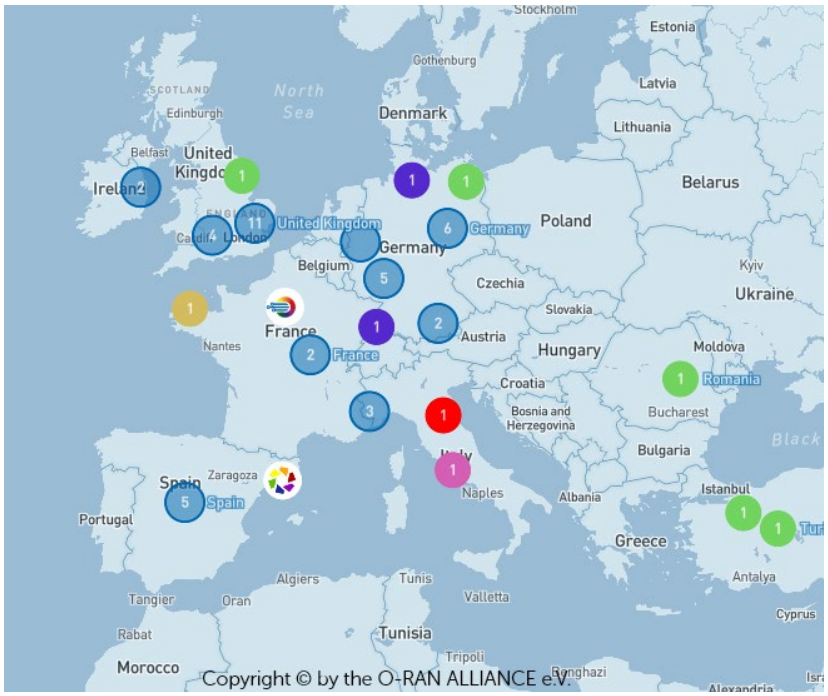
9.5.2 Open RAN produktív tesztüzemek

- Vodafone UK, 2022. január 21., Bath, UK
- BT és Nokia, 2022. január 26., Hull, UK
- O2 és Telefonica, 2022. január 17., München, Németország
- KT, Docomo és Fujitsu, 2022. január 6., együttműködési tesztlabor, Dél-Korea
- Vodafone Germany, 2023, Arnstorf környéi vidéki környezetben, Németország

A Vodafone 2023-ban további európai helyszíneken teszteli élesben az O-RAN technológiát és bejelentette, hogy 2030-ra az Európai hálózatai 30%-át O-RAN technológiával tervezi felszerelni.

[145] https://tecknexus.com/5g-network/the-top-openran-vendors-across-categories/

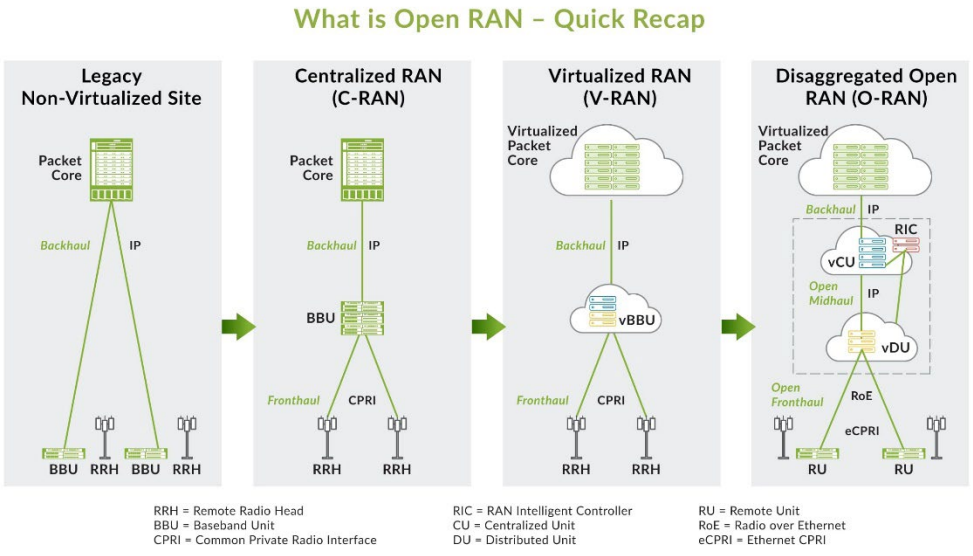
A jelenlegi O-RAN telepítéseket az Európai Unióban a 56. ábra[146] mutatja be.



56. ábra ORAN telepítések az Európai Unióban

9.6 C-RAN és O-RAN összehasonlítása

Mind az Open RAN, mind a Cloud RAN innovatív megközelítés a rádió-hozzáférési hálózatok modernizálására és hatékonyságának javítására. Mindkét megközelítésnek megvannak a maga erősségei és potenciális előnyei, és a választás a konkrét felhasználási esetektől és követelményektől függ (lásd 57. ábra[147]).



[146] https://map.o-ran.org/

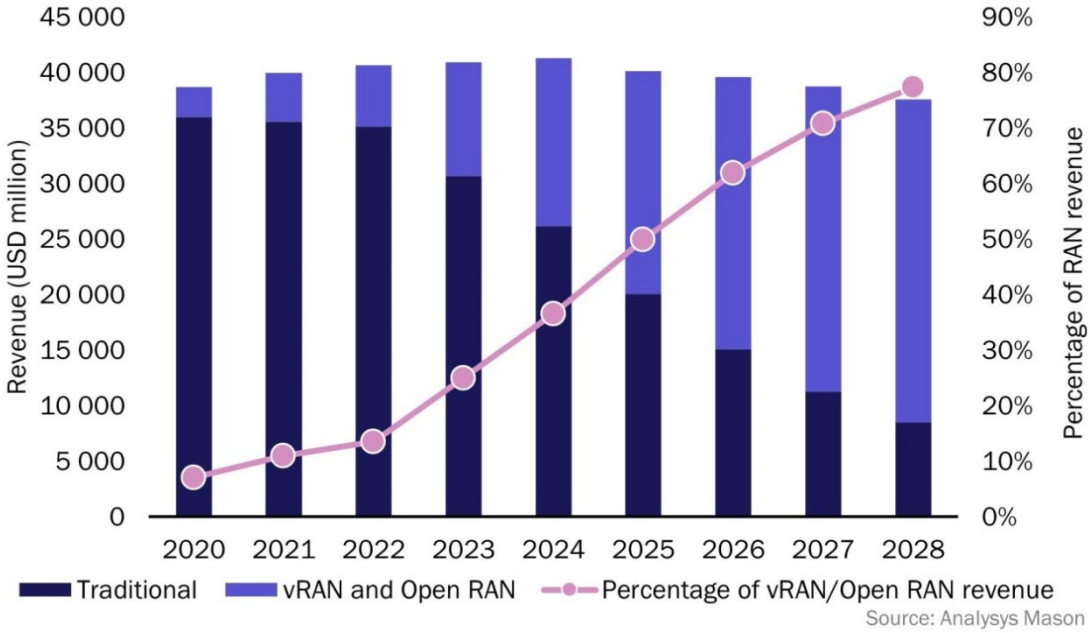
[147] https://www.juniper.net/us/en/research-topics/what-is-open-ran.html

57. ábra RAN modellek összehasonlítása

- Szállítói rugalmasság:
  - Open RAN: Több gyártóból álló ökoszisztémát támogat, lehetővé téve az operátorok számára, hogy különböző gyártóktól válasszanak összetevőket. Ez elősegíti a versenyt és az innovációt a piacon.
  - C-RAN: Általában integrált megoldást foglal magában, amelyet egyetlen szállító biztosít. Bár sok szempontból optimalizált megoldást kínálhat, korlátozhatja az operátor rugalmasságát az egyes alkatrészek kiválasztásában.
- Interoperabilitás:
  - Open RAN: Szabványosított interfészekre támaszkodik, amelyek megkönnyítik az együttműködést a különböző gyártók összetevői között. Ez csökkenti a szállítói bezárkózást és a segíti a hálózattervezés rugalmasabbá tételét.
  - C-RAN: Saját interfészekkel és protokollokkal rendelkezhet, ami potenciálisan zártabb ökoszisztémához vezethet.
- Költséghatékonyság:
  - Open RAN: A verseny és a szabványosítás előmozdításával az Open RAN költségmegtakarítást eredményezhet, mivel lehetővé teszi az üzemeltetők számára, hogy a költségek, a teljesítmény és a konkrét használati esetek követelményei alapján válasszanak ki összetevőket.
  - C-RAN: Bár a C-RAN rendkívül optimalizált megoldást kínál, magasabb kezdeti beruházási költségekkel és potenciálisan nagyobb függőséggel járhat egyetlen szállítótól.
- Skálázhatóság és rugalmasság:
  - Open RAN: Széttagolt jellege miatt nagyobb skálázhatóságot és rugalmasságot biztosít. Az üzemeltetők saját hálózati követelményeik alapján választhatnak összetevőket, és egyszerűen frissíthetik vagy cserélhetik az egyes elemeket.
  - C-RAN: Speciálisabbak és szorosan integráltak lehetnek, ami kiemelkedő teljesítményt eredményezhet, viszont kevésbé rugalmasak a testreszabhatóság szempontjából.
- Innováció és verseny:
  - Open RAN: Versenykörnyezetet ösztönöz, ahol a különböző gyártók hozzájárulhatnak az innovációhoz és a RAN-technológiák fejlődéséhez.
  - C-RAN: Bár a C-RAN rendszerek gyártói is képesek innovációra, a verseny szintje korlátozottabb lehet az ökoszisztéma potenciálisan zártabb természete miatt.

Végső soron az Open RAN és a C-RAN közötti választás több tényezőtől függ: i) a hálózat speciális követelményei, ii) a szolgáltató preferenciái és iii) a meglévő infrastruktúra. Mindkét megközelítésnek megvannak a maga előnyei, és jelentős előnyökkel járhat a mobilhálózatok kiépítésében. Összességében elmondható, hogy a következő öt éves időszakban az O-RAN technológia jelentős elterjedése prognosztizálható (lásd 58. ábra[148]).

[148] https://www.analysysmason.com/research/content/articles/mwc-open-ran-rma18/



58. ábra A hagyományos gyártói RAN-ok és a C-RAN/ORAN piaci részesedése a következő öt évben

9.7 Open RAN biztonsági problémák

A szakértői vizsgálatok arra jutottak, hogy az Open RAN jelenlegi fejlettségi szintjén potenciális biztonsági kockázatokat rejt magában. 2022 májusában az Európai Unió közzétett egy jelentést az Open RAN biztonságáról, amely felsorolta a lehetséges aggályokat, beleértve a nagyobb támadási felületet, a hibás konfiguráció fokozott kockázatát, az erőforrások megosztása miatti egyéb hálózati funkciókra gyakorolt hatások kockázatát, valamint a kiforratlan specifikációkat. Az O-RAN Alliance által gondozott specifikációkban kevés szó esik a biztonságról, megállapítható, hogy a biztonság nem szerepel az O-RAN technológiában elsődleges tervezési szempontként. A jelentés szerint az O-RAN újfajta kritikus függőségekhez vezethet a felhőkomponensekben.
A legfontosabb biztonsági aggályok:

- Felhőalapú vezérlés: az 5. generációs mobilhálózat az első teljesen felhőalapú kommunikációs infrastruktúra, így hasonlóan érintik a felhőhöz kapcsolható fenyegetettségek, mint az interneten elérhető nyilvános felhőszolgáltatásokat.
- A hardvergyártók egyre szélesedő köre: nehezen biztosítható, hogy minden komponens-gyártó azonos színvonalú biztonságok valósítson meg az eszközeiben. A hardver tervezési kódokat jelentősen nehezebb feladat biztonsági szempontból elemezni, mint a szoftveres forráskódokat.
- Jelentősen megnövelt komplexitás: újabb absztrakciós réteget, számos új interfész
- Nyílt forráskódú komponensek: a bennük megjelenő kisebb nagyobb hibák teljesen nyilvánosak. Megnőhet az esélye alacsony szintű, RAN-ra irányuló DDoS támadások sikeres kivitelezésének.
- Spektrum megosztása operátorok között: lehetséges interferencia, szolgáltatáskiesés

Az Európai Unió 2021-ben tette közzé az 5G hálózatokra vonatkozó kockázatcsökkentő intézkedések uniós eszköztárát (ToolBox), 2022 májusában pedig a kiberbiztonságról szóló jelentést.

9.8 Peremszámítás integrációja

Az edge computing közelebb hozza a számítási kapacitásokat a felhasználókhoz és az IoT eszközökhoz. Ezzel jelentősen hozzájárul az olyan alacsony és ultra alacsony késleltetésű alkalmazások megvalósításához, mint például a virtuális valóság, autonóm járművek, gyártásautomatizálás, okosváros.

Felhasználási esetek:

- IoT és intelligens eszközök: A peremszámítás létfontosságú az IoT-alkalmazásokban, mivel lehetővé teszi az eszközök számára az adatok helyi feldolgozását és a gyors reagálást.
- Autonóm járművek: Az edge computing lehetővé teszi az autonóm járművek valós idejű döntéshozatalát, csökkentve a központosított szerverektől való függőséget.
- Intelligens városok: Az edge computing különféle alkalmazásokat támogat az intelligens városokkal kapcsolatos kezdeményezésekben, mint például a forgalomirányítás, a környezetfigyelés és a közbiztonság.
- Ipari automatizálás: A peremszámítás kulcsfontosságú az alacsony késleltetést és nagy megbízhatóságot igénylő gyártási és ipari alkalmazásokban.

9.9 Mesterséges intelligencia (gépi tanulás) integrációja

Az automatizálás támogatásával egyre nagyobb teret kap a gépi tanulás a hálózatok és szolgáltatások menedzsment feladatainak elvégzésében. A gépi tanulóalgoritmusok alkalmazása gyorsíthatja az innovatív felhasználási esetek megjelenését és magas minőségű kiszolgálását.

Fontosabb menedzsment területek, ahol az AI hatékonyan alkalmazható:

- Dinamikus erőforrásallokáció
- Forgalommenedzsment
- Biztonsági incidensek kezelése
- Karbantartási feladatok előrejelzése

9.10 Network Slicing

A network slicing technológia lehetővé teszi egyetlen fizikai hálózati infrastruktúra felosztását több virtuális hálózatra, amelyek mindegyike egyedi felhasználási esetekre és alkalmazásokra van szabva (pl. rendkívül megbízható alacsony késleltetésű kommunikáció kritikus alkalmazásokhoz, továbbfejlesztett mobil szélessáv a nagy sebességű internethez stb., lásd 59. ábra[149]). Mindegyik hálózati szelet önálló hálózatként működik, egyedileg definiált specifikus karakterisztikával és erőforrásokkal. Az 5. generációs hálózatok a dinamikus menedzsmentfunkciók bevonásával új üzleti modellek létrejöttét is támogatják.

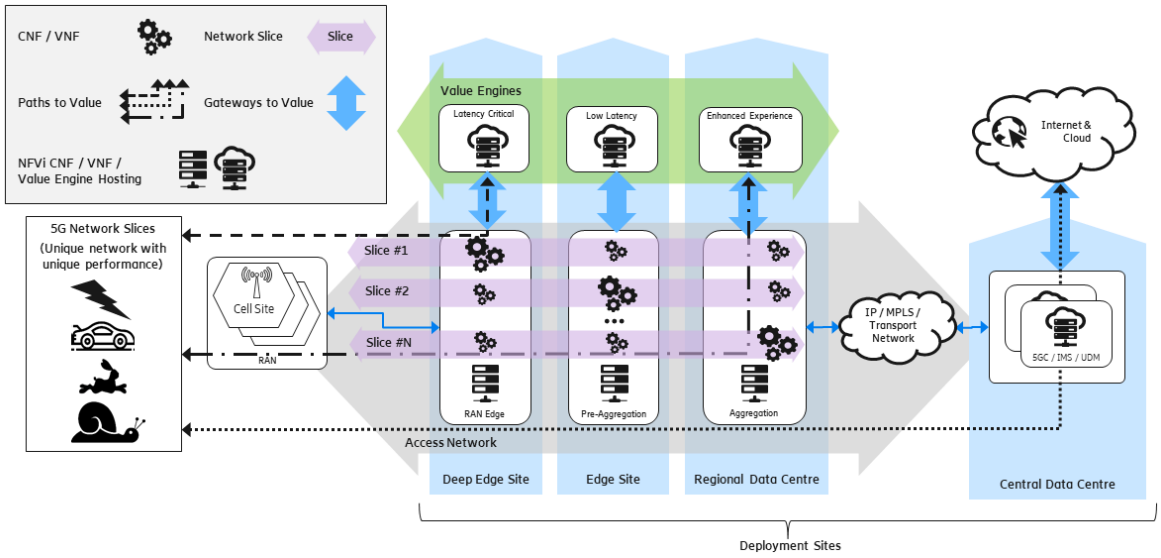
Legfontosabb előnyei:

- Teljes izoláció a szeletek között: az egyik virtuális hálózati erőforrásai nincsennek hatással a többi virtuális hálózat teljesítményére. Ez a tulajdonsága különösen nagy előnyt jelent kritikus alkalmazási esetekben.

[149] https://just.graphica.com.au/an-introduction-to-5g-architecture/

- Minden szelet egyedileg testreszabható: sávszélesség, késleltetés, megbízhatóság és biztonság
- Dedikált erőforrások a teljes átviteli útvonalon: rádiós, szállítási és maghálózati erőforrások
- Végponttól végpontig menedzselhető szeletek
- Dinamikus erőforrásallokáció valósidejű igények alapján

A network slicing technológia kiemelt felhasználási területei: autónóm járművek, ipari IoT, okosváros.



59. ábra 5G network slicing áttekintés

9.11 Privát LTE és 5G hálózatok

A nyilvános hálózatokkal szemben a privát mobilhálózatot egy szervezet egyedi kommunikációs céljaira hozzák létre. A teljes hálózat a szervezet specifikus üzleti céljai szerint kerül kialakításra. Ezeket a hálózatokat általában egy meghatározott földrajzi területen, például egyetemen, gyárban, kikötőben vagy más ipari vagy vállalati környezetben használják.

A privát LTE/5G hálózatok legfontosabb jellemzői és előnyei:

- Dedikált és ellenőrzött: A privát hálózatok kizárólag egy szervezet tulajdonában vannak, így üzemeltetési szempontból teljes ellenőrzést biztosítanak a hálózati erőforrások, a biztonsági szabályzatok és a konfigurációk felett.
- Nagy megbízhatóság és alacsony késleltetés: A magánhálózatokat nagy megbízhatóságra és alacsony késleltetésre tervezték, ami kulcsfontosságú az olyan alkalmazásokhoz, mint az ipari automatizálás, az autonóm járművek és a kritikus kommunikáció.
- Fokozott biztonság: A vállalatok képesek saját biztonsági protokolljaikat és intézkedéseiket megvalósítani, így a privát hálózatok a nyilvános telepítésekhez képest magasabb szintű ellenőrzést és biztonságot nyújtanak.
- Testreszabott szolgáltatásminőség (QoS): A magánhálózatok lehetővé teszik a szervezetek számára, hogy meghatározott QoS-paramétereket határozzanak meg és

kényszerítsenek ki, biztosítva, hogy a kritikus alkalmazások megkapják a szükséges sávszélességet, késleltetést és megbízhatóságot.

- Spektrum kiosztás: A vállalatok megszerezhetik és kezelhetik saját spektrumlicenceiket, így magasabb fokú ellenőrzést biztosítanak a rendelkezésre álló frekvenciák felett, és csökkentik a többi felhasználó által okozott interferenciát.
- Kapacitás és lefedettség optimalizálása: A magánhálózatok úgy alakíthatók ki, hogy megfeleljenek bizonyos kapacitás- és lefedettségi követelményeknek, a tervezett felhasználási esetekhez és alkalmazásokhoz optimalizálva a teljesítményt.
- IoT és ipari automatizálás: A magánhálózatok kiválóan alkalmasak nagyszámú IoT-eszköz támogatására, és lehetővé teszik az automatizálást ipari környezetben.
- Elszigetelés a nyilvános hálózatoktól: A magánhálózatok el vannak szigetelve a nyilvános mobilhálózatoktól, ami a biztonság és a teljesítmény szempontjából is fontos lehet.
- Megfelelőség és szabályozási ellenőrzés: A szervezetek saját hálózati infrastruktúrájuk kezelésével biztosíthatják az iparág-specifikus előírásoknak és szabványoknak való megfelelést.
- Költséghatékony megoldások: Bizonyos esetekben a magánhálózatok költségmegtakarítást jelenthetnek a nyilvános hálózatokra való támaszkodáshoz képest, különösen nagy adatforgalmat vagy speciális csatlakozási követelményeket támasztó környezetekben.

A privát LTE és 5G hálózatok iránt jelentős érdeklődés mutatkozik, különösen az olyan iparágakban, mint a gyártás, az egészségügy, a közlekedés, a közművek és az intelligens városok. Lehetővé teszik a szervezetek számára, hogy ellenőrzött és biztonságok környezetben aknázzák ki a fejlett vezeték nélküli technológiákat a kritikus fontosságú alkalmazásokhoz, és kihasználják az olyan feltörekvő technológiák előnyeit, mint az IoT és az automatizálás.

9.12 A közeljövő várható irányai

A bemutatott képességek és funkciók együttesen egy olyan a jövő felé mutatnak, ahol a mobilhálózatok az alkalmazások széles skálájának szerves részét képezik, és hatással lesznek az iparágakra, az egészségügytől és a közlekedéstől a szórakoztatásig és a gyártásig. A mobilhálózatok folyamatos fejlődése döntő szerepet fog játszani a jövő digitális világának kialakításában. Az 5G generációs kommunikációs hálózatok terjedésének (18% CAGR a következő öt évben) és az általuk nyújtott szolgáltatások fejlődésének egyik erőteljes katalizátora lehet a fent tárgyalt Open RAN technológia. Mind európai, mint globális szinten egyértelmű tendencia az első O-RAN hálózatok megjelenése produktív környezetben. A következő években exponenciális növekedést várunk az O-RAN technológiát alkalmazó kommunikációs hálózatok számában. A nemzetközi mobilszolgáltatók (kiemelve a Vodafone törekvéseit és a már létrehozott O-RAN laboratóriumait) integrációs laboratóriumok létrejöttét szorgalmazzák, melyekben az Open RAN gyártók együttműködve, integráltan tesztelhetnek komplett rádiós hálózatokat a megrendelőnek történő átadást megelőzően. A technológia jövőjét tekintve további fontos tényező, hogy az O-RAN támogatói között az új piaci szereplők mellett megjelentek a klasszikus távközlési gyártóvállalatok is, mint a Nokia, az Ericsson és a Samsung. Várhatóak olyan új, elsősorban ipari felhasználási esetek, melyek

kiemelten és átfogóan kezelik a valósidejűségi kritériumot: nem csak a kommunikációsban, hanem az adatok feldolgozásában, elemzésében és az automatizált döntéshozatalban is megjelentik elvárásként. Az 5. generációs mobilhálózatok ipari elterjedésével a peremszámítástechnika is egyre jelentősebb szerephez jut a fenti kritériumok teljesítésében. Az 5G hálózatokon megjelenő alkalmazások széles spektruma a hálózat- és szolgáltatásmenedzsment feladatokat is jelentősen komplexebbé teszi. A napi üzemeltetési feladatok jelentős részének automatizálása elkerülhetetlenné válik a megfelelő szolgáltatásminőség fenntartásához. Erre válaszul az elmúlt években megjelentek a mesterséges intelligencia alapú technológiák a hálózatmenedzsment és kiberbiztonsági rendszereben, melyek segítségével a feladatok egy részére a human-in-the-loop működésről az operátorok átállhattak human-on-the-loop megközelítésű működésre, ezzel jelentősen tehermentesítve a hálózati és biztonsági adminisztrátorokat.

10 Online platformok

Az online platformok a jelenkori Internet fejlődésének, bővülésének hajtómotorjai. Ezt az állítást arra a tényre alapozhatjuk, hogy az internet hozzáférési szolgáltatás segítségével a világhálóhoz kapcsolódó előfizetőket az online platformok által nyújtott szolgáltatások és tartalmak felhasználókká és fogyasztókká „alakítják át". Az előfizetői szokások és igények változása pedig a fejlesztések kiindulópontja tulajdonképpen minden, az Internet működéséhez, szabályozásához és fejlesztéséhez kapcsolódó területen (többek között, de nem kizárólagosan ilyenek például a sávszélesség bővülése, a valósidejű szolgáltatások igénybevételének lehetősége, a válaszidő csökkenése, a biztonság növekedése, a rendelkezésreállás és a megbízhatóság növekedése, a mobilitás, a személyiségi jogok védelme).
Az alábbiakban tárgyalt platformok közül nyilván vannak ismertebbek és népszerűbbek, és vannak olyanok is, amelyeknek a felhasználói köre az előzőekhez képest lényegesen kisebb. Például nyilvánvaló, hogy az Internet forgalmának túlnyomó része, mostanra akár háromnegyede is, hosszabb-rövidebb videók átviteléből származik, de ez nyilván nem jelenti azt, hogy összességében a videómegosztó platformok és a streaming szolgáltatók ügyfélköre biztosan a legnagyobb. Ebből is levezethető, hogy a különböző platformok a sajátos jellegzetességeik miatt külön-külön is mind fontosak a technológiai fejlődés szempontjából. Mielőtt az egyes platformokat részletesebben bemutatnánk, meg kell jegyeznünk, hogy az egyes alkalmazások/szolgáltatások besorolása sokszor nem egyértelmű, némelyik több platformnak a jellemző sajátosságait is magán viseli. Sőt a fejlesztések iránya is az, hogy egyre több szolgáltatást nyújtó, minél inkább univerzálisan felhasználható és ezért minden másik alkalmazás használatát feleslegessé tevő[150], egy tulajdonosi kézben lévő ökoszisztémák jöjjenek létre. Ezeket nagyon jól példázzák az Alphabet és a Meta törekvései.

10.1 Információk és tartalmak online megosztását lehetővé tevő szolgáltatások (webes fájltárolás és -megosztás)

Ha általánosan tekintjük, az Internet és benne kifejezetten a World Wide Web a magánszemélyek közötti elterjedése óta arra szolgál, hogy információkat és tartalmakat osszunk meg általa. A több évtizede divatosnak és ismertnek számító protokollok és szolgáltatások (például az FTP vagy a Gopher) is pontosan ilyen igények kielégítésére jöttek létre. Tanulmányunk jelen részében ezeknek a szolgáltatásoknak egy lényegesen kisebb halmazát tekintjük át, nevezetesen a webes fáljtárolást és fáljmegosztást. Ez még mindig egy nagyon széles területet takarhat, amibe a torrentoldalakat éppúgy bele lehet érteni, mint a

[150] Egyre több esetben látjuk azt, hogy az univerzális internetes ökoszisztémák fejlesztése során a technológiák és a szolgáltatások szabad versenyét gátló vagy éppenséggel ellehetetlenítő megoldások születnek. Fontos lépésnek számított 2009-ben, hogy az Európai Bizottság arra a kötelezte a Microsoftot, hogy az operációs rendszereiben a szabad böngészőválasztást már telepítéskor lehetővé tegye. A döntés ugyan csak 2014-ig volt érvényben, de a böngészőpiacot teljesen átrendezte (lásd még: https://pcforum.hu/hirek/16720/kiszedte-a-bongeszovalasztot-a-windows-okbol-a-microsoft). Annak a döntésnek a legnagyobb haszonélvezője a Google lett, amelynek Chrome böngészője dominánsá vált.
Ma hasonló helyzet állt elő Google keresőmotorját illetően, amely monopolhelyzetbe került, amellyel sokak szerint vissza is él (lásd többek között itt: https://hirado.hu/kulfold/cikk/2023/06/14/az-eu-szerint-a-google-visszael-erofolenyevel-az-unios-hirdetesi-piacon/ vagy itt: https://index.hu/kulfold/2023/09/12/egyesult-allamok-google-monopolhelyzet-trosztellenes-torveny-per-birosag/).

bizonyos típusú médiatartalmak – például képek – megosztására szerveződött szolgálatatásokat, úgymint a Photobucket, a Pinterest, a Tumblr, a Reddit és még számtalan másik. Ha elég szűkre húzzuk az értelmezés lehetőségét, akkor leginkább a következő kritériumokat fogalmazhatjuk meg:

- Webes szolgáltatás, tehát mind a fájl elhelyezése, mind annak elérése leginkább – legtöbbször kizárólagosan – a HTTP(S) protokoll felhasználásával egy böngészőn keresztül történik.
- Az elhelyezett és elért digitális állományoknak, vagyis a fájloknak, nincs valamilyen jellemző szűkítő értelmet hordozó jelzőjük vagy jellemzőjük, tehát például nem képek vagy éppen nem programkódok. A szolgáltatás tehát nem bizonyos speciális típusú állomány kezelésére jött létre (lásd a képekre a fentebb felsorolt példákat, a programkódokra pedig a GitHub-ot), hanem tulajdonképpen bármilyen digitális állományra alkalmazható[151].
- A fálj elhelyezése történhet kizárólag tárolási céllal, de a különböző megosztási lehetőségeket használva a felhasználók a tárolt állományaik egy halmazát vagy egészét elérhetővé tudják tenni más felhasználók számára is akár az elhelyezés után közvetlenül, akár számottevően később. Általánosan elmondható, hogy az állomány elhelyezője és az elérést kezdeményező személyek között valamilyen kapcsolat áll fenn, amelyre, illetve itt a fájl elhelyezésének megtörténtére is az elhelyező a rendszeren belül vagy azon kívül figyelmeztetni tudja a partnereit.

10.1.1 Fájltároló és megosztó szolgáltatások

Elvileg megkülönböztethetünk file hosting és file sharing rendszereket, azonban ezek ma már nem igazán léteznek ilyen tiszta állapotban. Sőt, a legtöbb ilyen rendszerhez már számtalan egyéb szolgáltatás is kapcsolódik, például a felhasználói könyvtárral való szinkronizálás, vagy éppen az ütemezett biztonsági mentés. Ezek rendszerek ma már többnyire felhőalapúak, értelemszerűen a nagy felhőszolgáltatók (Amazon, Google, Microsoft) önálló platformokat is nyújtanak, amelyek egyébként a piacai felmérésekben a népszerűségi vagy ismertségi listák első felében szerepelnek, ugyanakkor konkrét piaci arányokat nagyon nehezen állapíthatunk meg, mivel az egyes elérhető elemzések jelentős eltéréseket mutatnak, ráadásul a vizsgálat vagy akár csak a rangsorolás módszertana sem teljesen világos a legtöbb esetben. Ezen felül még hozzá kell tennünk, hogy a digitális állományok online tárolására és megosztására szolgáló platformok sok esetben nem önállóak, hanem egy-egy fokozatosan kialakuló, manapság is bővülő szolgáltatáshalmazú kollaboratív szoftvercsomag részei, ami azzal is jár, hogy magának a file hosting és sharing szolgáltatásoknak az ismertsége vagy népszerűsége nem választható el a kollaboratív rendszer felhasználói körének nagyságától.

Az ismert nagy felhőszolgáltatók mellett mindenképpen említeni kell még tőlük független szereplőket, akik többnyire tényleg csak a fájltárolással és –megosztással foglalkoznak, illetve az ezekkel szorosan összefüggő szolgáltatásokat nyújtanak. A legismertebbek ezek közül a Box, a Dropbox, a Baidu Wangpan, a MediaFire, a Mega és még talán a Yandex. Ez utóbbi leginkább Oroszországban népszerű, a Baidu Wangpan leginkább Kínában, míg a többiek nemzetköziek. Azt látnunk kell, hogy ebben a szegmensben nagyon jelentős a technológiai vagy gazdasági alapú piaci mozgás, vagyis az elmúlt évtizedek trendjei alapján eléggé valószínűnek mondható, hogy 10 éven belül az ebbe a csoportba sorolható szolgáltatások

[151] Egészen pontosan a típusa lehet bármilyen, viszont ha túlságosan nagy lenne a mérete, akkor az problémákat okozhat.

jelentős része – akár a fele is – már nem lesz elérhető. Korábban ismert, de ma már nem létező szolgáltatásokra példaként említhetjük a Copy.com-ot, a Fileserve-t, a Hotfile-t, a Megauploadot, a RapiShare-t vagy éppen a Yahoo! Briefcase-t.
Egy külön csoportot képez egymagában az Apple iCloud szolgáltatása, amely nemcsak az állományok – elsősorban a felhasználó által készített saját médiatartalmak és a biztonsági mentések – hosszútávú, biztonságos és kényelmes tárolására szolgál, hanem emellett levelezési lehetőséget, illetve a kontaktlista és a naptár szinkronizálására is lehetőséget nyújt. Ennél is lényegesebb azonban az, hogy több rendszerszolgáltatás és az Apple által fejlesztett applikáció (például Apple Home, Apple Wallet, Safari, Siri, stb.) számára az iCloud a backend. Mivel ezek az Apple-ökoszisztéma legfontosabb részei, amelyek kiemelten szolgálják a felhasználók kényelmét és biztonságát, ezért az iCloud előreláthatólag hosszútávon a piac jelentős szereplője lehet.

10.1.2 A fájltároló- és megosztó szolgáltatások megbízhatósága és biztonsága

Az információk és tartalmak online tárolására és megosztására szolgáló rendszerek legfontosabb „értékei" a rendelkezésreállás és a biztonság. Könnyen belátható, hogy az éppen elérhetetlen tárhely nemcsak a közösen végzett munkát és az együttműködést teszi lehetetlenné, hanem a kizárólagos felhős tárolás esetén az önálló munkát is. „Biztosításként" az ilyen szolgáltatók némelyike lehetőségként felajánlja az aktuálisan használt állományok lokális tárolását[152] és a szinkronizálást. Ennek a biztonsági szempontok mellett az is az indoka, hogy ezáltal lényegesen ritkábban kell a hosting szolgáltató tárterületét elérni, ami nemcsak a szolgáltató számára takarít meg erőforrást, hanem a hálózati forgalmat is csökkenti.
Az file hosting szolgáltatások adatbiztonsági kérdésein sokszor átsiklanak az elemzések. Való igaz, hogy a megfelelően erős jelszó esetén a felhasználói fiókok feltörése elég hosszú időbe telik ahhoz, hogy ne érje meg. Ezen felül a tárolt állományokat túlnyomórészt titkosítják és titkosított a feltöltés és a letöltés adatfolyama is. Ne felejtsük el azonban, hogy amiként a torrent által letöltött állományok egy része fertőzött lehet, a file hostingon keresztül is letölthetünk a saját tárterületünkre rosszindulatú kódokat tartalmazó állományt. Ezen felül egy nem olyan régen (2023. augusztus 18-án) történt eset[153] rávilágít arra, hogy elegendő egyetlen lyuk a biztonsági protokollon ahhoz, hogy egy felhőszolgáltató által kezelt **összes adat elvesszen** – az elosztott és redundáns tárolás ellenére.
A korábbi rendszereket sokszor el lehetett érni FTP-n keresztül is, ma már ehelyett webes elérésen vagy éppen a szolgáltató által kényelmesebbnek és biztonságosabbnak mondott saját applikáción keresztül lehet a távoli tárterületen az állományokat elhelyezni. A letöltésre legtöbbször a webes felület használatos.

10.1.3 Speciális fájltároló- és megosztó rendszerek és a magyar piac

A fáljmegosztó rendszerek egyik meglehetősen speciális fajtájához tartozik a Jumbomail, amelynek már neve is arra utal, hogy nagyon nagy méretű digitális állományok elektronikus levélben való továbbítását lehet vele megoldani. Erre az azért van szükség, mert gyakorlatilag mindegyik levelező program korlátozza az elküldhető levél maximális méretét. Ennek elsősorban biztonsági okai vannak és az asztali levelezőprogramokra, az applikációkra

[152] Alapvetően ez az aktuális számítástechnikai eszközy háttértárát jelenti, de nyilván a lokális hálózaton elhelyezett NAS is használható erre a célra.
[153] https://sg.hu/cikkek/it-tech/154987/bunozok-tonkretettek-a-cloudnordic-dan-felhoszolgaltatot

vagy a webes levelezőkre egyaránt fennáll, noha a korlátok különbözőek lehetnek[154] (például GMail: 25 MB a küldésnél és 50 MB a fogadásnál, Outlook: 20 MB). A mostani levelezőkliensek (pl. a Mozilla Thunderbird) egyébként nagyobb méretű csatolmányok esetében felajánlják, hogy a fájl ne a levélben kerüljön továbbításra, hanem az online tárhelyre feltöltött állomány linkjét tegyük csak a levélbe. A Jumbomail szolgáltatás erre kínál megoldást, bár méretkorlát ott is létezik, viszont az 1 TB. A címzett értesítést kap a különleges üzenetről és külön kell kezdeményeznie a nagyméretű csatolmány letöltését és értelemszerűen a postafiókban elmentett levél nem foglal el túlzott méretű tárhelyet, hiszen a csak egy értesítést tartalmaz a nagyméretű csomagról, nem magát a csomagot. A Jumbomail valamilyen szinten tárolásra is felhasználható, de arra kényelmesebben használható megoldások is léteznek.

Magyarországon a széleskörben használt külföldi eredetű rendszerek mellett már hosszú ideje létezik a Data.hu, ami a Mediafire-hez, vagy a korábbi Megauploadhoz vagy Rapidshare-hez hasonlóan megkülönböztet normál és prémium ügyfeleket. A prémium ügyfelek azok, akik fizetnek a szolgáltatás igénybevételéért, tipikusan a letöltésért. A prémium ügyfelek a tagságuk miatt különböző előnyökhöz jutnak (például reklámmentesség, azonnali letöltés, korlátlan letöltési sávszélesség és adatmennyiség, több állomány párhuzamos letöltési lehetősége, letöltésvezérlő használatának lehetősége, stb.). A szolgáltatás a prémium tagok befizetéséből és reklámkihelyezésből tartja fenn magát és azokat a feltöltőket, akinek a megosztott állományai jelentős forgalmat generálnak prémium tagsággal jutalmazza.

10.2 Közösségi hálózat

A közösségi hálózatok – vagy ha technikailag pontosabban akarunk fogalmazni, akkor a közösségi hálózatok tagjai közötti kommunikációt támogató platformok – széleskörű megjelenése és elterjedése a harmadik évezred jelensége. Azzal együtt is mondhatjuk ezt, hogy a social media korai elődei, mint a chat roomok vagy a BBS, már az 1970-es, 1980-as években is léteztek.
Itt kell megjegyeznünk, hogy a magyar terminológiában a social media kifejezést gyakran és régóta használjuk a social networking helyett. Az előbbit közösségi médiaként lehetne leginkább fordítani és hozzá képest a közösségi hálózatépítés eredetileg szűkebb értelmű volt, bár mostanra a jelentések összemosódása az angol nyelvterületen is tapasztalható[155].
A közösségi média olyan interaktív technológiák és virtuális[156] térben végzett tevékenységek összessége, amelyek elősegítik információk, ötletek, érdeklődési körök és egyéb kifejezési formák létrehozását és megosztását virtuális közösségeken és hálózatokon keresztül. Ez a

[154] A méretkorlátot végsősoron természetesen nem a levelező kliens, hanem az levelezést kiszolgáló Mail eXchange (MX) szerver határozza meg.
[155] Ennek oka lehet az, hogy a közösségi média és a közösségi hálózatok nagyon népszerű témát jelentenek, ami azt is implikálja, hogy a róluk beszélők egyre nagyobb hányada nem rendelkezik olyan ismeretekkel, hogy a két kifejezés jelentéstartalmát elkülönítse. Ugyanakkor azt is látnunk kell, hogy a közösségi hálózatok egyre inkább felfalnak és magukba olvasztanak olyan területeket, amelyek korábban a social media más ágai voltak. Ilyen például a hírek, a publicisztikai igényű írások és a videótartalmak megjelenése és egyre nagyobb súlya a közösségi hálózatok hírfolyamaiban.
[156] Itt a „virtuális” szóval arra utalunk, hogy nem személyes találkozás során történik az információ- vagy tartalommegosztás.

definíció persze egyrészt elnagyolt, másrészt nem is fedi le a közösségi média teljes vertikumát, de van néhány közös jellemző:

- A közösségi média szolgáltatások interaktív, Web 2.0 alapú alkalmazások.
- A közösségi média attól közösségi, hogy a tartalmat – például szöveges bejegyzések vagy megjegyzések, digitális fotók vagy videók, valamint az összes online interakció során keletkezett adatok formájában – magának a közösségnek a tagjai generálják vagy némely esetben csak beillesztik az üzenetfolyamba – megosztják – a mások által generált tartalmat.
- A felhasználók szolgáltatás-specifikus profilokat hoznak létre a webhelyhez vagy az alkalmazáshoz, amelyeket a közösségi média szervezet tervez és tart fenn.
- A közösségi média segíti az online közösségi hálózatok fejlődését azáltal, hogy összekapcsolja a felhasználó profilját más egyének vagy csoportok profiljával.

A közösségi kifejezés a médiával kapcsolatban azt sugallja, hogy a platformok felhasználó-központúak és közösségi tevékenységet tesznek lehetővé. Mint ilyen, a közösségi médiát úgy tekinthetjük, mint az emberi hálózatok online elősegítői vagy erősítői – az egyének hálói, akik fokozzák a közösségi kapcsolatokat.

10.2.1 Az ismertebb közösségi hálózatok

A közösségi hálózatok legnagyobbika a 2004-ben létrehozott Facebook, amelynek 2023 végére körülbelül 3 milliárd olyan felhasználója volt, aki egy hónapon belül aktív volt. A napi szinten aktív felhasználók száma ennek kicsivel több, mint kétharmada, míg a hirdetések a havi szinten aktív felhasználó nagyjából háromnegyedét érik el. A Facebook aktív felhasználóinak száma sokáig szinte változatlan ütemben növekedett[157], azonban 2021 második felétől ez a növekedési ütem érezhetően lelassult.

A Messenger eredetileg a Facebook azonnali üzenetküldő szolgáltatásaként indult 2008-ban, de 2011-ben különvált tőle és mostanra többé-kevésbé önállónak is tekinthető, bár a tulajdonosi kör természetesen ugyanaz, ma már a Meta. Az eredeti funkcióin túl természetesen beszélgetésre is alkalmas, valamint 2020 áprilisa óta a Messenger Rooms nevű funkciója révén akár 50 fős videókonferencia hívások lebonyolítására is használható. A Messenger aktív felhasználóinak száma az utóbbi az utóbbi időszakban 1 milliárd[158] közül ingadozott körülbelül +/-100 milliós eltérésekkel, amellyel a WhatsApp és a Weixin/WeChat mögött észrevehetően lemaradva a harmadik[159] legnépszerűbb üzenetküldőnek számít.

A WhatsApp eredetileg egy üzenetküldő alkalmazás, amely később egészült ki a VoIP-funkciókkal. A 16-64 éves korosztály körében világszerte a legkedveltebb social media platform, vagyis ezt tekintik legtöbben kedvencüknek[160]. Ezen felül a felnőtt korú keresőképes népességcsoportban ez tekinthető az alapvető social media platformnak. Ez a helyzet megkönnyíti a reklámozni kívánó cégek számára ennek a csoportnak az elérését. A WhatsApp felhasználóinak száma 2023 elején 2-2,5 milliárd körül volt, a fellelhető adatok

[157] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[158] https://www.oberlo.com/statistics/how-many-people-use-facebook-messenger
[159] https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/
[160] https://engage.sinch.com/blog/global-messenger-apps-usage-statistics/

szórása elég nagy[161]. A vállalkozást eredetileg 2009-ben alapították, majd 2014-ben felvásárolta a Facebook (manapság: Meta). A felhasználóinak száma még mindig növekszik, akár évi 100 milliós nagyságrendben is. A Messengerrel együtt meghatározó szereplők az egész világon, amit az a tény is jellemez, hogy nagyjából 10 olyan ország van a Földön, ahol nem a Meta valamelyik gyorsüzenet-küldője a piacvezető. Az együttes növekedési ütemük – amelyből leginkább a WhatsApp veszi ki a részét, észrevehetően meghaladja a Facebookét.

2012 óta szintén a Meta tulajdona az Instagram, amely kép és videomegosztó közösségi platform. Az eredeti, ma már kissé merevnek ható megkötések valamelyest enyhültek mostanára, például 640 pixeles oldalhosszúságú négyzet alapú képek helyett ma már lehet 1080 pixeles méretig feltölteni. Lehetséges a képeket és videókat címkékkel ellátni, illetve ma már természetesen beszélgetni is lehet és elérhető a „story", amelyben egy szekvenciába lehet szervezni a képeket, amely szekvencia 24 órán keresztül érhető el. Az Instagram felhasználóinak száma valamelyest kisebb, mint a WhatsAppé, nagyjából 2,2-2,4 milliárdra tehető, ugyanakkor az Instagram részesedése a Meta bevételeiben 2022-re elérte a 45%-ot[162].

A Twitter – illetve manapság a tulajdonosváltást követő névváltozás óta az X – az előzőleg említettekhez képest egy sokkal kisebb felhasználói közösséggel rendelkező platform. 2023-ban nagyjából 400 millióra tehető a felhasználóinak a száma. Az eredetileg nagyon rövid, az SMS-sel megegyező hosszúságú, 140 karakteres posztokat lehetővé tevő platform komoly hatást gyakorolt az internetes közösségi oldalakon használatos sajátos szleng kialakulására. Az Egyesült Államokbeli felhasználói közösségének köszönhetően az utóbbi évtizedben komoly szerepet játszott az ottani választási küzdelmekben, amely a felhasználóinak táborát is megosztotta.

A WeChat a kínai Tencent techóriás által létrehozott kínai közösségi oldal, a felhasználóinak száma 2022-ben meghaladta az 1,26 milliárdot, az éves bevétele 2021-ben 17,5 milliárd dollár volt, a Tencent bevételének a 19%-a. A WeChat szinte csak Kínában rendelkezik felhasználókkal, ugyanakkor elmondható, hogy szinte valamennyi kínai okostelefontulajdonos a WeChat felhasználója. Részben az anyacég technológiai hátterét felhasználva a WeChat alkalmazás áruházat is működtet, amelyben 2022-ben már 3,5 millió úgynevezett „mini program" volt elérhető. Ezen felül Kína második legismertebb online fizetési platformját is magában foglalja, amelynek 2021-ben 900 milliós ügyfélköre[163] volt már.

10.2.2 A közösségi hálózatok fejlődési irányai

Miközben a közösségi média piac mostanra telítetté vált és úgy tűnik, hogy újabb felhasználókat már csak egymástól tudnak szerezni a kisebb-nagyobb szereplők, a cégek vezetése különböző irányokban keresi a kitörési lehetőségeket. Az elsődleges cél a természetesen a haszon növelése vagy legalábbis fenntartása. Az már most is elmondható, hogy a lépések nem minden felhasználó tetszését fogják elnyerni és adott esetben más, akár

[161] 2 milliárd a https://engage.sinch.com/blog/global-messenger-apps-usage-statistics/ szerint és 2,4 milliárd a https://www.businessofapps.com/data/whatsapp-statistics/ szerint
[162] https://www.businessofapps.com/data/instagram-statistics/
[163] https://www.businessofapps.com/data/wechat-statistics/

a közösségi média szektoron kívüli gazdasági szereplők érdekeit is sérthetik. Néhány ilyen irányt sorolunk fel az alábbiakban:

- Fizikai hálózatba való beruházás, a jelenlét az IXP-ekben. Amíg a tartalomszolgáltatók megtehetik, hogy a legnépszerűbb tartalmakat hálózati szempontból minél közelebb viszik a felhasználókhoz, addig a közösségi média esetén a tartalom tükrözésének nincs sok értelme, nem is igazán megvalósítható teljeskörűen. Azt viszont el tudják érni ezek a nagy piaci erejű cégek, hogy dedikált hálózati kapacitásuk legyen legalább gerinchálózati szinten. Érdemes látni, hogy egy olyan országban is, mint hazánk, ahol egyetlen nyilvános IXP van csak, a Metának 2x100 Gbps-os kapcsolata van hozzá. Ha világszerte megnézzük, akkor két ASN-t használva (63293[164] és 32934[165]) többszáz IXP-hez csatlakozik.
- A felhasználók által előállított médiatartalmak mellett gyártott vagy átvett média is. A közösségi médiától elkanyarodva a szolgáltatás fejlesztése során ezek a platformok eljutottak oda, hogy hagyományos jellegű médiatartalmak jelennek meg rajtuk. A hagyományos médiatartalmakat egyrészt maguk a gyártók (lapkiadók, szerkesztőségek, televízió- vagy rádiócsatornák), másrészt a hagyományos médiát fogyasztó magánszemélyek osztják meg a közösségi oldalakon. A jelenség következtében a hírek és egyéb tartalmak fogyasztása egyre inkább a közösségi médiaplatformokra tevődik át – a világ egyre nagyobb részén a közösségi oldalakat többen tekintik megfelelő hírforrásnak[166] (tehát nem keresnek másikat), mint a hagyományos sajtót, ideszámítva az online lapokat is. Ez a hagyományos média számára káros, mert a saját olvasó hiányában a hirdetési bevételektől elesnek[167], másrészt nekik fizetni kell minden hirdetés után a közösségi oldalak felé. 2021-ben a News Corp. médiabirodalom kezdeményezett bírósági eljárást Ausztráliában a Facebook ellen, amely megegyezéssel zárult. Ugyanakkor kezdeti lépésként a Facebook mindenféle hír megosztását letiltotta az országban. Jelenleg Kanadában zajlik hasonló.[168]
- A felhasználók szórakoztatása (például a Facebookon az Instant Games). A felhasználók saját médiatartalmai és a megosztások kétségkívül érdekesek, szórakoztatóak, izgalmasak, tanulságosak, stb. lehetnek, de a Facebookon már megjelentek a játékok is, amelyek ugyan lényegesen egyszerűbbek és kevésbé látványosak, mint a nagy játékkészítő stúdiók A-listás címei, viszont elfutnak a felhasználó kliensén, ami nagyon sok esetben mobiltelefon vagy tablet és mostanra már elég sok van ahhoz, hogy a szokásos zsánerekből akár többtucatnyiból is lehessen választani. Ezek a játékok[169] bizonyára sikeresen lekötik az ilyen érdeklődésű felhasználókat, ugyanakkor a közösségi média alulról szerveződő mivolta tovább erodálódik ettől, hiszen nyilvánvaló biztonsági okokból a játékok csak a Facebook részletes ellenőrzése és jóváhagyása után kerülhetnek ki.
- Profil igazolás pénzért és fizetett szolgáltatás (Twitter, Facebook). A közösségi média platformok hatalmas és évről évre növekvő bevételei a hirdetések megjelenítéséből fakadnak. Ráadásul a folyamatos felhasználói interakciók elemzése segítségével

[164] https://www.peeringdb.com/net/14490
[165] https://www.peeringdb.com/net/979
[166] Például Ausztrália: https://mandiner.hu/hirek/2021/2/ausztralia-facebook
[167] https://qubit.hu/2020/08/19/ki-fizesse-a-szabad-sajtot
[168] https://mandiner.hu/kulfold/2023/08/disztopia-eloben-kanadaban-sorra-tunnek-el-a-hirek-a-facebookrol
[169] https://www.facebook.com/games/instantgames/

például a Facebook az ügyfelei túlnyomó részét alaposan feltérképezte, ezáltal az ajánlórendszere meglehetősen hatékony. Ugyanakkor a felhasználói nyomás, a személyiségi jogok komolyabb védelme, de főleg a felhasználói tudatosság növekedése miatt ennek várhatóan kisebb szerep jut a közeljövőben. Ezért a nyugati világban ismertebb platformok szinte egységesen abba az irányba indultak el, hogy tulajdonképpen előfizetéses szolgáltatásként értékesítik a rendszereikhez való hozzáférést. Ennek egyik alapja, hogy a fizetős szolgáltatás reklámmentes lesz[170]. A másik állandó bevételt előállító megoldás a felhasználói profilok hitelesítésének díja. A felhasználói profilokat azért kell hitelesíteni, hogy az álprofilok felhasználásával végzett pénzszerzést megakadályozzák. Az igazolási szolgálatás neve Twitter Blue a Twitteren (ma már X), Meta Verified pedig a Meta által koordinált oldalak között. A nagy közösségi média vállalkozások közül legalább részben előfizetéses modellt indított már a Snapchat és a Telegram Messenger is.

10.2.3 A közösségi hálózatokkal kapcsolatos problémák

A közösségi hálózatokkal kapcsolatban időről időre felmerülnek különböző problémák, amelyek közül a jelentősebbeket az alábbiakban próbáljuk összefoglalni:

- A nagyméretű felhasználói bázis és nagyvolumenű hirdetési bevételek jelentős gazdasági szereplőkké tették a platformok tulajdonosait, akik számtalan vélemény szerint ezt másféle területeken, például véleményformálásban, társadalmi befolyásban és politikai hatalomban is érvényesíteni kívánják. Ezzel a törekvésükkel számos érdeket sérthetnek meg. A közösségi hálózatok hagyományos területükön való túlterjeszkedésére több jelet is találunk:
    - Térfoglalás a hagyományos média területein. Fentebb már említésre került, hogy a közösségi hálózatokon a felhasználók által előállított médiatartalmak mellett egyre inkább megjelennek a hagyományos médiából átvett tartalmak, amelyeket a közösségi hálózatok felhasználói osztanak meg. Nyilván ez a megosztás úgy lehetséges, hogy ezek a tartalmak már eredetileg is digitálisan léteznek és a tartalom fogyasztását lehetővé tevő alkalmazás – tipikusan egy böngésző – rendelkezik a közösségi hálózat beépülő moduljával, amely lehetővé teszi a megosztást. Természetesen a felhasználók ezen tevékenységét többnyire elősegíti az adott médium is, amely a tartalmai mellett a tartalomfogyasztók számára megosztási lehetőségeket kínál. A hagyományos tartalomgyártók szándéka nyilván az lett volna, hogy a tartalmaikkal a fogyasztóik közösségi tereiben is megjelennek és ezáltal nagyobb közönséghez jutnak el, magasabb hirdetési bevételekre tesznek szert. Ehelyett már 2020-ra oda[171] jutottunk, hogy az Egyesült Államok felnőtt lakosságának 36%-a rendszeres hírforrásként kezeli a Facebookot, míg a Twitter (ma már X) esetén ez az arány 15% volt. Nyilván ez azt is jelenti, hogy a hirdetési bevételek is a közösségi hálózatoknál jelennek meg, nem pedig a hagyományos médiánál, ami már egészen középtávon is az utóbbi gazdasági ellehetetlenüléséhez vezet.
    - Tényellenőrzés: álhírek. A COVID-19 vírus által okozott járvány idején jelent meg, vagy legalábbis akkor kapott kiemelt hangsúlyt a közösségi oldalak

[170] https://raketa.hu/hamarosan-tenyleg-johet-a-fizetos-facebook
[171] https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/

„tényellenőrzés” névvel illetett tevékenysége, amely névlegesen az adott oldalon megosztott „álhíreket” jelölte meg, illetve szankcionálta az ilyen posztok elhelyezőit. A kimondott cél akkor az volt, hogy a koronavírus fertőzés egészségkárosító hatását vagy éppen a védőoltások hatékonyságát megkérdőjelezőkkel szemben a tudományos tényekre alapozott híreket helyezzék előtérbe. Ez a „tényellenőrzés” ugyanakkor kétségkívül a cenzúra bizonyos formája, a szólásszabadság és a véleményszabadság megsértése, még pedig olyan formában, amit nem lehet alátámasztani bűnüldözési vagy nemzetbiztonsági érvekkel és valószínűleg ezt a bíróságok is indokolatlan korlátozásként ismernék el. Ráadásul a COVID-19 okozta pandémia enyhülésével „tényellenőrzés” nem szűnt meg, inkább a kiterjesztését tapasztaljuk. Ma többnyire valamilyen társadalmi csoport vélt vagy valós sérelmére hivatkozva korlátozzák posztok megjelenését vagy láthatóságát, illetve a felhasználók tevékenységét, valamiféle „népnevelést” megkísérelve ezáltal.

  - Tényellenőrzés: politikai befolyás szerzése. Bár csak az utóbbi két amerikai elnökválasztás esetén kapott globálisan nagy hangsúlyt a közösségi hálózatok politikacsináló, választásokat eldöntő szerepe, bizonyára ezeken kívül is lehetne rengeteg példát hozni az utóbbi évtizedből. Az egyik esetben a közösségi hálózatokon keresztül történő külföldről kezdeményezett befolyásolási kísérletet emlegettek, a másik esetben azonban maguk a közösségi platformok voltak az „elkövetők”, akik az egyik jelölthöz köthető negatív hírek eltusolásával és a másik jelölt posztjai valóságtartalmának megkérdőjelezésével próbáltak hatni a választókra. A gondolat és a véleménynyilvánítás szabadsága ugyan minden embert megillet a demokratikus gondolkodásmód alapján, amíg ez nem korlátozza mások hasonlói jogait, viszont éppen demokratikus politikai szintér fennmaradása érdekében kiemelten fontos az, hogy a politikusok szabadon, cenzúra nélkül kifejthessék a véleményüket. Objektív szempontból vizsgálva a kérdést azt látjuk, hogy ugyanez lenne az érdeke már középtávon is a közösségi média tulajdonosainak is, mivel a szólásszabadság korlátozása a felhasználókat egyrészt eltántoríthatja a közösségi oldal aktív használatától, vagyis posztolástól, másrészt akár a passzív használattól is, vagyis a felhasználó elhagyhatja a szolgáltatást. Mindkettő csökkenti a közösségi média szolgáltató bevételeit. Nyilván a közép- és a hosszútávú érdekeket érvényesítését megelőzheti egy nagyon kockázatos, de kiemelkedő haszonnal kecsegtető lehetőség, ami a politikai szintéren egy magas pozíció elnyerését jelentheti, de erre egyelőre a hagyományos médiából láttunk példát[172], a közösségi média tulajdonosi körét érintve csak pletykaszintű hírek jelentek meg arról, hogy Mark Zuckerberg, a Facebook (ma: Meta) elnök vezérigazgatója indulna a 2020-as amerikai elnökválasztáson.

- Hálózatsemlegesség megsértése. A közösségi hálózatokat működtető globális szintű vállalatok már régóta rendelkeznek saját fizikai hálózattal és eszközökkel, azonban amint erre céloztunk tanulmányunk korábbi részében, a legnagyobb szereplők

[172] Silvio Berlusconi olasz üzletembert és politikust, egykori miniszterelnököt említhetjük például, aki számos médiaérdekeltség többségi tulajdonrésze felett rendelkezve kezdte meg politikusi pályafutását.

hálózata globális és sok helyen kapcsolódik a nyilvános világhálóhoz (például a Metaé a BIX-ben is). Az ilyen típusú közelség nyilván a helyi felhasználókat kiszolgáló ISP-k számára kényelmes, hiszen ezért a forgalomért vélhetően nem kell senkinek tranzitdíjat fizetniük, ugyanakkor a kapcsolat bizonyára aszimmetrikus abban a tekintetben, hogy elég valószínűtlennek látszik, hogy a BIX-ben jelenlévő, magyarországi felhasználókat kiszolgáló ISP-k bármilyen adatot is továbbíthassanak mondjuk a Meta hálózatán. Ráadásul a közeli IXP-kben elérhető közösségi hálózatok szolgáltatásminőség szempontjából akarva-akaratlanul is előnyben kerülnek azokkal a konkurenseikkel szemben, akik a magyarországi felhasználókat kiszolgáló ISP-kel nem tudnak társasviszonyt (peering) létesíteni, vagyis sérül a hálózatsemlegesség elve[173].

- Személyiségi jogok, adattárolás. A közösségi hálózatok rengeteg adattal rendelkeznek a felhasználóikról. Ezek egy részét maga a felhasználó adja meg, részben a regisztráció során, részben a szolgáltatás passzív igénybevétele által (például helyadatok, a terminál adatai, stb.), más részét pedig az aktív tevékenységével, a posztokkal, megosztásokkal, a továbbosztásokkal és a mások posztjaira adott reakciókkal. A közösségi oldalak felhasználói profiljai akár kétezer különböző adatot is tartalmazhatnak, amelyek az egészen nyilvánvalóktól a felhasználó legszemélyesebb magánéletére vonatkozóig terjednek és ismeretükben lehetségessé válik olyan döntések predikálása is, amelyeket a felhasználó még nem hozott meg és ugyanakkor a megnyílik az út ugyanezeknek a döntéseknek a befolyásolására is. A közösségi média vállalkozások szerint a felhasználói profilok ilyen részletességű ismeretére többnyire csak az ajánlórendszerek minél pontosabb működése miatt van szükség[174]. Ha ezt el is fogadjuk – ami elég naív hozzáállás lenne –, akkor is felmerül két kérdés:
    - 1. Valóban szükséges-e az összes gyűjtött adat az ajánlások megfelelő működéséhez, a felhasználó vajon megadná-e közvetlenül mindezeket az adatait, ha megkérdeznék erről? A válasz erre természetesen az, hogy a felhasználók többsége a begyűjtött adatoknak csak töredékét adná meg, ha azokat közvetlenül tőle kérdeznék meg. Nyilván a felhasználóknak a saját személyes adataikhoz való jogaik valamilyen szinten sérülnek, ugyanakkor azt is el kell mondanunk, hogy a felhasználók túlnyomó része erről nem vesz tudomást, elfogadja a kényelmet, az ingyenes szolgáltatásokat és az adatait adja érte cserébe.
    - 2. Hol tárolják ezeket az adatokat? Ez a kérdés lényegesen megfoghatóbb és ha nem is a felhasználók, de az EU-n belül legalább az adatvédelmi hatóságok

[173] Az EU TSM rendelet nem terjed ki a peeringre, csak az internet hozzáférés szolgáltatás felhasználói részére és más erre vonatkozó úniós jogszabály sincs, vagyis jogsértés formálisan nem történik.

[174] Nagyon jó példa erre az a reakció, amivel a Meta a norvég adatvédelmi hatóság (Datatilsynet) döntésére reagált nemrégiben. A Datatilsynet nehezményezte, hogy a Meta – elsősorban a Facebookon és az Instagrammon keresztül úgy gyűjt adatokat a felhasználói profilok pontosításához, hogy a felhasználóknak célzottan kínált hirdetésekre való reakcióját vizsgálja. A norvég hatóság megkeresésére az Európai Unió Bíróságához fordult, amely megállapította, hogy a Meta ezzel a tevékenységével védett adatokat - faji és etnikai hovatartozás, vallási hovatartozás, szexuális irányultság, stb. – gyűjt ezzel a tevékenységével. A norvég hatóság bírságot is kiszabott, amely azonban csak jelentéktelen része a Meta adott időszakra eső profitjának, ráadásul a bírság csak 3 hónapig tartható fenn. A Meta védekezése arra az állításra alapult, hogy a felhasznlók hozzájárultak ahhoz, hogy a Meta célzott hirdetéseket mutasson nekik. Bővebben lásd: https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/meta-case-brought-to-the-european-level/ és https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/temporary-ban-of-behavioural-advertising-on-facebook-and-instagram/

foglalkoznak ezzel a kérdéssel és a szabályozások szerint az EU állampolgárainak adatait nem lehet kivinni az Unió területéről. Az ilyen törvények vagy rendeletek betartásának ellenőrzése persze kérdéses, hiszen amint fentebb írtuk, a szolgáltatók fizikai magánhálózatokkal rendelkeznek, amelyek adatforgalmát a hatóságok szinte egyáltalán nem tudják ellenőrizni.

10.3 Videómegosztó platform

A videóforgalom a mostanra a publikus Internet teljes forgalmának nagyjából 71%-át adja[175], de ez az arány az előrejelzések[176] szerint tovább növekszik majd a következő 5 évben 80%-ra. Ugyanakkor ezekkel az előrejelzésekkel érdemes óvatosan bánni, azt mindenképpen felvethetjük, hogy például az 5G mobil hálózatok robbanásszerű kiépülése lehetővé teszi az M2M kommunikáció új szintre kerülését, mind a végpontok számát, mind a lebonyolított forgalmat tekintve, tehát a videóforgalom arányának további térnyerésére azzal a fenntartással érdemes fogadni, hogy az emberi felhasználók tevékenysége által keletkezett forgalmat vizsgáljuk. Nyilván az 5G technológiák terjedése a videófogyasztást is támogatja, hiszen az átbocsátóképesség növekedése és szolgáltatásminőségi paraméterek javulása az olyan, a hálózatot intenzíven igénybe vevő szolgáltatások használata és tartalmak fogyasztása közben tapasztalható érzeti minőséget is észrevehetően javítja, mint a video streaming. A javuló minőség mellett a felhasználókat a fogyasztás növelésére ösztönzi a hozzáférési szolgáltatás fejlesztések következtében csökkenő egységára is.

10.3.1 A videómegosztó platformok tipizálása és a legnépszerűbb platformok bemutatása

Amikor videómegosztó platformról beszélünk, akkor a legtöbb esetben a Youtube merül fel példaként, mint olyan platform, amelyet majdnem mindenki ismer. Ugyanakkor nem ez volt az első, széleskörűen elterjedt platform, hanem a Vimeo, amelyet 2004-ben alapítottak és még ma is létezik, bár a felhasználói tábora lényegesen kisebb, mint a Youtube-é. A Youtube – ahogy a Vimeo is – a hagyományos videómegosztók közé tartozik, ahol a nagy fogyasztói közönség mellett jelentős számú feltöltő is van, vagyis akik a tartalmakat hozzáadják. Ezek a tartalmak nagy változatosságot mutatnak mind hosszukat, mind minőségüket, mind műfajukat és céljukat tekintve. Vannak csatornák, ami ugyanattól a szerzőtől származó videók halmazát jelenti. A videók megtekintése legtöbbször ingyenes, a felhasználó hirdetéseket és megtekint a videó elején – hosszabb videó esetén időnként közben is – amelyből az üzemeltetőnek bevétele keletkezik. Másrészt előfizetési díj fejében a szolgáltatás reklámmentessé válik. A nagy nézettségű tartalmak elhelyezőit a Youtube premizálja, ugyanakkor a jogvédett tartalmak illetéktelen felhasználást a maga eszközeivel bünteti.

A Similarweb szerint az Internet második legmagasabb forgalmát produkáló platformja a Youtube, amely nemcsak széleskörű kínálatával, hanem a szolgáltatás színvonalával, a mögötte meghúzódó folyamatos mérnöki innovációval is élenjáró. A platform olyan hosszú ideje – 2006 óta –már a Google tulajdona, hogy nem is igazán emlékszünk a kezdeteire, ráadásul a Google részeként eltöltött életciklusában is megkülönböztethetünk korszakokat. A

[175] https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/traffic-by-application

[176] Ericsson Mobility Report, June 2023, https://www.ericsson.com/49dd9d/assets/local/reports-papers/mobility-report/documents/2023/ericsson-mobility-report-june-2023.pdf

szokásos felosztástól eltérően ezek nem egymás után következő időszakok, inkább korszakhatárok, és a felsorolás sorrendje sem akar fontossági sorrendet tükrözni:

1. Érdemesnek látjuk megkülönböztetni azt az időszakot, amíg a videók lejátszásához szükség volt az Adobe Flash Player beépülő modulra, attól, amikor azt elhagyták. A platform indulásakor egyedül megengedett 320x240-es felbontást és a videók később korlátozott hosszúságát tekintve a Flash Player egy elfogadható megoldás volt, ráadásul egy – többé-kevésbé – működő technológiát használt fel egy újszerű szolgáltatás megvalósításához. Nyilván a plug in erőforráskezeléssel és biztonsággal kapcsolatos problémái a Youtube használatakor is egyre többször előkerületek, így 2010 januárjától kísérleti jelleggel, majd 2015 januárjától alapértelmezett megoldásként a HTML5 lett a lejátszási mód azokon a böngészőkön, amelyek ezt támogatták. Mostanra nyilvánvalóan az összes böngésző ilyen. A HTML5 az MPEG-DASH-t használja a streamelésre, ami a rendelkezésre álló hálózat minősége alapján adaptívan változtatja a kódoló forrássebességét és a lejátszott videó minőségét. A lépés azért volt fontos, mert egy – ezt nyugodtan kimondhatjuk – elavult megoldást, ami a platform elterjedését és népszerűségének növekedését, valamint a párhuzamos technológiai fejlesztéseket akadályozta, lecseréltek egy modern eszközre, amelyik mindezeket támogatta.
2. A következő szakaszhatár az élő adás megjelenése és szokványossá válása. A Youtube 2010-ben kezdte meg a saját technológiájú élő streamelés tesztjeit, majd 2011 áprilisától nyílt meg a lehetőség – kezdetben kiválasztott keveseknek. A korlátozásokat 2013 decemberében törölték el teljesen. A mobil applikációban a bevezetés csak 2017-ben történt meg, kezdetben ott is korlátozásokkal, amelyből még ma is megmaradt az, hogy annak, aki élő videót szeretne sugározni, legalább 50 előfizetővel rendelkeznie kell. Az élő stream maximális minősége 4K felbontás és 60 fps lehet, amihez tartósan legalább 10 Mbps sávszélességre van szükség, de az ideiglenes maximum elérheti a 40 Mbps-t is[177]. Az élő videófolyamban lehetséges HDR videók[178] és 360°-os videók[179] továbbítása is.

   Az élő videófolyam megjelenése és elterjedését több okból is korszakhatárként tarthatjuk számon. A legbanálisabb ezek közül, hogy a bevezetés menetrendjéről leolvashatjuk, hogy az Internet aktuális infrastruktúrája mikor tette lehetővé üzemszerűen az élő videó jelfolyam továbbítását vezetékes, illetve rádiós átviteli közegen, tulajdonképpen egy lenyomatát kapjuk az időszak kapacitásbővítési erőfeszítéseinek, amit az ISP-k és a mobil operátorok elvégeztek. A másik ilyen ok, hogy az élő videófolyamban mindig benne van a váratlan történés lehetősége, ami az előre felvett, feltöltött és több-kevesebb ember által korábbról ismert tartalmak esetén nem áll fenn. Az élő adás tulajdonképpen a televízió élő műsorainak (például sportközvetítés, élő koncert közvetítése, vitaműsorok) megvalósítása, így a hírműsorok kivételével – és itt sem a technológia vagy valamely más képesség hiányzik, hanem inkább a szándék – annak felváltása egy VoD platformra. Ez mindenképpen új terület volt a Youtube számára, ahol azonban hamar felzárkózta mellé a vetélytársak is, mint például a Twitch vagy a Facebook Watch. Egy harmadik indok az, hogy az élő videóközvetítés egészen más hirdetők számára jelent vonzó

[177] https://support.google.com/youtube/answer/2853702
[178] https://support.google.com/youtube/answer/10265272
[179] https://support.google.com/youtube/answer/6396222

piacot, mint a korábban létező tartalmak. Ezáltal a platform és végső soron a tulajdonosai újabb hirdetési pénzeket tudnak a hagyományos médiától az online média irányába átcsatornázni. Végül felemlíthetjük, hogy ugyanabban az időszakban jelentek meg és terjedtek el a streaming szolgáltatók, amelyek – messziről nézve a helyzetet – a Youtube konkurensei és ha már megjelenésük megosztotta a Youtube közönségét, amire valamilyen új, komoly érdeklődésre számot tartó innováció bevezetésével kellett reagálni.

3. Manapság a látjuk a platform gazdasági modelljének változását, amire már korábban is voltak kísérletek, de eddig nem jártak sikerrel. Az előfizetéses modell tulajdonképpen szintén a streaming szolgáltatók megjelenésére adott válasz, vagyis a Youtube meg akarja mutatni az erejét azon a területen is, amely nem tűnik az erősségének. A reklámok és hirdetések elhagyása komoly bevételkiesést jelent, másrészt ezáltal a Youtube felad valamit abból a hatalmas előnyből is, amit azért alakul ki, mert a Google-ökoszisztéma az egyének és a közösségek online jelenlétének egyre nagyobb részét tudja lefedni[180], vagyis a jelenlét nyomait érzékelve a felhasználó digitális profilját egyre részletesebben tudja megrajzolni.
   Ugyanakkor az előfizetéses modell esetleges sikere a Youtube előtt megnyithat újabb lehetőségeket, mint például a saját médiatartalom gyártása.

A hagyományos videómegosztók megjelenésükkör hirtelen jelentős, ráadásul egyre növekvő felhasználói bázisú vetélytársat jelentettek a hagyományos műsorszórók számára. Hasonló konkurencia lett aztán például a Youtube számára a Netflix, amely online DVD-kölcsönzőként indult még 1998-ban és emellett indult be a 2000-es évek közepén a streaming szolgáltatás. Ez utóbbi nagyjából 2010-re növekedett meg olyan mértékben, hogy indokolja a két üzletág szétválasztását[181]. A Netflix streaming szolgáltatása, bár ugyanúgy online videómegosztó, mint a Youtube, azért markáns különbségeket látunk:

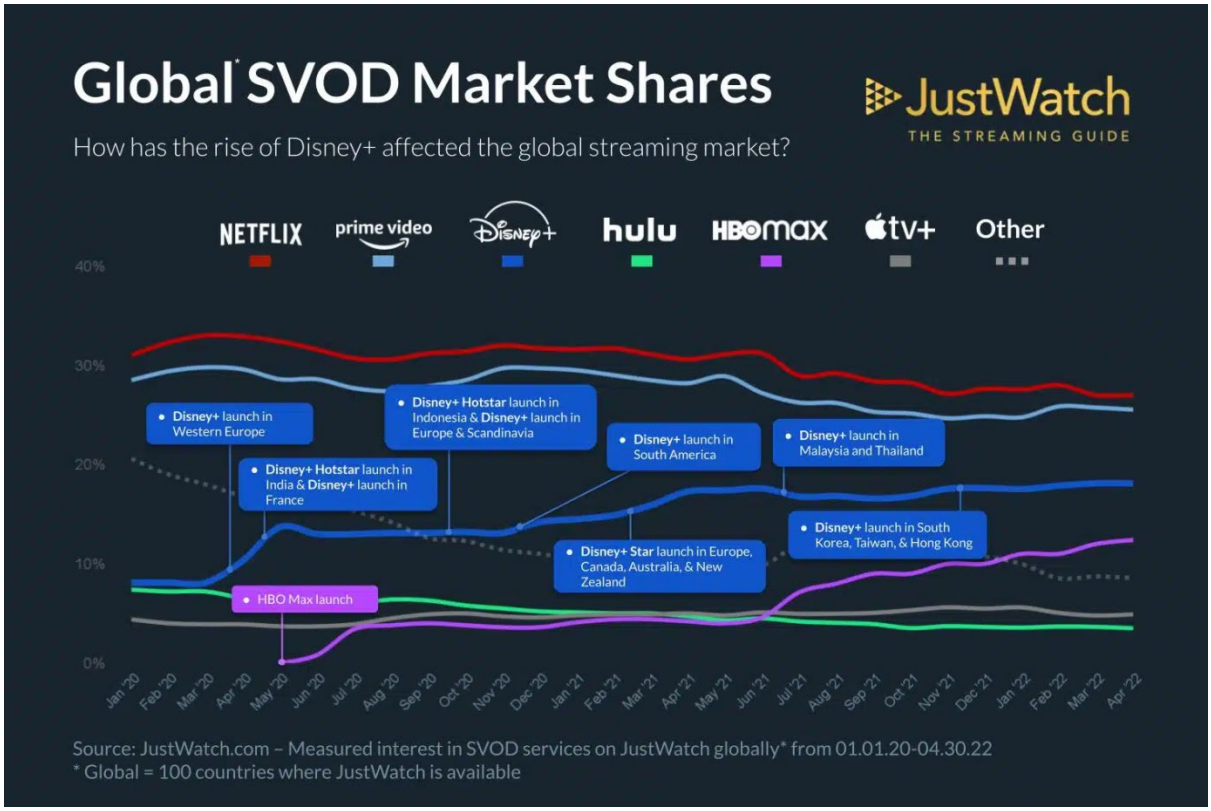
- A Netflix, már csak a DVD-kölcsönzői örökség miatt is kezdettől fogva jogvédett és legálistartalmakat kínált.
- A jogvédett tartalmakért kezdettől fogva fizetni kellett, ugyan az első időkben a kölcsönzés után, de hamarosan átálltak havidíjas előfizetési rendszerre.
- A nemzetközi terjeszkedés és az üzletágak szétválasztása nyomán keletkezett válságra a Netflix saját tartalmak gyártásával reagált (amelyek közül az első volt a 2013-ban bemutatott House of Cards-sorozat).

A Netflix előfizetőinek száma nagyjából 240 millió, ami ugyan kevesebb, mint a tizede a Youtube 2,5 milliárd feletti felhasználójának és természetesen lényegesen elmarad a Facebook 3 milliárdot meghaladó felhasználószámától is, inkább a Vimeo 300 milliós ügyfélkörének nagyságrendjébe esik. Ugyanakkor ez az összehasonlítás csalóka, hiszen amíg

[180] Könnyen belátható, hogy a hirdetés sokkal hatékonyabb, vagyis egy adott számú elhelyezés mérhetően több megrendelést/vásárlást indukál, ha a reklámokat a média tartalma és a médiafogyasztó preferenciáit egyaránt ismerve helyezik el. A közösségi médiában feltűnő influenszerek is erre alapozva működnek: olyan személy reklámoz egy-egy terméket, aki valamiképpen a médiafogyasztó figyelmét már felkeltette, tetszését/bizalmát elnyerte.

[181] Egészen aktuális hír, miszerint a Netflix felszámolja a DVD kölcsönzési tevékenységét. Az utolsó jellegzetes piros borítékokat 2023. szeptember 29-én küldték ki. Amikor az előfizetők visszaküldik a DVD-ket, az üzletág lezárul. Bővebben lásd: https://about.netflix.com/en/news/netflix-dvd-the-final-season és https://about.netflix.com/en/news/thanks-for-watching

a többieknél többnyire egyéni ügyfelekről beszélünk, akik a szolgáltatásért nem fizetnek[182], a Netflix esetén minden előfizető bevételt[183] termel és az előfizetés nem személyre, hanem háztartásra vonatkozik. Az elért nézők száma így milliárdos nagyságrendbe eshet, bár nyilván valamelyest kisebb lett azóta, hogy a Netflix tiltja[184] a jelszómegosztást, viszont az előfizetők száma 2023 második negyedévének végére 5,9 millióval növekedett[185] az előző negyedévihez képest.
A Netflix végül sikeres lett, ma már Észak-Korea, Kína, Oroszország és Szíria kivételével a világ összes országában elérhető. A nyomdokán haladva több konkurens szolgáltatás is megjelent a piacon, például a Hulu, a Disney+, az Apple TV+, az Amazon Prime és a HBO Max, hogy csak a legismertebbeket nevezzük meg. Ezek a szolgáltatók, hasonló modell szerint működnek, mint a Netflix, gyártanak saját tartalmakat is, amely között kifejezetten nagy költségvetésű filmek vagy sorozatok is vannak. A forgalmat tekintve a Netflix máig a legnépszerűbb közöttük, de mint az 60. ábra[186] is mutatja, piaci részesedéséből veszített az elmúlt években. Az előfizetések számát tekintve Amazon Prime Video mellett a dinamikusan bővülő Disney-csoport (a Disney+, a Hulu és az ESPN együtt) nagyon közelíti már.



60. ábra A videó streaming szolgáltatók piaci részesedésének alakulása 2020.01-2022.04 között

[182] Természetesen a Youtube Premiumnak és a Vimeonak is vannak előfizetői, előbbinek nagyjából 80 millió (2022-ben), utóbbinak 1,6 millió (2021 végén). A Vimeo esetén az előfizetők többségében szervezetek és vállakozások.
[183] A magyarországi árak: https://help.netflix.com/en/node/24926
[184] A tiltást 2023. május 23-án hirdették ki: https://about.netflix.com/en/news/update-on-sharing-may-us. Egyúttal létrehozták a vendégfiók lehetőségét, ami díjazásért cserébe tette lehetővé az előfizetés megosztását. A vendégfiókhoz önálló jelszó is tartozik.
[185] https://techcrunch.com/2023/07/19/netflix-gains-nearly-6m-subscribers-as-paid-sharing-soars/
[186] Az ábra forrása: https://www.geeknative.com/142495/market-share-stats-the-global-state-of-streaming-video-on-demand/

Azt mindenképpen meg kell jegyeznünk, hogy a piaci részesedések megállapítása komoly nehézségekbe ütközik, mivel nincs közmegegyezés a megfelelő mérőszámról. Hiába állíthatjuk például, hogy a Prime előfizetői az Egyesült Államokban mára többen vannak, mint a Netflix előfizetői, amikor a fogyasztásuk lényegesen kisebb, már csak azért is, mert az Amazon Prime előfizetéshez tartozó Prime Video szolgáltatást nem is veszi minden előfizető igénybe. Másrészt a grafikonból látható, hogy akárcsak 1-2 év alatt az újonnan piacra lépő szereplők (például a Disney+ vagy az HBO Max) jelentős szeletet kaphatnak a globális tortából. Természetesen az utóbbi 2-3 év statisztikáit jelentősen befolyásolja a COVID-19 okozta járványügyi helyzet miatti bezárkózás, vagyis, hogy az emberek jobban preferálták az otthoni szórakozási lehetőségeket. Miután a lezárások megszűntek, látszik is némi visszaesés /stagnálás az egész piac tekintetében is, amelyet növekedéssé átfordítani csak innovatív megoldásokkal és izgalmas tartalmakkal lehetséges. Ezen felül a globális részarányok alakulását befolyásolják majd a feltörekvő kínai szolgáltatók (iQIYI, Tencent Video) ahogy a nemzetközi piac felé nyitnak, másrészt az egyes szolgáltatók beágyazottsága is, tekintettel például arra, hogy az Amazon Prime előfizetőinek több mint háromnegyede, az Apple TV+ 75 millió felhasználójából[187] 39 millió egyesült államokbeli[188].

A harmadik csoportnak a legismertebb képviselője a TikTok, amely nagyon rövid idő alatt lett a piac egyik domináns szereplője, hiszen a 2016-os alapítású kínai vállalat mostanra a 1,6 milliárd felhasználóra tett szert, amibe még nem számoltuk bele kínai változatának, a Douyinnak csaknem 800 millió felhasználóját[189]. A kettőt összeadva azt látjuk, hogy a TikTok/Douyin páros 2,4 milliárd felhasználója nem sokkal marad el a Youtube 2,6 milliárdos felhasználói táborától, ami elég szép teljesítmény, főként, ha a TikTok jellegét is figyelembe vesszük. A TikTok eredetileg nagyon rövid, lipsyncinges és táncolós videótartalmak megosztására adott lehetőséget, tulajdonképpen mondhatnánk ezeket vírusvideónak is. Mostanra természetesen teljes értékű videószolgáltatássá nőtte ki magát, azonban az eredete és jellege is sokkal inkább rokonítja a közösségi médiával, mint például a Youtube-bal. A rövid idő alatt hatalmas piacra szert tevő platform természetesen „megihlette" a távolabbi konkurenseit is, a Youtube például 2020-ban jelentette be a Youtube Shorts szolgáltatását, amelyet általánosan a TikTokhoz hasonlítanak. Ugyanakkor a TikTok elterjedése valamelyest meg is „tisztította" a Youtube-ot, vagyis miután a TikTok-stílus kedvelőinek lett egy önálló platformja, amiről aztán őket magukat is elnevezték, a Youtube-on jelentősen lecsökkent az ilyen típusú videók száma és az ajánlatokban való felbukkanásuk gyakorisága is.

Az összes különbözőség ellenére mindhárom szolgáltatástípus esetén a működés, a népszerűség növekedésének és az új felhasználók bevonzásának kulcsa a nagyon jól működő ajánlórendszer, vagyis az az algoritmus, amely a felhasználó által korábban és aktuálisan megtekintett videók jellemzői alapján ajánlatokat tesz a következő videóra.

[187] https://www.statista.com/statistics/1136261/number-of-apple-tv-plus-subscribers-us/. A felhasználóknak csak egyharmada tényleges előfizető, kétharmaduk valamilyen promóció keretében kapott egy évre szóló jogosultságot.
[188] https://vpncentral.com/apple-tv-plus-statistics-worldwide/
[189] https://www.businessofapps.com/data/tik-tok-statistics/

10.3.2 A videómegosztó platformok jövője – trendek, lehetőségek, kockázatok

Amint korábban is említettük, a videóforgalom abszolút domináns az Interneten már jelenleg is és részaránya valamelyest emelkedni is fog még. Érthető, hogy minden platform, amelyik a népszerűségét, felhasználóinak számát és bevételeit növelni szeretné, törekedni fog arra, hogy a tevékenységi körét valamilyen videószolgáltatással bővítse, vagy ha már rendelkezik ilyennel, akkor azt minél innovatívabbá és egyedibbé tegye. Az HBO Max példája azt mutatja, hogy hogy megfelelően vonzó médiatartalommal és marketingkampánnyal egy telítettnek látszó piacon is rövid idő alatt számottevő részesedést lehet szerezni. A TikTok példája viszont arra világít rá, hogy az innovatív ötletek és az ajánló rendszerben alkalmazott mesterséges intelligencia képes új piacot nyitni és azon trendformálóként tulajdonképpen monopolhelyzetet létrehozni. Ezeknek a platformoknak a nagyon gyors népszerűségnyerése és a COVID-19 járványhelyzet leküzdésére hozott társadalmi együttélési szabályok következményei rávilágítanak arra, hogy akár 2-3 évre előre sem lehet megbízható előrejelzésünk, vagyis igazából már most tapasztalható jelenségek alapján írhatunk csak a várható trendekről.

Az jövőben vélhetően a platformok konvergenciája sokkal inkább észrevehető lesz, és itt elsősorban az online médiamegosztó platformokra és a közösségi hálózatokra gondolhatunk. A Facebookon történő előre felvett vagy élő videó közvetítése belátható módon technológiai szempontból semmiben nem különbözik attól, ahogyan ezt a videómegosztók végzik. A videómegosztókon elhelyezett értékelések és kommentek ugyanígy jellegükben nem különböznek a közösségi oldalak posztjaitól és a posztokra adott hangulatjelektől.

A TikTok és hozzá hasonló társai a rövid idejű videók mellett az egészen kitűnő ajánlórendszereiknek köszönhetik az elnyert népszerűségüket. Ugyanakkor az ajánlórendszerek által az egyes felhasználókról gyűjtött masszív adatmennyiség nagyon komoly aggodalmat keltett – és nem csak az ún. „nyugati világban" –, olyannyira, hogy több országban betiltották a vagy korlátozták használatát. Ezeket az adatokat névlegesen az ajánlórendszer pontosságának növelése érdekében gyűjtik. Az aggályok két fontos dologba kapaszkodnak bele leginkább, az összegyűjtött felhasználói adatok mennyiségére – mivel szakértők szerint túl sok adatot gyűjtenek és olyanokat is, amelyekre tényleg semmi szükség nincs. A másik aggodalomra szolgáló ok az adatok tárolásának helye. A szolgáltató szerint mind az adatgyűjtés, mind az adattárolás megfelel a szolgáltatásban érintett ország helyi hatóságaitól származó előírásoknak. Ennek legfontosabb eleme, hogy az európai felhasználói adatok tárolás az Európai Unióban történik. Az Egyesült Államokban az aggodalom olyan szintet értek el, hogy a Microsoft kísérletet tett a TikTok felvásárlására 2020 nyarának vége felé. A tervezett tranzakció pénzügyi tekintetben minden korábbit felülmúlt volna a hírek szerint. Az engedélyt meg is kapták magától az USA elnökétől is, de a tárgyalások nem jártak sikerrel, majd az új kormányzat alatt le is kerültek a napirendről, hogy aztán mostanra ismét visszatérjünk oda, hogy az amerikai kormány a TikTok szövetségi szintű betiltásával fenyeget. Tiltást egyébként több ország is alkamaz, elsősorban a hivatali informatikai eszközökön.[190]

A játékok és az e-sport közvetítések felbukkanása az online platformokon szintén abba az irányba mutat, hogy az felhasználók digitális térben való megjelenését teljes egészében kiszolgálni szándékozó – és ennek kapcsán az adataikat birtokolni akaró – komplex rendszerek létrejötte felé tartunk. Hogy egy-egy ilyen rendszer irányába való elköteleződés esetén a kapott szolgáltatások kényelme és a zárt rendszer által nyújtott biztonság

[190] https://en.wikipedia.org/wiki/Censorship_of_TikTok, https://mashable.com/article/tiktok-ban-countries, és https://en.wikipedia.org/wiki/Restrictions_on_TikTok_in_the_United_States

hangsúlyosabb-e a monopólium számára való kiszolgáltatottság veszélyénél, még nem tudható biztosan. Azt mindenképpen láthatjuk, hogy jelen állás szerint az államok nem biztos, hogy meg tudják védeni polgáraikat egy-egy ilyen helyzetben.

10.3.3 Elsősorban pornográf tartalmak megosztását célzó online platformok

A pornográf tartalmak megosztására szolgáló online platformokkal a videómegosztó platformokon belül érdemes foglalkozni, mivel a pornográf médiaforgalom túlnyomó része videó. Az ezzel foglalkozó oldalak közül négy is szerepel az Similarweb internetforgalmi rangsorának első 25 helyezettje között[191]. Előfizetők számára vonatkozó friss adatokat értelemszerűen nehéz találni, viszont a tanulságos látni, hogy 2022 novemberében a legnagyobb látogatottságú oldalak rangsorában a negyedik és az ötödik pozíciót[192] foglalta el a Pornhub (10,2 milliárd oldalfelkeresés) illetve az Xvideos (8,7 milliárd oldalfelkeresés). Összehasonlításképpen a harmadik helyen a Facebook áll, 10,7 milliárd oldalfelkereséssel.

A pornográf videómegosztók működésével kapcsolatban hasonló kérdések merülnek fel, mint a hagyományos videómegosztókkal kapcsolatban. Az egyik ilyen kérdés lehet a megosztott videófelvételek szerzői joga. Ezzel kapcsolatban a pornográf videómegosztók ugyanazon elvek szerint jártak el, mint a hagyományos megosztók, vagyis törölték a megosztott videókat. Egy másik kérdés lehet a felhasználók személyiségi jogainak védelme. Ez a probléma itt még nagyobb jelentőséggel bír, mint a hagyományos videómegosztóknál, mivel az látogatók és az előfizetők túlnyomó többségükben szeretnék a személyazonosságukat elrejteni. A nagyobb oldalak természetesen titkosítással védik az adatokat, de attól még időről időre előfordulnak kisebb incidensek.

A pornográf videófelvételek esetén is érvényesülnek a felvételen szereplők személyiségi jogai. Több részterületre bontható ez a jogérvényesítés, közöttük olyanokkal, miszerint a szereplők belegyeztek-e abba, ami velük történik a felvételen, belegyeztek-e a felvétel készítésébe és nyilvánosságra hozásába. Ennek betartását akár a bíróság, akár a magánszemélyek vagy vállalkozások képesek kikényszeríteni. Emlékezetes eset például, hogy 2020 decemberében társadalmi nyomás hatására a MasterCard és a Visa is felmondta a szolgáltatását a Pornhub felé. A hagyományos fizetési hálózatoktól ilyen módon elvágva[193] a Pornhub néhány nap múlva bejelentette, hogy törli az összes vitatott videót és a meg nem erősített felhasználók feltöltéseit[194], miáltal a kínálata 13 millióról 4 millió videóra csökkent. Ugyanakkor arra egyelőre nincs semmilyen megoldás, hogy például teljes biztonsággal megakadályozzák, hogy kiskorúak férjenek hozzá a pornográf tartalmakhoz.

A Livejasmin nevű platform kiemelkedik az pornográf videó megosztók közül abban a tekintetben, hogy webkamerával készített élő videóadást osztanak meg, tipikusan egyszerre egy vagy néhány felhasználóval és a felhasználók, illetve a megosztó között kétirányú kommunikáció lehetséges. Természetesen a felhasználót mindeközben megilleti a teljes diszkréció. A Livejasmin 2001-ben indult Magyarországon és 2003-tól nyújt globális szolgáltatást. Ez már az az időszak volt, amikor a korabeli webkamerák által adott médiafolyamot egy DSL-összeköttetésen keresztül is el lehetett juttatni a felhasználóhoz.

[191] https://www.similarweb.com/top-websites/ . Az adatsor 2023 augusztusára vonatkozik.
[192] https://www.statista.com/statistics/1201880/most-visited-websites-worldwide/
[193] Érthető talán ezek után, hogy a pornográf tartalmak megosztói figyelemmel kísérik a kriptovalutákat, adott esetben befektetésekkel is igyekeznek elősegíteni a fejlődésüket.
[194] https://www.theguardian.com/technology/2020/dec/14/pornhub-purge-removes-unverified-videos-investigation-child-abuse

10.4 Online piacterek

Az online piactér egy olyan online platform, amelyen valamilyen kézzelfogható árucikk vagy valamilyen szolgáltatás megvásárlására nyílik lehetőség. A valódi piacoknak megfelelően az online térben is többnyire a piac működtetője és az árucikk vagy szolgáltatás előállítója nem ugyanaz a személy vagy vállalkozás. Sőt, itt előfordulhat az is, hogy a piac működtetőjének még ideiglenesen sincs birtokában az, amit eladásra kínál, hanem tulajdonképpen csak közvetítő szerepet vállal, nyilván valamilyen a jutalék vagy részesedés fejében.

10.4.1 Alkalmazásáruház (AppStore)

Bár az alkalmazásáruház fogalmát sokan a 2008-ban piacra kerülő első Apple iPhone telefonhoz kötik, onnan csak az elnevezés származik, a koncepció, vagyis, hogy legyen egy olyan platform, amely digitális úton tesz elérhetővé szoftvereket, amelyeket alkalmazásoknak hívunk, régebbi időkből származik. Egy-másfél évtizeddel korábban a többek között a Linux rendszerek esetében használt *package manager* ugyanazt a szerepet töltötte be, mint egy alkalmazásáruház: a rendszer működéséhez nem nélkülözhetetlen, de a felhasználók számára fontos funkciókat megvalósító package-eket lehetett letölteni és telepíteni a számítógépre és ezeknek a package-eknek a szerzője legtöbbször nem az operációs rendszer vagy a használt Linux-disztribúció készítője, hanem egy harmadik személy. Az iPhone-t megelőzően is létesültek már telefonplatformra tervezett alkalmazásáruházak, azonban a széttagoltság miatt minden gyártónak külön volt ilyen, például a Nokia által 2006-ban a Symbian rendszerű telefonjai számára bevezetett Nokia Download!-ot lehet itt említeni. Az AppStore az iPhone-on volt elérhető, de a tulajdonosa használhatta asztali számítógépen az iTunes-t is.
2008 szeptemberében érkezett az első Androidos telefon és vele az Android Market, amelyet később Google Play-re neveztek át, majd 2009-ben a Blackberry, a Nokia és a Microsoft alkalmazásáruháza. A Windows 10-zel kezdődően a Microsoft az asztali rendszereinél is ugyanazt a sémát követi, bár egyébként ennek voltak előzményei korábban is, hiszen az első már a Windows 95 esetén a felhasználó kezébe adták a döntés szabadságot a biztonsági és kényelmi frissítések és a hibajavítások telepítéséről. Igaz, ez többnyire egy igen vagy egy nem válasz volt, tulajdonképpen a külső hardverkiegészítők meghajtói jelentettek kivételt, ahol a gyártói és a Windows-hoz kiadott Microsoft-os driverek közül lehetett választani.

Az alkalmazás áruházak speciális fajtái a játékok terjesztésével foglalkozó platformok. Ezeket azért érdemes megkülönböztetve kezelni, mert az üzleti modell, amelyet közülük az első, jelentős ismertsége szert tevő platform, vagyis a Steam alkalmazott, abban nyilvánult meg, hogy a játékos nem birtokolja a játékot, hanem csak használati jogot vásárol – ami miatt mindjárt önmagában is olcsóbb. Jellegzetességüknek tekinthető még, hogy a piacterek tulajdonosai többnyire játékgyártó cégek, tehát a termékek legalább egy részét saját maguk termelik meg.
A már említett Steam, amelyet a Valve hozott létre 2003-ban egy egyszerű szoftver kliensként eredetileg arra a célra, hogy saját gyártású játékaihoz automatikus frissítéseket és javításokat terítsen ma számos, a játékosok számára lényeges funkcióval rendelkezik, mint például a játékállások felhőbe mentése vagy a játékosok közötti közvetlen beszédkommunikációs csatornák biztosítása. A Valve 2008-ban adta ki a nyilvános Steam API-t és még abban az évben számos játékfejlesztő használatba is vette. Először csak

Windows-okon futott, de ma már létezik MacOS-re és Linuxra is. Ma a kínált játékok száma meghaladja a 83 ezret[195]. A cég készített saját, Linuxra épülő operációs rendszert SteamOS néven, amely a márkához tartozó hardvereken, többek között a Steam Decken fut. A Steam számos játékkészítő stúdióval szerződött, olyanokkal is, akik saját játékterjesztő platformot is működtetnek, mint például a Microsoft, az Ubisoft, vagy az Electronic Arts. A konzolok közül a Playstation támogatja a Steamet, az Xbox nem.
A Steam vetélytársaként szeretne feltűnni az Epic Games Store, amelyet 2018-ban hozott létre az Epic Games Windows-ra és macOS-re. A Steamhez képest sokkal kevesebb címet kínál. A játékosoknak hetente 1-2 ingyenes játékot kínál fel, amelyek néha akár 20 dollárt is meghaladó értékűek, azonban a platform működése továbbra is veszteségesnek tűnik. Ráadásul az Epic Games évek óta pereskedik az Apple-lel, mert az Apple szerint az Epic a ***saját*** címeiben játékon belüli vásárlásokra ösztönzi felhasználóit. Az Epic pedig azért perli az Apple-t, mert nehezményezi, hogy a játékon belüli vásárlások kizárólag az Apple fizetési rendszerén mehetnek keresztül, amelyből az Apple jelentős mértékű jutalékot von el. A perek tartanak, de az Epic már jelentős elbocsátásokat jelentett be, hogy ezeknek a pereknek a pénzügyi vonzatait ki tudja gazdálkodni.
A GOG szintén egy játékgyártó stúdió tulajdona, mégpedig a CD Projekt-é. Az AAA-s címek mellett régebbi játékokat is terjeszt.
A játékokat árusító online piacterek legnagyobb vetélytársai a konzolgyártók és a hagyományos, széles áruskálával és nagy felhasználótömeggel rendelkező alkalmazásáruházak.

10.4.2 Szálláshely és személyszállítás szolgáltatás

A szálláshely szolgáltatást nyújtó online piacterek működtetői túlnyomórészt közvetítők, tehát saját magunknak nincsenek kiadható szálláshelyeik. A legnépszerűbb szereplők a Booking.com, az Experia, az Airbnb és az Agoda, Magyarországon a fentieken kívül még a Szallas.hu. A szolgáltatás az utóbbi évtizedben vált népszerűvé, elsősorban annak köszönhetően, hogy a felhasznált internetes kommunikációs és fizetési csatornáknak köszönhetően az utazásszervezés és a szállásfoglalás folyamata leegyszerűsödött és fel is gyorsult. Másrészt bizonyos szolgáltatók komplex csomagokat hoztak létre, amely az utazás/üdülés minél több momentumát fedte le. Például amíg a Szallas.hu[196] és az Airbnb szálláshelyet kínálnak csak, a Booking.com ezen kívül az utazás megszervezésében, a közlekedési eszközökre szóló jegyek rendelésében vagy programok megrendelésében is segítségére van a felhasználóknak.
A személyszállítás szolgáltatásra az egyik legalkalmasabb példa az Uber, de ide sorolható valamilyen szinten a hazánkban is ismert Flixbus is. Az Uber nagyon jellegzetes szolgáltatás abban a tekintetben, hogy a hozzá kapcsolódó jellemzők elég jól általánosíthatók például a szálláshelyszolgáltatást megvalósítókra is. A pozitív jellemzők egyértelműen a gyorsaság, a rugalmasság, az áttekinthetőség, a legalább részleges papírmentesség és az olcsóság.
A negatív jellemzőket is érdemes megemlíteni, sőt akár részletesebben leírni azokat, amelyek magyarázatra szorulnak:

- Az egyik nehézség abból fakad, hogy a cég, amelyiknek a weboldalát felkeressük vagy a alkalmazását igénybe vesszük, csak közvetít, de többnyire sem saját szálláshellyel, sem közlekedési vagy szállítóeszközzel nem rendelkezik. Sőt, elég könnyen

[195] Az aktuális számot bárki megnézheti: https://store.steampowered.com/search/?category1=998
[196] A Szallas.hu a szálláslehetőségek mellett nagyon részletes programkínálattal is rendelkezik.

előfordulhat, hogy harmadik országban van a felhasználó kiindulási helyéhez és az igénybe vett szolgáltatás helyéhez képest. Jelentősen megnehezül ezáltal a panaszok kezelése, hiszen az ügyfél az esetleges minőségi kifogásait a közvetítő felé teheti meg, hiszen vele áll szolgáltatási viszonyban. Ez alapesetben kezelhető problémát jelent – bár nyilván egy esetleges időeltolódás jelentősen ronthat a kommunikáció minőségén.

- A másik probléma az adó megfizetés/beszedésének nehézsége, ami azt takarja, hogy a például egy magyarországi szállásadó a Booking.com-on egy brit turista által lefoglalt szállás után a szállásadónak bevétele keletkezik. A pénzt azonban nem turistától kapja, hanem a közvetítőtől és nem annyit, mint amennyit a turista fizetett, hanem valamivel kevesebbet. A különbözet a közvetítő jövedelme. Jövedelme lesz tehát a szállásadónak és a közvetítőnek. Már az utóbbinak az adófizetése is kérdéses, viszont a NAV számára a magyarországi szálláskiadók fontosabbak, pontosabban az, hogy ők rendesen befizessék bevételük és jövedelmük után a megfelelő adó- és járuléktételeket.
- Harmadrészt problémás helyzetet teremt, hogy a szolgáltatás ára a közvetítőhöz kerül és bár van arra határidő, hogy mikor kell a szállásadóhoz kerülnie, ez néha nem teljesül. A Booking.com idén nyári esete arra mutat rá, hogy a szállásadó ügyfelek meglehetősen ki vannak szolgáltatva a közvetítőnek, aki a fizetés hosszadalmas elhúzásával akár a nehéz anyagi helyzetbe hozza a szálláskiadókat, akik néha állami támogatásra is szorulnak, akár jogszabályi, akár anyagi értelemben.
- Összességében ezek a problémák egy-egy településen, régióban vagy országban észrevehető gazdasági bizonytalanságot és egyensúlytalanságot idézhetnek elő, mivel a hagyományos, adott esetben hosszú múltra visszatekintő beágyazottsággal rendelkező, helyi munkaerőt foglakoztató és hosszútávú stratégiai tervekre alapozott befektetéseket eszközlő vállalkozások számára okoznak piaci alapon nem kezelhető problémákat. Ezt a helyzetet több esetben csak politikai szinten, új törvények és rendeletek alkotásával lehetett kezelni (például az Uber vagy az Airbnb szankcionálása).

11 Záró gondolatok

Tanulmányunkban áttekintettük az online ökoszisztémákat, a Földet behálózó globális IP alapú hálózatoknak elsősorban azokra a részleteit kezelve hangsúlyosan, amelyek a felhasználók döntő hányada számára az Internettel egyenértékűek. Az Internet sokaknak valójában a hálózat („térerő") és az online platformok által nyújtott szolgáltatások egységét jelenti. Észrevehetjük, hogy a hálózat fenntartása, az infrastruktúra fejlesztése, a menedzsment feladatai elsősorban az ISP-kre és a mobil operátorokra hárulnak, amelyért a felhasználók az internetszolgáltatás előfizetési díját fizetik be minden hónapban. Ugyanakkor a szolgáltatások szintén fejlődnek, az online platformok tulajdonosai bővítik a kiszolgáló felhőket, fejlesztik a szolgáltatások frontendjét és backendjét, néhány esetben maguk is előállítanak vagy megvásárolnak tartalmakat, illetve fizetik a jogdíjakat a harmadik felek tulajdonában maradt tartalmak után, cserébe viszont a felhasználóktól a szolgáltatás előfizetési díját és a hirdetések fogyasztását, a hirdetőktől a reklámbevételeket kapják.

Amíg a két táborban elhelyezkedő szereplők között a nyereség megosztásának aránya nem egyoldalú, addig a felhasználók az Internet fejlődését tapasztalják, viszont a jelenlegi helyzetben az egyensúlytalanság az ISP-k elégedetlenségét eredményezi, mivel a hálózati infrastruktúra fejlesztési igényei az exponenciálisan növekvő forgalom és a növekvő költségek miatt folyamatosan növekednek, viszont a bevételek túlnyomó része az online platformokhoz kerül. Nem újkeletű felvetés[197], hogy a tartalom- és alkalmazásszolgáltatók (Content and Application Service Providers – CAPs), vagyis azok a vállaltok, amelyek az előzőekben bemutatott online platformok tulajdonosai és működtetői, hozzájáruljanak a hálózat fejlesztési és fenntartási költségeihez.

A tartalom és alkalmazásszolgáltatók természetesen folyamatosan eszközölnek befektetéseket, de ha azok összetételét megvizsgáljuk[198], akkor azt látjuk, hogy az abban vizsgált 3 év alatt a CAP-ek 33 milliárd dollárnyi befektetésének nagyjából 90%-át emésztette fel a hosting, vagyis a tartalmak tárolása, lehetőleg minél közelebb a felhasználóhoz, míg a maradékon osztozott a kiszolgálás transport és delivery fázisa. Ez a helyzet a későbbiekben sem javult[199]. Azt látjuk, hogy ha egy CAP hajlandó is hozzájárulni a fizikai hálózat fejlesztésének és fenntartásának költségeihez, akkor azt azért teszi, mert számára gazdasági szempontból megéri.
Ilyen eset volt, amikor 2014-től a Netflix a megállapodásuk alapján egy nem publikus összeget fizetett a Comcastnak[200], amely cserébe a Netflix szervereit közvetlenül bekötötte a

[197] Lásd például: Economides, Nicholas. „Why Imposing New Tolls on Third-Party Content and Applications Threatens Innovation and Will Not Improve Broadband Providers' Investment." NYU Law and Economics Research Paper 10-32 (2010).
[198] Abecassis, David, et al. „Investment in networks, facilities and equipment by content and application providers." Analysys Mason Report (2014).
[199] Abecassis, David, et al. „The impact of tech companies' network investment on the economics of broadband ISPs" Analyys mason Report (2022)
[200] A Comcast a legnagyobb amerikai multinacionális távközlési és médiakonszern. A társaság árbevétel alapján a világ második legnagyobb műsorszóró és kábeltelevíziós társasága (az AT&T mögött), emellett a legnagyobb fizetős televíziós társaság, a legnagyobb kábeltelevíziós társaság és a legnagyobb otthoni internetszolgáltató az Egyesült Államokban. Az NBCUniversal nemzetközi médiavállalat tulajdonosa 2011 óta, rajta keresztüli olyan műsorszóró hálózati csatornákat is birtokol és üzemeltet, mint például az NBC, a Telemundo, a TeleXitos és a

saját hálózatába[201]. Később a Netflix hasonló megállapodásra[202] jutott az AT&T-vel, a Verizonnal és a Time Warner Cable-lel is. A megállapodás előzménye az volt, hogy a Netflix ügyfeleket kezdett veszíteni azért, mert a Comcast és a Verizon által nyújtott internethozzáférési szolgáltatás minősége jelentősen rontotta a Netflix alkalmazáshoz kapcsolódó felhasználói élményt. A Comcast azzal védekezett, hogy másképpen nem tudja kezelni a megnövekedett forgalmat, amely csúcsidőszakban akár az USA internetforgalmának egyharmadát (!) is jelenthette. Az esetet és a Netflixnek a Verizonnal való vitáját is vizsgálta az FCC, de végül mindkét ügy megállapodással zárult.

Az ISP-k nyilván hasonló megállapodást kötnek más nagy techcégekkel[203] is, hogy ennek milyen anyagi következményei lesznek, az nyilván a két megállapodó fél közötti erőviszonytól függ. A két nagy amerikai szolgáltató a hálózatsemlegességet technológiai szinten megsértve érte el, hogy a Netflix belefizessen az infrastruktúrába. A közelmúltban végzett vizsgálatok szerint azonban már a hálózatsemlegesség adminisztratív jellegű megsértése, nevezetesen a zero-rating alkalmazása által is végső soron károsodik a fogyasztó[204].
Amint már korábban is említettük, az IXP-kben a nagy online platformok egyöntetűen jelen vannak és így a társviszonyon keresztül viszonylag egyszerűen és mindenképpen költséghatékonyan tudnak oda adatot, tartalmat továbbítani. Arról semmilyen információval nem rendelkezünk, hogy viszonossági alapon az IXP-ben jelen lévő ISP-k hozzájuthatnak-e egyáltalán a platform által birtokolt vagy bérelt kapacitáshoz.
Európában jelenleg is erős vita zajlik többek között arról, hogy a CAP-eknek milyen módon kellene hozzájárulniuk az ISP-k által működtetett hálózati infrastruktúrák fejlesztéséhez. Kiterjedt hálózatokkal rendelkező ISP-k a CAP-ekre terhelhető forgalomarányos hálózathasználati díj bevezetéséért lobbiznak a törvényhozóknál. Ennek bevezetése sok szereplő szerint felborítaná a kialakult megállapodásokat és együttműködéseket. A CAP-ek oldalán kiakalult ellenzői tábor szerint az ISP-k infrastruktúra-fejlesztésre fordított CAPEX költségei alapvetően nem emelkedtek a forgalommal arányosan. Ezen felül a CAP-ek, érvelésük szerint jelenleg is kiveszik részüket a fejlesztési költésekből, valamint a szolgáltatásaik által indukált forgalomnövekedés többletbevételt jelent a mobil operátorok számára. A CAP-ek hálózati infrastruktúrális oldalon három fő irányban fejlesztenek: i) tartalom-gyorstárazó infrastruktúrák kitelepítése ISP hálózatokba, ii) nagytávolságú hálózai összeköttetések (pl. tenger alatti optikai kapcsolatok) kapacitás-bővítésének támogatása és iii) közvetlen kapcsolódás regionális IXP-khez, valamint publikus és privát peering kapcsolatok kialakítása. A fentieken felül új üzleti irányként azt is látjuk, hogy bizonyos alkalmazásszolgáltatók dedikált erőforrásokat szeretnének vásárolni 5G mobil távközlő hálózatokban, egészen a rádiós bázisállomásig.

Cozi TV; több csak kábeles csatorna, például MSNBC, CNBC, USA Network, Syfy, Oxygen, Bravo és E!; a Universal Pictures filmstúdió; a Peacock VOD streaming szolgáltatás.Rendelkezik filmstúdiókkal és 2018 októbere óta a Sky Group anyavállalata is egyben.

[201] https://consumerist.com/2014/02/23/netflix-agrees-to-pay-comcast-to-end-slowdown/, https://www.businessinsider.com/netflix-comcast-deal-explained-2014-2

[202] https://money.cnn.com/2014/08/29/technology/netflix-comcast/index.html

[203] Például a Verizon a Netflix mellett az Apple-lel és a Microsofttal is kötött megállapodást, hogy a szervereiket közvetlenül bekapcsolja a saját hálózatába. https://money.cnn.com/2014/07/18/technology/netflix-verizon/

[204] Lorenzon, Emmanuel. "Zero-rating, content quality, and network capacity." Information Economics and Policy 58 (2022): 100965.