

híradástechnika

1945 VOLUME LXXIX. 2024

hírközlés ■ informatika

2



HTE 75 Infokommunikációs víziók

A Hírközlési és Informatikai Tudományos Egyesület folyóirata

Tartalom

HTE 75 Infokommunikációs víziók	1
SALLAI GYULA, VIDA ROLLAND, BACSÁRDI LÁSZLÓ, VÁGUJHELYI FERENC, GYIRES-TÓTH BÁLINT, BUTTYÁN LEVENTE, BARANYI PÉTER, RAB ÁRPÁD, BARTOLITS ISTVÁN	
A hálózati technológiák jövője: vízió 2040-re	4
VIDA ROLLAND	
A kvantum-infokommunikáció jövőképe	7
BACSÁRDI LÁSZLÓ	
Blokklánc technológiák: vízió az elkövetkezendő 10-15 évre	10
VÁGUJHELYI FERENC	
Mesterséges Intelligencia – a harmincas években	13
GYIRES-TÓTH BÁLINT	
Kiberbiztonság – helyzetkép és kitekintés a jövőre	16
BUTTYÁN LEVENTE	
Infotáció, az információ-vonzás koncepciója	19
BARANYI PÉTER	
Kell-e félnünk a jövőtől?	22
RAB ÁRPÁD	
Összegzés, a trendek összefonódása, feladataink	25
BARTOLITS ISTVÁN	
A HTE-ről dióhéjban	29

Hírközlési és Informatikai Tudományos Egyesület
www.hte.hu

Elnök
VÁGUJHELYI FERENC

H-1051 Budapest, Bajcsy-Zsilinszky út 12., 5. em./502.
Tel.: +36 1 353 1027 • E-mail: info@hte.hu

Szerkesztő
SALLAI GYULA
(BME, Távközlési és Mesterséges Intelligencia Tanszék)
Felelős kiadó
NAGY PÉTER

HU ISSN 2018-2028 • Layout: PLAZMA DS • Nyomda: KOERWI Kft.

A kiadvány támogatói



A folyóirat támogatói



HTE 75

Infokommunikációs víziók

SALLAI GYULA, VIDA ROLLAND, BACSÁRDI LÁSZLÓ,
VÁGUJHELYI FERENC, GYIRES-TÓTH BÁLINT, BUTTYÁN LEVENTE,
BARANYI PÉTER, RAB ÁRPÁD, BARTOLITS ISTVÁN

A HTE 75 éves évfordulójához kapcsolódóan a digitalizáció megatrendjének áttekintése után a cikk hét víziót tartalmaz, kitekintéseket a hálózati technológiák, a kvantum-infokommunikáció, a blokklánc technológiák, a mesterséges intelligencia, a kiberbiztonság, az infotáció és az infokommunikációs technológiák társadalmi hatásainak következő évtizedeire, és áttekinti összefonódásaikat.

Bevezetés, a digitalizáció megatrendje és a HTE

Egyesületünket, mai nevén a Hírközlési és Informatikai Tudományos Egyesületet (HTE, angolul Scientific Association for Infocommunications) 75 évvel ezelőtt, 1949-ben az analóg technika világában alapították, az 1950. évi első alapszabályában már Híradástechnikai Tudományos Egyesület (HTE) elnevezéssel. A 25 éves HTE-t a hálózati funkciók digitalizálása, a digitalizáció induló trendje már markánsan érintette. Az 50 éves HTE-t pedig már elnevezésének korszerűsítésére sarkalta: az informatikával való konvergencia és az infokommunikáció fogalmának elterjedése adta az Egyesület magyar és angol megnevezésének háttérét, a HTE rövidítés megtartása mellett.

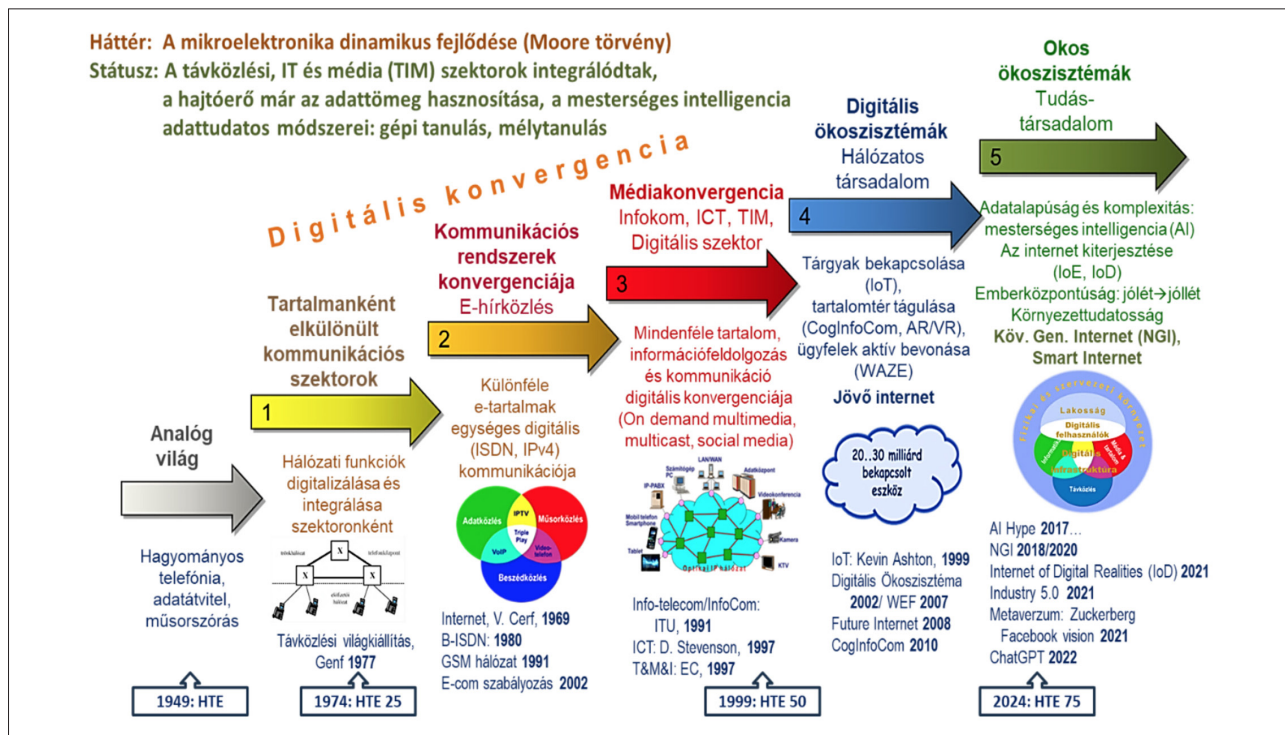
Mára a digitalizáció megatrendé vált, az internet általános elterjedése és a tárgyak, dolgok internetbe való bekapcsolása után már a digitalizáció ötödik fázisában vagyunk, a legfőbb hajtóerő a mesterséges intelligencia, és az internet további kiterjesztéséről, adatalapúságról, okos ökoszisztémákról, tudástársadalomról beszélünk. A digitalizáció elvárásaiban kiemelt hangsúlyt kap az emberközpontúság és a környezettudatosság. Az előbbi az életkörülmények minőségét kifejező jóllét (wellbeing) követelményeire utal, amely az anyagi jólétnél (welfare) szélesebb tartalmú, és amelybe olyan tényezők is beletartoznak mint a személyes adatok védelme vagy a kiberbiztonság. Az utóbbin a környezeti,

ökológiai fenntarthatóságra, a természeti erőforrások minőségének és reprodukálhatóságának védelmére gondolunk.

Az 1. ábra mutatja a digitalizáció megatrendjének fázisait, az egyes fázisok jellemzőit és meghatározó eseményeit¹, de elhelyeztük a HTE történetének negyedszázados időpontjait is.

A 2024-es ünnepi év Híradástechnika különszámában – e tartalmaz 75 éves időszakra való visszatekintések mellett – előre szeretnénk tekinteni, hogy melyek lesznek a HTE következő egy-két évtizedének izgalmas témái a digitalizáció megatrendje mentén, melyek lesznek a feltörekvő infokommunikációs technológiák, milyen is a nagyon gyorsan fejlődő szakmánk jelenleg, 2024 derekán látható jövőképe. Egy sorozatot indítottunk *HTE 75 Infokommunikációs víziók* címmel a HTE Hírlevelében, amelyhez elismert hazai szakembereket kértünk fel a HTE látókörébe tartozó szakterületekről, hogy fogalmazzák meg jövőképüket, az elkövetkező évtizedekben szakterületük előrehaladásának várhatóan átütő eredményeit. E cikkben az elkészült hét víziót és ezek összegzését egybe szerkesztve olvashatjuk.

¹ Sallai Gyula: „Evolution of Digitization toward the Internet of Digital & Cognitive Realities and Smart Ecosystems”, Infocommunications Journal, Special Issue: Internet of Digital & Cognitive Realities, HTE, 2023, p. 28., DOI: 10.36244/ICJ.2023.SI-IODCR.1



1. ábra – A digitalizáció megatrendjének fázisai

Elsőként a távközlés alapjául szolgáló *hálózati technológiák jövőképe*nek átgondolására **Dr. Vida Rolandot**, a BME VIK Távközlési és Médiainformatikai Tanszékének egyetemi docensét, a HSN (High-Speed Networks) kutatólaboratórium vezetőjét kértük. Vida Roland PhD fokozatát 2003-ban a párizsi Université Pierre et Marie Curie egyetemen szerezte, a HTE Külügyi Bizottságának elnöke, majd címzetes szenátora volt, jelenleg az IEEE Sensors Council alelnöke. Több mint 20 éve oktat a BME villamosmérnök hallgatóinak hálózati technológiákkal kapcsolatos tárgyakat és vesz részt ilyen tematikájú projekteken.



A sorozat 2. tagjaként a *kvantum-infokommunikáció jövőképe*nek megfogalmazására **Dr. Bacsárdi László** kvantum-informatikust, a BME VIK Hálózati Rendszerek és Szolgáltatások Tanszékének egyetemi docensét kértük. Bacsárdi László 20 éve foglalkozik kvantum-informatikával és kvantum-



kommunikációval kapcsolatos kutatásokkal, doktori disszertációját a kvantumvilág és az úrtávközlés kapcsolatából írta. A Műegyetem Mobil Kommunikáció és Kvantumtechnológiák Laboratóriumának, valamint a Kvantuminformatikai Nemzeti Laboratórium kvantum-kommunikációs programjának vezetője.

A sorozat 3. tagjaként a *blokklánc technológiák perspektíváját, jövőképét* mutatjuk be, amelynek összeállítására **Vágujhelyi Ferencet**, Egyesületünk elnökét kértük fel. Vágujhelyi Ferencben már ELTEs egyetemi tanulmányai alatt kialakult a kötődés a számelmélethez, a kriptográfiához, a blokklánc alapjához, és ma a Blockchain Koalíció elnöke, a Nemzeti Hírközlési és Informatikai Tanács elnöke, a Nemzeti Adó- és Vámhivatal vezetője.



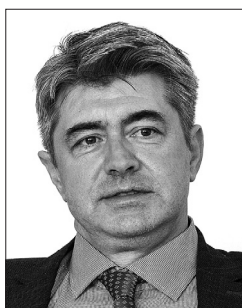
A sorozat 4. tagjaként a *mesterséges intelligencia jövőképe*nek megírására **Dr. Gyires-Tóth Bálintot**, a BME VIK Távközlési és Médiainformatikai Tanszékének egyetemi docensét kértük. Gyires-Tóth Bálint villamosmérnöki diplomáját és doktori fokozatát a Műegyetemen szerezte, több mint 15 éve foglalkozik elméleti és alkalmazott gépi tanulással, 2014 óta a deep learning (mélytanulás) az elsődleges kutatási területe. Számos sikeres MI kutatási és ipari projektben vett részt. A mélytanulás alapú MI kutatás és oktatása terén végzett eredményes munkáját számos elismerés kísérte.



A sorozat 5. tagjaként a *kiberbiztonság jövőképe*nek megfogalmazására **Dr. Buttyán Leventét**, a BME VIK Hálózati Rendszerek és Szolgáltatások Tanszékének egyetemi tanárát kértük. Buttyán Levente mintegy 30 éve foglalkozik informatikai biztonsággal kapcsolatos kutatásokkal. Doktori fokozatát a svájci EPFL-en, Lausanne-ban szerezte 2002-ben, az MTA Doktora címet 2021-ben kapta meg. 2003-tól oktat és kutat a Műegyetemen, a CrySyS Adat- és Rendszerbiztonság Laboratórium (CrySyS Lab) egyik alapítója és vezetője, számos hazai és nemzetközi kiberbiztonsági projekt témavezetője.



A sorozat 6. tagjaként a *digitális valóság internetének továbbgondolására* **Dr. Baranyi Pétert**, a Budapesti Corvinus Egyetem Adatelemzés és Informatika Intézetének egyetemi tanárát, a Kognitív Infokommunikációs kutatólaboratórium vezetőjét kértük. Baranyi Péter mintegy 20 éve foglalkozik rendszer- és irányításméssel. Doktori fokozatát a BME-n szerezte 1999-ben, az MTA Doktora címet 2006-ban kapta meg. 2006-ban lett a Magyar Mérnökakadémia tagja és 2009-ben a BME-n lett egyetemi tanár. A kognitív infokommunikáció általa megfogalmazott tudományos koncepciója nemzetközi tudományos konferenciák sorozatán át önálló tudományterületté vált.



A sorozat 7. tagjaként az *infokommunikációs trendek társadalmi hatásainak vízióját* **Dr. Rab Árpád** jövőkutató, a Nemzeti Közszerológati Egyetem Információs Társadalom Kutatóintézetének tudományos főmunkatársa fogalmazta meg. Rab Árpád két évtizede kutatja a digitális technológiák és a társadalom viszonyát, a jelen trendjeit és a jövő lehetséges forgatókönyveit a társadalom és a munka világában. Kiemelt kutatási területei a digitális kultúra, a társadalom helyzetének javítása a technológia segítségével, az életminőségjavító eszközök, a társadalmilag jó mesterséges intelligencia és az e-egészségügy.



A víziók összegzésére, az *infokommunikációs trendek összefonódásainak bemutatására* **Dr. Bartolits Istvánt**, a Nemzeti Média- és Hírközlési Hatóság Technológiaelemző főosztályának vezetőjét kértük. Bartolits István villamosmérnök, a BME címzetes egyetemi docense, a HTE vezetőségének 1990 óta tagja, az infokommunikáció történelmének szakavatott ismerője, „A HTE 60 éve” kötet szerkesztője, a HTE „Párhuzamos mérőldkövek” kiadványának szerzője, a digitalizáció technológiai trendjeinek szakértője, elemzője, rendszeres előadója.



A HTE 75 Infokommunikációs víziók szervezője, szerkesztője, bevezetőjének szerzője **Dr. Sallai Gyula**, a HTE tiszteletbeli elnöke. Sallai Gyula okl. villamosmérnök, az MTA doktora. Életpályája során a távközlés, ill. az infokommunikáció területén kutatóként, majd kutatási, stratégiai és szabályozási vezetői munkakörökben dolgozott. 1997-től a BME egyetemi tanára, nyolc évig a Távközlési és Médiainformatikai Tanszék tanszékvezetője, négy évig az egyetem rektorhelyettese. A HTE-nek több mint 20 évig vezetőségi tagja, hat évig elnöke volt. Jelenleg a BME professor emeritusa.



A hálózati technológiák jövője: vízió 2040-re

VIDA ROLLAND

BME, Távközlési és Médiainformatikai Tanszék*

Ahhoz, hogy valaki megjósolja a technológiai fejlődés jövőjét, ráadásul 10-15 éves időtávlatban, viszonylag nagy bátorságra van szükség. Számos olyan példát ismerünk, amikor híres szakemberek, piacvezető világ-cégek, vagy ismert újságírók, véleményvezérek álltak elő olyan jóslatokkal, melyek egyáltalán nem váltak valóra, kínos helyzetbe hozva a mögöttük felsorakozó szakértőket.

Az egyik legismertebb példa talán erre Bob Metcalfe, az Ethernet technológia kidolgozójának esete, aki 1996-ra az internet teljes összeomlását jósolta, majd egy évvel később kénytelen volt látványosan megenni papírra kinyomtatott szavait egy konferencián, egy pohár víz kíséretében [1]. Szintén nem vált valóra az a jóslat sem, miszerint a címtartomány kimerülése miatt az IPv4-et nagyon gyorsan felváltja majd az IPv6. Egy 2002-es Internet Engineering Task Force (IETF) meetingen Atlantában a hivatalos konferencia-pólón egy óriási IPv6 felirat díszelgett, és mindenki az IPv6 megállíthatatlan elterjedéséről beszélt a „következő 1-2 évben”. Az egyetemen azóta is minden évben abban a pólóban jelenek meg a hallgatók előtt, amikor az IPv6-ról tartok előadást. A póló már eléggé megviselt, de igyekszem kímélni, hátha kitart még a 15-20 év múlva esedékes nyugdíjba vonulásomig, hiszen mindeközben a felhasználók többsége 2024-ben is még IPv4-es címeiről csatlakozik az internetre [2].

Magyarországon az egyik legismertebb kissé félresikerült technológiai jóslás Uj Péter nevéhez fűződik talán, aki bár egy 2000-ben megjelent cikkében [3] helyesen titulálta a WAP (Wireless Application Protocol) szabványt egy „blöffnek”, de a WAP csak mint konkrét technológiai megoldás bizonyult zsákutcának. Maga az elv viszont, hogy a mobiltelefonokat internetezésre és video tartalmak fogyasztására fogjuk használni, teljes

mértékben megvalósult. Pedig cikkében olyanokat állított, hogy senki nem akar majd liftben vagy autóban internetezni az apró monokróm kijelzős mobiltelefonján, amikor ott lesznek a telepített, kényelmes és gyors vezetékes eszközök, melyek elé csak oda kell ülni, illetve csupán „integrációs hóbortnak” nevezte azt az elképzelést, hogy a mobiltelefont amolyan svájcibicskaként másra is használnánk, mint telefonálásra. Több mint 20 év távlatából ma már megmosolyoghatjuk ezeket a sorokat, bár Uj Péter mentségére legyen mondván, 2000-ben ő még nem számolhatott azzal, hogy néhány évvel később megjelennek az okostelefonok, melyek gyökeresen megváltoztatták tartalomfogyasztási szokásainkat és az azokat kiszolgáló hálózati technológiákat is.

Mindezek ellenére, a következőkben mégis megpróbálkoznék azzal, hogy röviden felvázoljam, mi is várható a hálózati technológiák területén a következő 10-15 évben. És remélem, hogy 2040-ben, ha majd lesz alkalmam újra olvasni e sorokat, nem fogok majd túlságosan szégyenkezni az esetleges tévedéseim miatt.

A 2030-as évek második felére a 6G hálózatok világszerte elérhetőek lesznek, a 7G hálózatok szabványosítása pedig a végső fázisába ér. Ezekben a hálózatokban több száz gigabites/terabites sebességek, mikroszekundumos késleltetések, és hét-kilences rendelkezésre állás várható. Ehhez szükség lesz a sub-terahertzes és terahertzes frekvenciák használatára, a falakba és tereptárgyakba integrált nanoantennákra, nano-műholdakra és kooperatív drónokra.

Kezdeném talán a legkézenfekvőbb területtel, mégpedig a mobil technológiákkal, hiszen nagy kockázatvállalás nélkül kijelenthető, hogy a 2030-as évek második felére a 6G hálózatok már világszerte elterjedtek lesznek, és a 7G hálózatok szabványosítása a végső fázisába ér majd. A kockázat ebben az esetben azért

* 2024. július 1-től névváltozással: BME, Távközlési és Mesterséges Intelligencia Tanszék

minimális, mert a mobil technológiák generációi rendszeresen 9-10 évente váltják egymást. A GSM (2G) 1991-ben indult, az UMTS (3G) hálózatok 2001-ben jelentek meg, az első LTE (4G) telefon 2010-ben került piacra, az 5G szolgáltatások 2019-ben indultak, a 6G szabványokat pedig 2028-2030-ra várják. Összességében elmondható, hogy a generációk ilyen jellegű számozása inkább takar marketing megfontolásokat, mintsem konkrét technológiai mérföldköveket. A szakértő kutatók és mérnökök persze meghatároznak konkrét fejlesztési irányokat és célokat a következő generációs technológiát illetően, ám ha marketing szempontból szükségessé válik az új generáció piacra kerülése, akkor az rendszerint meg is történik, függetlenül attól, hogy sikerült-e időközben elérni a kitűzött célokat, vagy sem. A kérdés tehát nem az, hogy lesz-e 6G és 7G hálózat 1015 éven belül, hanem inkább az, hogy ezek konkrétan milyen technológiai megoldásokat fognak majd tartalmazni, és milyen paraméterekkel rendelkeznek majd.

A mobil technológiák különböző generációi felé jellemzően mindig egyre komolyabbak az elvárások a hálózati paramétereket illetően. Ennek megfelelően, míg az 5G hálózatok jellemzően 1 Gbps-es (vagy az alatti) felhasználói letöltési sebességeket nyújtanak manapság, a 6G hálózatoktól 10-100 Gbps-es sebességeket remélnék, a 7G-ben a cél pedig várhatóan a terabites sebességek elérése lesz. Ami a késleltetést illeti, az 5G hálózatoknál az 5 ms alatti késleltetés elérése volt a cél, a 6G-ben viszont már várhatóan mikroszekundumos tartományban mozgó késleltetés lesz, a 7G hálózatok pedig ezt tovább csökkentik majd. De fontos lesz a 6G/7G hálózatokban a még nagyobb, várhatóan „hét kilences”, azaz 99,99999%-os rendelkezésre állás (ami 3 mp/év kiesést jelent), a hasonló szintű megbízhatóság, a milliárdnyi IoT eszköz csatlakozásának támogatása, és kiemelt fontosságú lesz az energiahatékony működés.

De hogyan érjük majd el ezt a jelentős javulást az említett paramétereket illetően? Egyfelől egyértelmű iránynak tűnik, hogy az 5G által használt mmWave (milliméteres hullámok) mellett a 6G/7G hálózatokban sor kerül majd az úgynevezett sub-terahertzes (100-300 GHz) és a terahertzes (300 GHz és 3 THz közötti) frekvenciák használatára is, melyek biztosítani tudják a jóval nagyobb sávszélességet és alacsonyabb késleltetést. Ezeknek a frekvenciáknak a hátránya azonban, hogy többnyire közvetlen rálátást igényelnek, és kis távolságokat tudnak csak hatékonyan áthidalni. Ezért várható a mindennél jelenlevő, épületek falaiba, utcai tereptárgyakba, bútorokba ágyazott nanoantennák elterjedése, melyek egymással együttműködve, közösen szolgálják majd ki

a felhasználókat, a hagyományos cellás elrendezéstől eltérően. Mindemellett a folyamatos rendelkezésre állás biztosításához a 6G hálózatok nagymértékben építenek majd az úgynevezett NTN (Non-Terrestrial Networks) kommunikációra, mely integrálja úgy a hagyományos műholdakat, a nano-műholdakat, mint a kooperatív drónokat.

10-15 éves távlatban a WiFi 10/11/12 szabványok is megjelennek majd, ezekben a felhasználók közötti versengést az erőforrásokért felváltja majd a mesterséges intelligenciára alapuló együttműködés. A WiFi offloading, azaz a mobil hálózatok forgalmának részleges áttérrelése WiFi csatornákra, kiemelt fontosságú lesz.

A WiFi, napjaink másik meghatározó vezeték nélküli kommunikációs technológiája, nagy valószínűséggel szintén velünk lesz 10-15 év múlva is. A WiFi esetén a generációk viszont jóval gyorsabban váltják egymást. Jelenleg a WiFi 7 szabványosításának véglegesítése zajlik, de az 5G URLLChoz (Ultra Reliable Low Latency Communications) hasonló kiemelt megbízhatóságot nyújtó IEEE 802.11bn UHR (Ultra High Reliability) WiFi 8 szabvány kidolgozása is elkezdődött már, annak lezárása 2028-ra várható. 10-15 éves távlatban pedig majd minden bizonyosan a WiFi 10/11/12 szabványok is megjelennek majd.

Az, hogy a hasonló technológiai paramétereket a WiFi szabványok csak néhány év késéssel tudják nyújtani a 3GPP (3rd Generation Partnership Project) mobil kommunikációs szabványokhoz képest nagyrészt annak tudható be, hogy amíg az 5G esetén a licensztköteles frekvenciákon történő erőforrás-kiosztást, a csatornához való hozzáférést és a különböző adatfolyamok prioritizálását a szolgáltató egymaga tudja biztosítani, addig a WiFi mindeddig a licenszmentes csatornákon zajló szabad versenyre épített. Az újabb WiFi szabványokban azonban a felhasználóknak versengés helyett inkább együtt kell majd működniük, a hálózati erőforrások mesterséges intelligenciára alapuló optimális kezelésére támaszkodva.

Mindemellett a mesterséges intelligenciának az úgynevezett WiFi-offloading megoldásokban is jelentős szerepe lesz. Az offloading lényege az, hogy a mobil szolgáltatók a forgalmuk egy részét a rendelkezésre álló WiFi csatornákon vezetik keresztül, jelentősen kiegészítve ezzel a mobil hálózatok erőforrásait. A WiFi offloading kérdésével már viszonylag régóta foglalkoznak, a 2030-as években azonban ez a technológia már várhatóan minden hálózatban kiemelt fontosságú lesz.

A vezetékes hálózatokat 10-15 év múlva teljes mértékben az optikai technológiák fogják dominálni, több terabites átviteli sebességeket biztosítva egyetlen optikai szálon. Mindemellett azonban az olyan hagyományos hozzáférési megoldások, mint a réz érpáron működő modernebb DSL verziók se tűnnek még el teljesen a kínálatból.

Végezetül mindenképp szükséges beszélnünk a vezetékes hálózatokról, melyeket 10-15 év múlva várhatóan teljes mértékben az optikai technológiák fognak dominálni, úgy a hozzáférési részen, mint a gerinchálózatokban. Az egyre nagyobb átviteli sebességeket és egyre alacsonyabb késleltetést igénylő alkalmazások kiszolgálására olyan hatékonyabb modulációs technikák terjednek majd el, mint a PCS (Probabilistic Constellation Shaping), illetve széleskörben bevezetésre kerülnek a hullámhosszosztásra épülő DWDM (Dense Wavelength Division Multiplexing) megoldások, melyek segítségével több-terabites átviteli sebességek válnak elérhetővé egyetlen optikai szálon keresztül is. Mindemellett azonban a 10-15 éves időtáv várhatóan nem elegendő ahhoz, hogy a többi „hagyományos” hozzáférési technológia teljes mértékben eltűnjön a kínálatból. Így például a korábbi vezetékes telefonhálózatok réz érpárjait használó DSL (Digital Subscriber Line) megoldások is velünk lehetnek még akár 2040-ben is, olyan frissen elfogadott szabványok vagy egyelőre csak a kutatólaboratóriumokban tesztelt technológiák segítségével, mint az MGFast vagy a Terabit-DSL.

Összegzésként elmondható, hogy a következő 10-15 évben a hálózati technológiák folyamatos fejlesztésére lesz majd szükség annak érdekében, hogy a szolgáltatók képesek legyenek olyan terabites átviteli sebességeket, mikroszekundumos késleltetéseket és/vagy hét-kilences megbízhatóságot igénylő alkalmazásokat támogatni, mint az önvezető járművek kommunikációja, a kiterjesztett valóság megoldások, a digitális iker technológiák, vagy olyan más alkalmazások, melyekre ma még nem is gondolunk. A hálózati erőforrások hatékony kezelésében mindenképpen nagy szerepet játszik majd a mesterséges intelligencia, és kiemelt figyelmet kell majd fordítani az energiahatékonyságra és a fenntarthatóságra. A technológiai fejlesztések pontos irányát azonban nagymértékben befolyásolhatják olyan gazdasági és politikai szempontok is, mint az egyes országok különböző frekvenciagazdálkodási és szabályozási döntései, vagy a technológiai megoldások mögött álló multinacionális nagyvállalatok lobbijereje.

Hivatkozások

- [1] Sky Dayton: „When your hero forecasts your demise”, Medium, 2024. január 9.
<https://medium.com/@skydayton/when-your-hero-forecasts-your-demise-232947be1932>
- [2] IPv6 Adoption Statistics, Google, 2024.
<https://www.google.com/intl/en/ipv6/statistics.html>
- [3] Uj Péter: „A nagy WAP-blöff”, Index, 2000. április 6.
<https://index.hu/tech/mobil/wapup/>

A kvantum-infokommunikáció jövőképe

BACSÁRDI LÁSZLÓ

BME, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelenünk: a második kvantumtechnológiai forradalom kora

A kvantummechanika születését követően az első kvantumtechnológiai forradalom számos eszközt adott számunkra, és ma már elképzelhetetlen lenne az életünk napelemek, nukleáris energia, félvezetők vagy éppen lézerek nélkül. Napjainkban a második kvantumtechnológiai forradalom korát éljük, amelyet az jellemez, hogy képesek vagyunk egyedi részecskéket (atomokat, spineket, fotonokat) is manipulálni, oly módon, amely korábban elképzelhetetlennek tűnt. Ez a forradalom négy nagy területen jelenik meg: kvantumszámítógép, kvantumkommunikáció, kvantumszimuláció és kvantumérzékelés. 2023-ban közel negyven milliárd dollárra becsülték a kvantumtechnológiával kapcsolatos kutatások és fejlesztések értékét. A négy terület közül a kvantumkommunikációnak, amelyet inkább már kvantum-infokommunikációnak nevezhetnénk, kiemelt jelentősége van, már most több kereskedelmi célú termék érhető el a piacon, s folyamatosan jelennek meg újabb cégek innovatív termékeikkel.

A kvantum-infokommunikáció számos érdekes megoldást kínál számunkra, mint a kvantum alapú kulcszétosztás, kvantum alapú véletlenszámok, illetve a kvantuminternet. A **kvantum alapú kulcscsere** (angolul quantum key distribution, QKD) során kvantumcsatornán keresztül osztunk meg egy titkos kulcsot, amelyet utána klasszikus szimmetrikus kulcsú titkosításra használunk fel. Ennek révén növelni tudjuk a rendszereink biztonsági szintjét, ugyanis a kvantum alapú kulcsszétosztás biztonságát a kvantumfizika törvényei garantálják, biztosítva, hogy passzív támadást (lehallgatást) nem tudunk végrehajtani, aktív támadásról (beavatkozásról) pedig értesülnek a kommunikáló felek. A **kvantum alapú véletlenszám-generátorok** (angolul quantum random number generator, QRNG) segítségével kvantumfizikai folyamatokra alapozva tudunk

véletlen számokat előállítani. Mind QKD-eszközökből, mind QRNG-eszközökből számos érhető el a piacon, s van olyan mobilgyártó, aki a készülékébe is integrált QRNG chipet. A jelenleg inkább kísérleti körülmények között létező **kvantuminternet** olyan jellegű megoldásokat takar, amelyek lehetővé teszik majd, hogy nagy távolságba juttassunk el kvantuminformációt, kihasználva olyan meglepő kvantumfizikai jelenségeket, mint az összefonódás.

Jelenünk: Magyarország a világtérképen

Magyarországon többen is foglalkoznak különböző kvantumtechnológiai fejlesztésekkel. A Kvantuminformatika Nemzeti Laboratórium (KNL) segíti a kvantumtechnológia térnyerését a hazai oktatásban és kutatás-fejlesztési projektekben, inkubátorként és szakmai referenciaként működik a hazai vállalkozások és a magyar kormány szervei számára, valamint megjeleníti és képviseli a hazai kvantumtechnológiai ökoszisztémát európai uniós és egyéb szervezetekben. A KNL öt tagja a HUN-REN Wigner Fizikai Kutatóközpont, a Budapesti Műszaki és Gazdaságtudományi Egyetem Természettudományi Kara (BME TTK) és Villamosmérnöki és Informatikai Kara (BME VIK), az Eötvös Loránd Tudományegyetem (ELTE) Informatikai Kara és Természettudományi Kara. A BME Villamosmérnöki és Informatikai Karán már több mint 20 éve foglalkoznak kvantuminformatikával és kvantumkommunikációval, az elméleti kutatások mellett az egyetem szakemberei különböző kvantumkommunikációs rendszerek építésébe is belevágtak. A Műegyetem szakmai eredményeire alapozva a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) vezetésével a BME, ELTE és HUN-REN Wigner FK részvételével 2023 januárjában indult el a QCIHungary projekt, amely az európai kvantumkommunikációs infrastruktúra részeként egy nemzeti kvantumkommunikációs infrastruktúra kezdeti kialakítását célozta meg.

Nagy hangsúlyt kell fektetni a következő generáció képzésébe is, a Műegyetemen ezért indult el 2023 tavaszán az országban elsőként a kvantuminformatika mellékspecializáció mérnökinformatikus mesterszakos hallgatók számára. De a Műegyetemen futó egyéb, kvantuminformatikával és kvantumkommunikációval foglalkozó tárgyaknak köszönhetően már több ezren hallottak a magyar mérnökök közül arról, milyen fontos is ez a terület.

A kvantum-infokommunikációra a HTE is kiemelt figyelmet fordít. 2021 novemberében a HTE Infokom konferencián a „Kvantumkommunikáció 2030” elnevezésű kerekasztal-beszélgetés során szakértőkkel egy tízéves jövőképre tekintettünk ki (a felvétel elérhető a HTE YouTube-csatornáján), és a 2024-es HTE Infokom konferencián is elő fog kerülni a témakör. A HTE Távközlési Szakosztály által szervezett Távközlési klubon is rendszeresen visszatérnek a kvantumos világ különböző kérdései, 2024-ben is lesz kvantumkommunikációval foglalkozó HTE Távközlési Klub. A HTE által kiadott Infocommunications Journalban pedig a területen elért izgalmas kutatási eredményekről lehet olvasni hazai és nemzetközi szerzőktől.

Jövőbe nézve: a terület 2040-ben

Azt, hogy 2021-ben mit gondoltunk arról, milyen lesz a kvantum-infokommunikációs világ 9 évvel később, meg lehet nézni a HTE Youtube csatornáján a Kvantumkommunikáció 2030 panelbeszélgetés felvételén. De vajon milyen lesz a terület 2040-ben? Többféle forgatókönyv is lehetséges, de a 75 éves HTE előtt tisztelgetve egy optimista jövőkép jelenik meg most a jósgömbben.

Képesek leszünk arra, hogy kifejlesszünk hatékony hibajavító megoldásokat, amelyek stabilabbá fogják tenni a kvantumkapuk működését. Ennek a technológiai fejlődésnek köszönhetően el fogunk jutni a nagy kvantumbitszámmal megbízhatóan operáló kvantumszámítógépek korába. Ezekben olyan kvantumalgoritmusokat tudunk futtatni, amelyek segítségével hatékonyabbá tehetjük a gyógyszerkutatást, a pénzügyi kockázatbecslést, a nagyméretű adatbázisokban való keresést. A kvantumszámítógépek – méretükből adódóan – továbbra is az ezzel foglalkozó szakemberek számára lesznek elérhetőek, azaz a mindennapi életünkben továbbra is a megszokott klasszikus eszközeinket fogjuk használni, de egyre többször fogjuk igénybe venni a kvantumszámítást mint szolgáltatást (Quantum-as-a-Service (QaaS)). Azon szervezetek, akik számára kritikus, hogy megbízható hardver- és szoftver-

elemekből építkező eszközeik legyenek (és ne kelljen megbízni egy másik országban működő szolgáltatóban), saját kvantumszámítógéppel fognak rendelkezni.

Azokon a helyeken, ahol számít a biztonság (kommunikáció, adatok titkosítása, digitális aláírások stb.) olyan megoldásokat fogunk használni, amelyek matematikailag és/vagy fizikailag bizonyítottan védettek a kvantumszámítógép támadásaival szemben. A matematikailag bizonyított eljárások közé tartoznak az úgynevezett posztkvantum algoritmusok, amelyek használata széles körben elterjedt lesz. Ugyanakkor még mindig nem fogjuk pontosan látni, hogy a kvantumszámítógép információelméleti szempontból milyen problémaosztályokban képes feladatokat megoldani, ezért a klasszikus kriptográfiával foglalkozó szakemberek továbbra is dolgozni fognak azon, hogy a kvantumszámítógép által jelentett biztonsági fenyegetésre válaszul újabb és újabb posztkvantum-algoritmusokat alkossanak.

A fizikailag bizonyítottan védett kvantum alapú megoldásokat – amelyek a fizika törvényeire alapozva védettek a támadásoktól – sok helyen fogják használni. Ilyenek pl. az úgynevezett kvantum alapú kulcsszétosztó hálózatok, amelyek a mindennapi infrastruktúra részét fogják képezni a kormányzati, a pénzügyi és a kritikus infrastruktúrát üzemeltető szektorok esetén. Az Európai Unió területén üzemelni fog az Európai Kvantumkommunikációs Infrastruktúra (European Quantum Communication Infrastructure, EuroQCI) legújabb verziója, amely alapgondolatát 2019-ben júniusában fogalmazták meg az EuroQCI deklarációjában. Az EU-s tagországok közötti optikai szálak kapcsolaton túl az európai kvantumkommunikációs műholdak is az összeköttetés szerves részét fogják jelenteni.

Már a 2020-as évek közepén is számos kvantumkommunikációs cég jelent meg a piacon, de az elérhető termékek köre még szélesebb lesz 2040-re. A földi környezetben (optikai szálon) használható megoldásokon túl számos cég fog kínálni általa üzemeltetett kvantumkommunikációs műholdakra alapozott szolgáltatást, amelyekről optikai kommunikációval (vagyis lézerek segítségével) lehet majd továbbítani a kulcsokat. A kriptográfiai szempontból kritikus hardvereszközök jelentős része fog tartalmazni integrált kvantum alapú véletlenszám-generátort.

A kvantuminformaticus és a kvantumkommunikációs mérnök kifejezésekkel leírt szakma már nemcsak egy fehér holló jellegű ritkaság lesz, hanem szélesebb körben is elismertté válik, hasonlóan ahhoz, ahogy a 2020-as években az űrmérnök kifejezés és az űrmérnök képzet is elterjedt hazánkban.

A kutatások jövője: kvantuminternet

A jósgömbben idáig látottak levezethetők a jelenlegi technológiai trendekből. Amely terület jövőbeli technológiai érettségét homály fedi, az a kvantuminternet világa. Egy olyan hálózaté, amelyek segítségével több csomóponton áthaladva vagyunk képesek kvantuminformációt továbbítani. Egy olyan hálózaté, amely különleges hardvereszközöket és különleges szoftvereket tartalmaz. A kvantuminternet segítségével képesek leszünk jelentősen megnövelni az összefonódáson alapuló kvantumkommunikációs protokollok működési távolságát és összekapcsolni távoli helyeken működő kvantumszámítógépeket.

Ilyen hálózat – nagy távolságban – jelenleg a kvantumfizika törvényei szerint (különösen a Nincs másolás tétel miatt) nem megvalósítható, ugyanis nem tudunk olyan erősítőket építeni, mint amit a klasszikus világban megszokhattunk. Az összefonódás-megosztás (entanglement swapping) és a kvantummemóriák segítségével

azonban lehetőségünk lenne a kvantumteleportáció protokollját használva távoli kvantumrendszerek összekapcsolására. Számos kutatás zajlik ezzel kapcsolatban szerte a világon, Európában és Magyarországon is. (A Műegyetem kutatói is kidolgoztak olyan protokollokat, amelyeket a kvantuminterneten lehet majd használni). Ráadásul nemcsak földi környezetben működhet: többek között az Európai Űrügynökség is vizsgálja, hogyan lehetne kvantummemóriákat a műholdakon elhelyezni. Az Internet Engineering Task Force (IETF) kvantuminternettel foglalkozó munkacsoportja már kidolgozta a kvantuminternet első szabványos protokolljait, vannak kísérleti rendszerek Európában is, de a tényleges, nagy távolságú kvantuminternethez szükség van megfelelő hardverekre. Csak bízni lehet abban, hogy a kapcsolódó kutatások sikeresek lesznek, és a különböző fizikai technológiákra alapozott kvantummemóriák koherenciaideje a milliszekundumról/percekről órákra/napokra fog nőni. Ha ez megtörténik, akkor 2040-re a kvantumkulcs-csere hálózatok mellett a kvantuminternet is a műszaki világ része lesz.

Blokklánc technológiák: vízió az elkövetkezendő 10-15 évre

VÁGUJHELYI FERENC

HTE elnök, a Blockchain Koalíció elnöke

Mi a blokklánc (blockchain) és mi hívta életre?

A blokkláncról elmondható, hogy a legtöbb előnyt nem ott fogjuk kiaknázni a technológiából, ahol megalkotói gondolták. Ők ugyanis egy decentralizált rendszerben működő elektronikus pénz megteremtését tűzték ki célul. Ehhez hiteles elektronikus „bankjegyeket” (vagy pénzérméket) kellett létrehozniuk, amihez az aszimmetrikus kulcsú kriptográfián alapuló elektronikus aláírást használták. Mivel az elektronikus jel korlátlanul és tökéletesen másolható, így azt is meg kellett oldani, hogy annak elköltésére csak az utolsó tulajdonos legyen képes, de ő is csak egyszer. Ez már csak egy közösen vezetett nyilvántartással volt megoldható. Fáradozásait azért koronázhatta siker, mert olyan konszenzus-protokollt találtak ki, amelyben mindenki a befektetett erőforrások arányában szólhatott bele a működésbe. Aki viszont sokat fektetett be, annak már több hasznot hozott a korrekt működés, mint a csalás, amely a teljes rendszerbe vetett bizalmat romba döntötte volna, így elértéktelenítve korábbi befektetéseit. Az eredmény a Bitcoin, az okoskereskedések futtatására képes Ethereum és számos társuk lett. A siker mérése az, hogy a kriptopiaccból 48 százalékkal részesedő Bitcoin piaci kapitalizációja jelenleg (2024.02.24.) ezer milliárd dollár, ami a gazdasági megfontolásokon túl a matematikai és műszaki megoldásba vetett óriási bizalmat is mutatja.

A fejlesztések eredménye megmutatta, hogy az elektronikus aláírásnál használt kulcspár nyilvános tagjának hash-kódja a kvantumszámítógépek által használható információ nélkül képes anonim módon megcímezni a tulajdonost. A kriptográfiai hash algoritmusokra építő, kizárólag a befektetett energiára épülő kiválasztási szabály megakadályozza, hogy valaki arra építsen támadást, hogy a következő blokkokat nagy valószínűséggel ő könyvelheti le. A digitális pénzverés, azaz a monetáris

eszköz megteremtése biztonságosan szabályozható egy teljesen nyilvános, bárki által hozzáférhető rendszerben. A bankrendszerben tárolt pénz túlnyomó része ma is elektronikus formában létezik, de ennek biztonságát az adja, hogy a pénzügyi rendszer zárt, és az a feltételezés, hogy meg lehet benne bízni. A blokklánc ezzel ellentétben nyitott, nincs központi döntéshozó, a felhasználók mégis rosszabbul járnak, ha eltérnek a protokolltól. Ezért kívülről úgy tűnik, mintha a szabályrendszer önmagát kényszerítené ki.

A blokklánc technológiák kihívásai és várható előre lépései

„Zöld” konszenzus protokoll

A Bitcoin rendszerben a node-ok gyűjtik a tárcaprogramok által összeállított és aláírt tranzakciókat, ellenőrzik, hogy azok a blokklánc szabályainak megfelelnek-e, és ha igen, összeállítják belőlük a következő blokkot. Ezzel egyszerre sok ezren próbálkoznak és központi döntéshozó nélkül kell egyetértésre jutniuk abban, hogy kinek a blokkjával folytatódjon a lánc. A győztes az, aki a saját blokkjához olyan (sónak is nevezett) adatot talál, amelyet a blokkhoz írva annak SHA256 hash-értéke egy adott értéknél kisebb lesz, például húsz nullával kezdődik. A feladat nehézségét körülbelül kéthetente, 2016 blokkonként határozzák meg a node-ok úgy, hogy a blokkidő tíz perc körül maradjon. Ha a teljes rendszer számítási kapacitása (hash power-je) nő, növelni kell a megoldandó feladat nehézségét, ha csökken, könnyíteni. Mivel a bányászat jövedelmező, így óriási számítógépfarmokat használnak SHA256 értékek kiszámítására különböző véletlenszerűen választott „só” értékekkel. Ez hihetetlen mennyiségű elektromos energiát igényel, így a konszenzust eredményező véletlen kiválasztáshoz egy új, energiatakarékos szabályrendszer kell találnunk. Az elkövetkező évtizedben ilyen megoldásokra fogunk áttérni.

A központ nélküli közösség – a szuverenitás közös és decentralizált gyakorlása

Az elektronikus hitelesség első eszköze az elektronikus aláírás volt. A bizalom jogszabály által meghatározott infrastruktúrán alapult: hatóság által kijelölt gyökértanúsító tanúsítvány kiadók, hatósági eszközökkel azonosított aláírók, és a hardverre és a kriptográfiai algoritmusra vonatkozó műszaki szabályok. Ezzel párhuzamosan, a PGP (Pretty Good Privacy) program megjelenését követően kialakult egy decentralizált közösségként működő rendszer a "Web of Trust", a „bizalom hálója”. Ha egy új csatlakozót azonosítani tudott egy régebbi tag, akkor saját aláírásával felülhitelesítette az új tag nyilvános kulcsát, kijelentve, hogy az adott személy hozzá tartozik. Itt a többi tagon múlt, hogy mennyire bízott az alkalmi hitelesítőben. A blokklánc rendszerekben se az állam főhatalmára, se bizalomra nincs szükség a protokoll szerinti működéshez. Ez megteremti a lehetőséget arra, hogy természetes személyek, vállalatok vagy akár országok működjenek együtt közösen létrehozott, de felettük álló központi szervezet nélkül. Az Európai Unió jó példa a hierarchiára épülő együttműködésre: a tagállamok minden olyan kérdésben, ahol közösen akarják gyakorolni szuverenitásuk egy részét, központi szervet hoznak létre. Ezek az Európai Bizottság főigazgatóságai vagy ügynökségei. Ezek létrejöttüket követően önálló életre kelnek, felismerik sajátos szervezeti érdekeiket, ellenőrzik, beperlik, sőt szankcionálják az őket létrehozó tagállamokat. Ugyanakkor a blokklánc rendszerekben is implementálható olyan működési modell, ahol a tagállamok illetékes szervei központi szerv nélkül vannak alávetve a közösen létrehozott protokollnak. Az ezt megsértő működés egyszerűen nem számít döntésnek, a tagállami node-ok nem fogják az ehhez kapcsolódó információt lekönyvelni. Az elkövetkező másfél évtizedben a szuverén közösségek (állami hatóságok, emberek, cégek) fokozatosan ilyen módon fogják kialakítani szakmai együttműködési közösségeiket.

A kvantumszámítógép és a blokklánc

A blokkláncban tárolt adatokon a tárcaprogramokban tárolt privát kulcs segítségével lehet tranzakciókat hitelesíteni. A hitelesítés ellenőrzéséhez szükség van a nyilvános kulcsra, amelynek csak a hash-kódját tárolja a blokklánc, így a tranzakció adataihoz csatolni kell. A tranzakciónak a könyvelő node-oknak történő elküldésének pillanatától kezdve viszont a kvantumszámítógépek megkísérelhetik a hitelesített adat, az aláírás és a nyilvános kulcs birtokában kiszámítani a titkos kulcsot, amellyel saját maguk számára jövedelmező módon megváltoztathatják a tranzakció tartalmát, aláírják, majd ők is igrkeznek minél több node-nak eljuttatni

saját verziójukat a tranzakcióról. Ha a blokkidő töredéke alatt képesek a törésre, akkor van rá esélyük, hogy időnként az ő verziójuk kerül be a következő blokkba, azaz hasznot realizálhatnak. A blokkidő lerövidítése csökkenti a törés veszélyét, de mivel nem lehetünk biztosak a támadó tényleges képességeiben, így teljes védelmet nem ad. Így előbb-utóbb a blokklánc rendszerek hitelesítő algoritmusát kvantum-algoritmus álló megoldásra kell cserélni. Ez a kvantumszámítógépek fejlődésével párhuzamosan meg fog történni.

ZK-proof, ZK-SNARK megoldások

Az elkövetkező évtizedben általános lesz, hogy a kereskedelemben és a gazdaságban a személyek és cégek azonosítása digitálisan történik. Ugyanez vonatkozik például egyes jogosultságok igazolására is. Ha például valaki cigarettát akar vásárolni, akkor igazolnia kell, hogy elmúlt 18 éves. Ha ezt hagyományosan, a személyazonosító kártyájának a bemutatásával teszi meg, akkor még az anyja nevét is megismerheti az eladó, de valójában még a nevére sem fog emlékezni, amikor kimegy az üzletből. Ha viszont ezeket az adatokat digitális eszközzel olvassa ki, akkor műszaki értelemben megszerzi azt a képességet, hogy el is tárolja, a fogyasztás jellemzőihez kösse és viselkedés elemzést végezzen rajta. Valójában még a születés időpontjának megismerése sem indokolt, mivel pontosan egy bit adatot kell hitelesen megismerni: nagykorú-e az ügyfél. Erre kiváló kérdezz-felelek alapú, valós idejű, zéró tudásátadással járó interaktív algoritmusok léteznek már ma is. A blokklánc rendszerekben nagyon sokszor ütközünk olyan problémába, hogy egy entitásnak egyetlen attribútumát kell hitelesen igazolni úgy, hogy magának az entitásnak a megismerése nem indokolt. A fizikailag távoli szereplők között, a blokkláncon keresztül megvalósult interaktív bizonyítás – ellentétben a dohányboltban történő vásárlással – sem időtartamát, se költségét tekintve nem ésszerű megoldás. Ezért a következő évtizedben fejlődni fognak a ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) megoldások, ahol a bizonyítást végző és az ellenőrzést végző olyan digitális adatokkal és algoritmussal rendelkezik, amely reális megoldást jelent a blokklánc architektúrában.

Okosszerződések, az orákulumok hitelessége

Az okosszerződések olyan programkódok, amelyeket a blokkláncot könyvelő gépek (nodeok) a tulajdonosok tárcaprogramjai által hitelesítve, összeállított tranzakciók utasítása alapján futtatnak. Ebben óriási lehetőségek és korlátok vannak. Korlát, hogy rendszeren kívüli adatforrást csak körültekintően lehet felhasználni, mert az okosszerződés futtatásának a sok ezer node mindegyikén ugyanazt az eredményt kell adnia. Az ilyen

külső adatforrások sokszor IoT eszközök, a további bizonyítás nélkül hitelesnek tekintett adatforrást pedig orákulumnak nevezzük. Az elkövetkező egy-másfél évtizedben az orákulumokra vonatkozó hitelességi és műszaki szabványok meg fognak születni.

Szervezet a láncban – decentralizált autonóm rendszerek

Az okosszerződések különleges fajtáját képezik a decentralizált autonóm szervezetek (DAOK). Ezek olyan okosszerződések, amelyeknek a programkódja a gazdálkodókhoz hasonló funkciókat valósít meg: letétet kezel, teljesítést igazol vagy vételárat fizet ki. Ha úgy hozzák létre, hogy senki ne legyen képes megváltoztatni a működését, akkor nem lehet addig leállítani (funkciói hívhatóak lesznek) ameddig a node-ok munkáját fedező „gáz”, azaz kriptoeszköz rendelkezésre áll. A decentralizált autonóm szervezeteket vagy akár cégeket (DAC-ok) a jövőben olyan tulajdonságokkal ruházhatják fel, hogy bizonyos események bekövetkezése indítson el folyamatokat. Ilyen esemény lehet az, ha a blokkláncban adott feltételek teljesülnek vagy akár az, ha egy orákulum ad valamilyen információt. Ilyenkor kérdés, hogy a kriptográfiai hitelesítést ki végezze el, mivel az okosszerződés a blokkláncban létezik, ahol viszont problémás lenne a titkos kulcs tárolása. Az elkövetkező évtizedben a problémára ki kell fejleszteni a biztonságos kriptográfiai sémát, például megfelelő többrésztvevős Threshold Signature Scheme megalkotásával.

Okosszerződések és a mesterséges intelligencia

Az okosszerződések akár rendszeren kívüli orákulumként, akár a blokkláncba integráltan mélytanulási módszerek által felismert összefüggéseket is felhasználhatnak paraméterként, illetve az ilyen modellek által kalkulált predikcióktól is függővé tehetik futásuk eredményét. Egy ilyen fejlesztés hihetetlen lehetőséget rejtene magában, ugyanakkor ehhez előbb fel kell oldani azt az ellentmondást, amely abban rejtezik, hogy a mélytanulási módszerek által alkotott modellek folyamatosan változnak az újabb és újabb tanított adatok feldolgozásával, ugyanakkor az okosszerződés egy-egy funkciójának pontosan ugyanazt az eredményt kell adnia az összes node-on futtatva, legalábbis egy adott blokk lezárása előtt. Az elkövetkező évtized bizonyosan megoldást hoz a kérdésben.

Okosszerződések és a tanútitkosítás (witness encryption)

Tegyük fel, hogy a Nagy-Fermat sejtésre (azóta tétel, mert több, mint 20 éve bebizonyították) a XIX. század közepén egy okosszerződésben letétbe helyezel egy 2 bitcoin-os díjat (tekintsünk el attól, hogy akkor még nem volt se elektronikus számítógép, se blokklánc), és kitalálsz egy olyan kriptográfiai rendszert, ahol a titkos kulcshoz akkor és csak akkor tudsz hozzájutni, hogy átutald magadnak a pénzt, ha ismered a bizonyítást, amiről akkor még azt sem tudod, hogy létezik-e. Ez a witness encryption. Ha sikerülne megkonstruálni, bizalom nélküli szerződéseket lehetne kötni. A kutatások jelenlegi állapota sajnos nem vetíti előre, hogy másfél évtizeden belül itt áttörés érhető el.

Átverés: blokkláncsal álcázott centralizáció

Az üzleti célú, zárt (permissioned) blokklánc rendszerekben a szereplők ismerik egymást és bíznak egymásban. Nyilvános kulcsukat megosztják egymással, így a Sybil-támadás ellen védettek. A blokkokat párhuzamosan állítják össze, de bányászat nincs. Többségi szavazás van, vagy egy kitüntetett szereplő dönt, ha erre szükség van. Ezek a zárt rendszerek jelentősen különböznek nyilvános társaiktól. Az első ilyen nagyméretű zárt rendszerű megoldás a kontinenseken átívelő ellátási láncok adatáramlását segítette. Az alapító globális szállítmányozó cég versenytársai egy idő után visszautasították, hogy saját adataikat feltöltsék, sőt azokat az ügyfeleket nem is szolgálták ki, akik használták a rendszert, mivel attól tartottak, hogy versenytársuk ellenük használhatja a blokkláncba feltöltött óriási mennyiségű adatot. A közösségi média vezető cégei esetében is felmerült például kriptovaluta kibocsátása, ahol a könyvelési platform akár nem decentralizált blokklánc rendszer is lehetett volna. Laikusként sokszor nehéz megítélni, hogy egy új blokklánc rendszer vagy egy okosszerződésen alapuló együttműködés valóban decentralizált-e. Az elkövetkező évtizedben várható a centralizáció jeleit kereső szolgáltatások felfutása.

Mesterséges Intelligencia – a harmincas években

GYIRES-TÓTH BÁLINT

BME, Távközlési és Médiainformatikai Tanszék*

A mesterséges intelligencia

A mesterséges intelligencia (MI vagy AI az angol *Artificial Intelligence* rövidítéséből) a számítástudománynak az az ága, amely intelligens viselkedésre képes informatikai rendszerek létrehozásával foglalkozik. Egy tágabb definíció szerint az MI olyan rendszereket vagy gépeket jelent, amelyek képesek a természetes intelligenciához hasonló kognitív funkciók elvégzésére, mint például a tanulás, a problémamegoldás, alkalmazkodás vagy a tervezés – miközben az ember által kezelhető adatoknál nagyságrendekkel nagyobb információmennyiséget képesek feldolgozni.

Napjainkban az MI-n belül a mélytanulás (*deep learning*) a domináns paradigma, amely jelentős áttörést hozott számos tudományterületen, például gépi látás, természetes nyelvfeldolgozás, beszédtechnológia vagy robotika.

Az MI rendszereket gyakran osztályozzák aszerint is, hogy milyen szintű intelligenciát céloznak meg. A szűk vagy gyenge MI (*narrow* vagy *weak AI*) egy konkrét feladatra specializálódik, míg az általános vagy erős MI (*general* vagy *strong AI*) az emberi intelligenciához hasonlóan széleskörű feladat megoldására és nagyfokú alkalmazkodásra képes. Az általános MI egyelőre első-sorban elméleti koncepció, a gyakorlatban használt MI rendszerek mind a szűk MI kategóriájába esnek – még ha néha igazán kreatív és akár öntudattal rendelkező megoldásnak is tűnnek.

Az MI rövid története

A mesterséges intelligencia fejlődése az 1950-es években kezdődött. Alan Turing felvetette a kérdést, hogy képesek lehetnek-e a gépek gondolkodni [1]. Pár évvel

később, az 1956-os *Dartmouth Summer Research Project on Artificial Intelligence* workshop során pedig már konkrét kutatási irányokat fogalmaztak meg [2]. Nem sokkal később megjelent a perceptron, az első olyan mesterséges neurális modell, amely képes volt tanulni [3] – azonban hamar rávilágítottak a perceptronok korlátaira is [4], ami jelentősen lassította az eljárás térnyerését. Az 1980-as években a backpropagation algoritmus létrehozása [5] új lendületet adott a neurális hálózatok kutatásának. Lehetővé vált a többrétegű hálózatok hatékony tanítása, ami utat nyitott az olyan összetettebb architektúráknak, mint például a konvolúciós [6] és a rekurens neurális hálózatok [7]. A 90-es években a neurális hálózatok ismét háttérbe szorultak az egyszerűbb, jobban értelmezhető – jellemzően szabály alapú, szakértői – módszerekkel szemben. 2012-ben az AlexNet [8], egy mély konvolúciós neurális hálózat jelentős fölénnyel nyerte az ImageNet képosztályozási versenyt, amely újra a neurális hálózatokat helyezte a gépi tanulással foglalkozó szakemberek figyelmének fókuszába. A következő években a mélytanulás alapú megoldások state-of-the-art eredményeket értek el számos tudományterületen (pl. beszédfelismerés [9], természetes nyelvfeldolgozás [10] vagy a játékok [11]). 2017-ben a transzformer architektúra [12] bevezetése és az önfelügyelt tanítás paradigma alkalmazása újabb áttörést hozott a természetes nyelvfeldolgozásban. A transzformer alapú neurális modellek, mint a BERT [13] vagy a GPT [14] architektúrák megdöntötték az addigi rekordokat szinte minden nyelvi feladaton. 2022 novemberében az OpenAI ChatGPT [15] megjelenése újabb mérföldkő volt: „Az MI iPhone pillanata” – ahogy Jensen Huang, az NVIDIA vezérigazgatója fogalmazott. A ChatGPT nyelvi modell szerteágazó témakörökben képes kérdésekre koherens, kontextusba illő válaszokat adni – legyen az akár mindennapi téma, jogi, egészségügyi vagy programozással kapcsolatos kérdés. Megjelenése élénk vitákat váltott ki az MI rendszerek képességeiről és potenciális hatásairól és veszélyeiről. A ChatGPT megjelenése óta számos további fizetős és nyílt nagy

* 2024. július 1-től névváltozással: BME, Távközlési és Mesterséges Intelligencia Tanszék

nyelvi modell jelent meg, ami az MI határait egyre jobban kitolja, és ezzel együtt egyre többen megismerik az MI paradigmát.

MI 2030

Óriási iramot diktál az MI fejlődése. Ezt többek között az is jól mutatja, hogy az MI-vel kapcsolatos legfontosabb napi híreket összegyűjtő hírlevél [16] átlagban 10...24 óra alatt elolvasható tartalmat foglal össze a szakmai közösségi média csatornákról – és ez a tudományos cikkeket és kapcsolódó forráskódokat nem, vagy csak részben tartalmazza. Ilyen hatalmas tempó mellett számos különböző jövőkép is felvázolható, most a nem túl távoli jövőben nagy valószínűséggel megvalósuló irányokra fókuszálunk.

Gyorsabb számítások és jobb skálázás

A hatékony mélytanulás alapú MI megoldásokhoz elengedhetetlenek a mátrixműveletek kiszámítására optimalizált hardver eszközök (pl. GPU és TPU). Ezek teljesítménye várhatóan tovább növekszik, skálázhatóságuk tovább javul. Ezáltal még nagyobb és összetettebb MI modellek létrehozása is lehetővé válik. A szerver infrastruktúra mellett a személyi számítógépek és a peremhálózati (edge) eszközök MI-specifikus teljesítménye is várhatóan tovább javul, ami széles körben teszi a modellek lokális futtatását lehetővé. A mélytanulás skálázási törvénye [17] azt mutatja, hogy a modellek méretének és a tanítóadatok mennyiségének növelésével a teljesítmény is javul, ráadásul a modell mérete és a teljesítmény közötti összefüggés szuperlineáris. Figyelembe véve ezeket a szempontokat, a jövőben egyre több, egyre nagyobb (több száz milliárd vagy billió paraméteres) modell megjelenése várható, melyek alkalmazási területe, teljesítménye és lehetőségei messze meg fogják haladni a maiakét.

Multimodális modellek térnyerése

Míg a korábbi és a jelenlegi MI modellek nagy része jellemzően egy modalitást kezel (pl. kép, mozgókép, szöveg vagy hang), néhány kereskedelmi forgalomban elérhető megoldás (pl. GPT-4, Claude 3) már most egyszerre nyújt kiemelkedő teljesítményt szöveges és vizuális adatokon. Ezáltal például természetes nyelven lehet egy képpel vagy egy scannelt dokumentummal kapcsolatos kérdéseket feltenni, és az MI a kért formában (pl. szabad szövegesen, JSON struktúrában) megadja a helyes választ. A jövőben várhatóan az olyan MI modellek terjednek el, amelyek több modalitást (pl. kép, szöveg, hang) együttesen képesek kezelni. Az eddigi tapasztalatok alapján a több modalitás együttes kezelése sokszor nemcsak

a modell lehetőségeit bővíti ki, hanem az egyes modalitások esetén elérhető pontosságot is tovább javítja. Ezáltal a multimodális modellek az MI rendszereknek mind a pontosságát, mind a robusztusságát és sokoldalúságát is növelni tudják.

Robotika reneszánsza

Az MI modellek, illetve a modelleket futtató kisméretű, beágyazott hardverek teljesítményének folyamatos fejlődése valószínűleg a robotikának is jelentős lendületet ad. Az elmúlt időszakban egyre több humanoid (pl. *Boston Robotics Atlas*, *Agility Robotics Digit*, *OpenAI Figure 01*, *Tesla Optimus*) vagy állatra emlékeztető (pl. a négylábú *Spot*) robotot hoztak létre. Napjainkra talán már minden robotvezérléshez és ember-gép interakcióhoz kapcsolódó terület – mint a gépi látás (képosztályozás, kép értelmezés, szemantikus szegmentáció stb.), a beszédtechnológia (beszédfelismerés, kulcszófelismerés, beszédgenerálás stb.), a természetes nyelvfeldolgozás (szövegértés, szöveggenerálás stb.) és a megerősítéses tanulás alapú vezérlés – elérte azt a kritikus szintet, ami alkalmassá tesz egy robotot a mindennapi használatra. Már csak idő kérdése, hogy a technológiák kombinálásával egy pénzügyileg megtérülő, az ipar és/vagy a nagyközönség számára a mindennapokban jól használható robot lásson napvilágot. Ezért a legmodernebb, és folyamatosan fejlődő MI technológiákra építve a korábbiaknál intelligensebb, sokoldalúbb, emberekkel jobban együttműködő robotok várhatóak. Részben ezt támogatja az MI világának egyik legmeghatározóbb vállalata, az NVIDIA által nemrég kiadott GR00T (*Generalist Robot 00 Technology*) mélytanulás alapú robotvezérlő és tanítható keretrendszer.

MI a mindennapi szoftverekben és eszközökben

A mesterséges intelligencia már napjainkban is egyre inkább hétköznapi szoftverkomponenssé válik – gondoljunk akár a gépi fordításra, keresésre, intelligens asszisztensekre, ajánlórendszerekre, vagy például a személyi számítógépen és az okostelefon futó különböző automatikus fotóretusáló megoldásokra. A felhasználói élmény javítása érdekében egyre több MI megoldás fog várhatóan a jövőben is beépülni a különböző alkalmazásokba, az okostelefontól kezdve a videójátékokon át az üzleti szoftverekig. Ezen túl az MI nemcsak szoftverekben, hanem a cél-, illetve mindennapi eszközökben is egyre hangsúlyosabban megjelenik. Várhatóan folyamatosan növekvő számú okos, MIvel támogatott eszköz vesz majd minket körül a hétköznapiakban, az okos otthoni asszisztensektől kezdve az önvezető autókban át az orvosi diagnosztikai berendezésekig.

Adatvezérelt vállalatok és közigazgatás

Ahogy a szervezetek vezetői az MI térnyerésével fokozatosan felismerik az adatokban rejlő értéket és az MI nyújtotta lehetőségeket, egyre inkább törekedni fognak arra, hogy adattudatos módon működjenek. Az összegyűjtött adatokra építve MI-alapú megoldásokkal automatizálhatják folyamataikat, optimalizálhatják működésüket, személyre szabhatják szolgáltatásaikat. Ezt a trendet támogatja az egyre könnyebben használható MI fejlesztőeszközök, valamint az MI mérnökök és fejlesztők folyamatosan növekvő száma. Ennek köszönhetően az üzleti és közigazgatási MI megoldások várhatóan egyre több új területen fognak megjelenni az elkövetkező években.

Epilógus

Természetesen a fentiek csak lehetséges forgatókönyvek, a mesterséges intelligencia tényleges fejlődési pályáját számos tényező befolyásolja a tudományos és technológiai kihívásoktól kezdve a szabályozási környezetig. Az azonban biztosnak tűnik, hogy a következő évtizedben az MI egyre nagyobb hatással lesz életünk szinte minden területére. Az sem kizárt, hogy olyan mértékben fogja átformálni a mindennapokat az MI technológia, ahogyan azt korábban az internet vagy az okostelefonok megjelenése tette. Izgalmas időszerzőnk!

Hivatkozások

- [1] Turing, A. M. (1950): "Computing machinery and intelligence", *Mind* 49, 433–460.
- [2] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (1955): "A proposal for the Dartmouth summer research project on artificial intelligence".
- [3] Rosenblatt, F. (1958): "The perceptron: A probabilistic model for information storage and organization in the brain". *Psychological Review*, 65(6), 386.
- [4] Minsky, M., & Papert, S. (1969): "Perceptrons: An Introduction to Computational Geometry". MIT Press.
- [5] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986): "Learning representations by back-propagating errors". *Nature*, 323(6088), 533–536.
- [6] LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998): "Gradient-based learning applied to document recognition". *Proceedings of the IEEE*, 86(11), 2278–2324.
- [7] Hochreiter, S., & Schmidhuber, J. (1997): "Long short-term memory". *Neural Computation*, 9(8), 1735–1780.
- [8] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012): "ImageNet classification with deep convolutional neural networks". *Advances in Neural Information Processing Systems*, 25.
- [9] Hinton, G., et al. (2012): "Deep neural networks for acoustic modeling in speech recognition". *IEEE Signal Processing Magazine*, 29(6), 82–97.
- [10] Collobert, R., & Weston, J. (2008): "A unified architecture for natural language processing: Deep neural networks with multitask learning". *Proceedings of the 25th International Conference on Machine Learning*, 160–167.
- [11] Silver, D., et al. (2016): "Mastering the game of Go with deep neural networks and tree search". *Nature*, 529(7587), 484–489.
- [12] Vaswani, A., et al. (2017): "Attention is all you need". 31st *Advances in Neural Information Processing Systems* 30 (NIPS 2017)
- [13] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018): "BERT: Pre-training of deep bidirectional transformers for language understanding". *arXiv preprint arXiv:1810.04805*.
- [14] Radford, A., et al. (2019): "Language models are unsupervised multitask learners". *OpenAI Blog*, 1(8), 9.
- [15] OpenAI. (2022): "Introducing ChatGPT". <https://openai.com/index/chatgpt/>
- [16] AI News, <https://buttondown.email/ainews>
- [17] Hestness, Joel, et al. (2017): "Deep learning scaling is predictable, empirically". *arXiv preprint arXiv:1712.00409*

Kiberbiztonság – helyzetkép és kitekintés a jövőre

BUTTYÁN LEVENTE

BME, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelen és jövő nagy vonalakban

Mára a kibertér mindennapi tevékenységünk színterévé vált, és függésünk az információs technológiáktól (azaz a számítógépes rendszerektől és az azokat összekötő hálózatoktól) kritikus mértékű. Sem a munkánkat, sem a magánéletünket nem tudjuk már elképzelni az internet és az azon keresztül elérhető szolgáltatások nélkül, és a fiatalabb generációkra ez még inkább igaz. Mindannyian tudjuk azonban, hogy ez a trend veszélyeket is jelent számunkra: informatikai rendszereink és az azok által kezelt adatok ki vannak téve a kibertér felől érkező támadásoknak. Rosszindulatú hekkerek próbálnak folyamatosan betörni rendszereinkbe, és ellopni vagy elérhetetlenné tenni adatainkat, hogy aztán eladják azokat vagy váltságdíjat követeljenek a visszaszolgáltatásukért.

A kiberbiztonság a fenti problémák megoldásával, enyhítésével foglalkozó terület. Egy informatikai rendszert biztonságosnak mondhatunk, ha az fel van készítve a kibertámadások elleni hatásos védekezésre és a rendszer üzemeltetője gondoskodik ennek a kellően védett állapotnak a folyamatos fenntartásáról is. A gyakorlati tapasztalat azt mutatja, hogy a biztonság elérése kihívásokkal teli feladat, és nem létezik tökéletesen védett rendszer. A nehézségek egyik forrása az, hogy – ellentétben azzal, amit maga a szó sugall – a kiberbiztonság megvalósítása nem kizárólag műszaki feladat. Ahogy azt Bruce Schneier, a terület egyik széles körben ismert szakembere megfogalmazta: „If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.” A kiberbiztonság eléréséhez, a hatásos műszaki megoldások mellett, jól átgondolt üzemeltetési szabályokra és eljárásokra, valamint fizikai védelmi módszerek és eszközök alkalmazására is szükség van. Arról sem szabad megfeledkezni, hogy egy informatikai rendszernek részét képezik a felhasználók és a rendszert üzemeltető személyzet is, így foglalkozni kell az ő képzésükkel, biztonság tudatosságuk és lojalitásuk

növelésével is. A nehézségek egy másik forrása, hogy e szerteágazó feladatokat egyenletes minőségben kell megoldani, a biztonság ugyanis olyan, mint egy lánc: a leggyengébb láncszem határozza meg az egész erősségét. Például hiába alkalmazzuk a legerősebb titkosítási eljárást, ha a felhasználóktól ki lehet csalni a titkos dekódoló kulcsot. Más megvilágításban: a támadónak elég egy kihasználható gyengeséget találni a rendszer védelmében, a rendszert üzemeltetőnek viszont minden nagy kockázatú fenyegetésre fel kell készülnie.

A fentiek tükrében nem csoda, hogy a kiberbiztonság, mint problémakör, évtizedek óta velünk van és a kérdést nem sikerült még „megoldanunk”. Sőt, egy kicsit pesszimistább hozzáállással azt is mondhatnánk, hogy a kiberbiztonság stagnál, azaz az elmúlt 2-3 évtizedben semmilyen átütő eredményt nem tudtunk felmutatni. Mintegy 20 évvel ezelőtt, 2006 februárjában, az MIT Technology Reviews folyóiratban megjelent egy írás „The Internet is broken” címmel [1], mely azt állította, hogy „az Internet alapvető hibái milliárdokba kerülnek a cégeknek, akadályozzák az innovációt és veszélyeztetik a nemzetbiztonságot.” Nos, ez ma sincs másként. A helyzet alapvetően nem javult: a kártékony programok (vírusok, férgek, trójaiak) nem tűntek el [2]; az informatikai rendszerekbe történő illetéktelen behatolás és az adatlopás mindennapos [3]; kritikus rendszereink ebben a pillanatban is éppen valamilyen elárasztásos (DDoS) támadás alatt állnak [4]. Mielőtt teljesen elszomorodnánk, érdemes persze mindezt perspektívába helyezni: jelenleg sokkal több informatikai rendszer működik és sokkal több adatot kezelünk, mint 20 évvel ezelőtt, és a sorozatos kibertámadások ellenére, a világ nagyjából mégis működik. Ez azonban csak annyit jelent, hogy a helyzet nem lett sokkal rosszabb sem, mint volt. A stagnálást jól illusztrálja, hogy míg a processzorok számítási kapacitása és a hálózatok sebessége több nagyságrenddel nőtt az elmúlt évtizedek során, és ennek következtében elképesztő új alkalmazások jelenhettek meg, addig a kiberbiztonság területén nem beszélhetünk ilyen mértékű javulásról vagy fejlődésről.

A múltból extrapolálva a jövő sem kecsegtet nagy reményekkel. A kiberbiztonság követi majd az aktuális technológiai trendeket és – az eddigiekhez hasonlóan – reagálni próbál a legfrissebb kihívásokra, legyenek azok a rendszerek jellemzőinek változásából származó kihívások vagy a támadási módszerek fejlődéséből származóak. Nem valószínű, hogy a kiberbiztonság ezen reaktív jellege megváltozna a jövőben. A nagyobb biztonság elérésének ugyanis magasabb a költsége, és ezt a plusz költséget csak akkor fizeti meg bárki, ha már nincs más választása. Azaz előbb az igény fog jelentkezni (pl. megnövekszik egy új fenyegetés kockázata), s ezt követi majd az arra adott válasz (pl. egy erősebb kódolási algoritmus kifejlesztése és bevezetése). Nem várható tehát olyan gyökeres fordulat, ami a kiberbiztonság problémakört teljes egészében megszünteti, vagy akár csak a főbb problématerületek valamelyikét eltüntetné. 15 év múlva is küzdeni fogunk még a kártékony programokkal, köztük a zsaroló vírusokkal, a gyenge jelszavakkal, az adatlopással, és a különböző típusú megtévesztéses támadásokkal. Feltéve, hogy lesznek még informatikai rendszereink...

Ha nagyon távolról nézve nem is fog jelentősen változni a kiberbiztonság képe a jövőben, közelebről tekintve a kiberbiztonság egy-egy részterületén minden bizonnyal tanúi leszünk innovatív új megoldások születésének. A teljesség igénye nélkül, a továbbiakban három olyan problématerületet mutatok be, ahol új kihívásokkal találkozunk és biztosan várható fejlődés a következő 15 évben.

Kiber-fizikai rendszerek kiberbiztonsága

A kiber-fizikai rendszerek folyamatos térhódításának vagyunk tanúi, és ez a trend várhatóan a jövőben is folytatódni fog. A kiber-fizikai rendszerek olyan rendszerek, melyekben beágyazott számítógépek felügyelnek és/vagy vezérelnek fizikai folyamatokat. Gondoljunk például egy modern autóra, amiben 40-50 beágyazott kontroller segíti a vezetést a jármű különböző részegységeinek (úgy, mint maga a motor, a kormány, a fékek, ...) felügyeletével. Hasonlóan, egy modern gyárban beágyazott számítógépek vezérlik a gyártósort, a futószalagokat és robotkarokat. Az élet minden területén egyre inkább megjelennek a beágyazott számítógépes rendszerek, melyek az eszközeinket és a környezetünket okosabbá, intelligensebbé teszik: okos otthonokban lakunk, intelligens közlekedési rendszereket használunk, okos városokban élünk majd. Ráadásul ezek a kiber-fizikai rendszerek ma már nem izoláltan működnek, hanem az internethez csatlakoznak és a „felhőbe” mentik az adataikat vagy azon keresztül nyújtanak különböző szolgáltatásokat.

Az előnyeik mellett, a kiber-fizikai rendszerek kiberbiztonsági kockázatokat is hordoznak: az őket alkotó beágyazott számítógépek hasonló módon megtámadhatók, mint a hagyományos számítógépek. Egyre erősödő trend például a beágyazott eszközök kártékony programmal történő fertőzése valamilyen hálózati kapcsolaton keresztül, majd a fertőzött eszközökből nagy méretű botnetek létrehozása [5], melyeket a támadók háttér infrastruktúráként használhatnak az interneten elérhető szolgáltatások támadása során [6]. A támadók dolgát speciális keresőmotorok segítik (pl. a Shodan [7] szolgáltatás), melyek internet kapcsolattal rendelkező, potenciálisan sérülékeny beágyazott eszközöket keresnek automatizált módon. A legnagyobb problémát – és egyben a legérdekesebb kihívást – azonban az jelenti, hogy a kiber-fizikai rendszereket ért kibertámadásoknak akár fizikai hatása is lehet! Ez jobb esetben csak anyagi károkat okoz majd (pl. tönkremegy egy robotkar egy gyárban), rosszabb esetben azonban környezetkárosító vagy akár emberéletet követelő baleset is vezethet (pl. egy kompromittált önvezető autó közúti balesetet okoz). Ezért az elkövetkezendő években, a kiberbiztonság egyik meghatározó alkalmazási területe a kiber-fizikai rendszerek védelme lesz.

Poszt-quantum kriptográfia

Egy másik erősödő trend a kvantumtechnológia fejlődése: kormányzatok és nagyvállalatok fektetnek dollármilliárdokat kellően nagy, a gyakorlatban is használható kvantumszámítógépek fejlesztésébe [8]. Az, hogy pontosan mire is lesznek jók ezek a számítógépek még nem teljesen világos, de egy alkalmazási terület biztosan nagy reményekkel kecsegtet: a gyakorlatban jelenleg használt publikus kulcsú kriptográfiai algoritmusok (pl. az RSA és az elliptikus görbe alapú kriptográfiai eljárások) feltörhetőek lesznek egy nagy, kriptográfiaileg releváns (azaz több tízezer kvantum-bites) kvantumszámítógép segítségével [9]. Bár egy ilyen kvantumszámítógép építése még több évtizedes kutatást és fejlesztést igényelhet, a problémával már most foglalkoznunk kell a „harvest now, decrypt later” támadások lehetősége miatt. Arról van szó, hogy bizonyos (pl. kormányzatok által támogatott) támadók folyamatosan, nagy mennyiségben rögzíthetnek számukra potenciálisan érdekes titkosított hálózati forgalmakat, és tárolhatják ezeket mindaddig, amíg rendelkezésre nem áll egy nagy kvantumszámítógép, amivel aztán feltörhetővé válik minden korábban rögzített titkosított forgalom [10].

Felmerülhet a kérdés, hogy egyáltalán lehetséges-e olyan új publikus kulcsú kriptográfiai algoritmust tervezni, ami ellenáll a kvantumtámadásoknak, vagy a kvan-

tumszámítógéppel minden jelenlegi és jövőbeli publikus kulcsú séma feltörhető? Szerencsére úgy tűnik, hogy a fenti kérdésre a válasz megnyugtató, azaz vannak olyan nehéz matematikai problémák, melyekre nem létezik polinom idejű megoldás sem hagyományos, sem kvantumszámítógépen [11], és ezek némelyikére építhető hagyományos számítógépen is futtatható publikus kulcsú titkosítás vagy digitális aláírás algoritmus. Az ilyen algoritmusok tervezésével és elemzésével foglalkozó területet nevezik „poszt-kvantum kriptográfiának”, és ez jelenleg a kriptográfia egyik legaktívabb területe. Most születnek azok az új ötletek, melyek a jövőbeli publikus kulcsú kriptográfiai algoritmusok alapjául szolgálnak. Az amerikai National Institute of Standards and Technology (NIST) már meg is kezdte az új poszt-kvantum sémák szabványosítási folyamatát [12]. A várakozás azonban az, hogy az átállás az új poszt-kvantum algoritmusokra még akár 10-12 évet is igénybe vehet, ezért a NIST 2035-öt tűzte ki a teljes poszt-kvantum átállás céldátumának. Ezalatt az idő alatt még sok minden történhet: jelenlegi jelölt algoritmusokról kiderülhet, hogy mégsem biztonságosak, új jelöltek léphetnek a szintérre, és akár még korábban néheznek vélt matematikai problémákról is kiderülhet, hogy mégsem olyan nehezek. A mérnököknek pedig óriási feladat lesz az új algoritmusok biztonságos integrálása a meglévő rendszerekbe, és egy olyan átmeneti időszak lehetővé tétele, melyben hibrid módon egyszerre fogunk hagyományos és poszt-kvantum kriptográfiát használni.

MI – a kétélű kard

S végül ebből a kitekintésből nem hagyhatjuk ki a Mesterséges Intelligencia (MI) potenciális hatásait a kiberbiztonságra. Ezen a területen az MI kétélű kardként jelenik meg: egyrészt a gépi tanulás és a legújabb generatív modellek segítségével hatásosabb biztonsági mechanizmusokat hozhatunk létre és hatékonyabbá válhat rendszereink biztonságos üzemeltetése; másrészt az új MI technikákat a támadók is sikerrel alkalmazhatják hatásosabb támadások kivitelezésére és rosszindulatú tevékenységük hatékonyságának fokozására.

Gépi tanulási modelleket már most is alkalmazunk kártékony programok és támadási mintázatok észlelésére, és a jövőben várhatóan egyre több feladatot oldunk meg ezekkel a modellekkel. Az MI segíteni fog a repetitív feladatok elvégzésében: a közeljövőben várhatóan MI-alapú asszisztensek segítik majd a biztonsági műveleti központokban ülő elemzők és a rendszerek penetrációs tesztelését végző szakemberek munkáját, míg egy kicsit távolabbi jövőben akár az is elképzelhető, hogy ezen feladatok megoldása nagy részben automatizálttá válik.

Ugyanakkor, a gépi tanulásnak megvannak a saját biztonsági problémái, mint például a tanító adatok szennyezése (poisoning) [13], kiskapuk (backdoor) elhelyezése [14], vagy az ellenséges minták (adversarial samples) lehetősége [15]. Ezek kihasználásával a támadók manipulálni tudják a gépi tanulási modellek viselkedését, predikciós képességeit. A generatív modelleknek szintén vannak biztonsági problémáik, például a jailbreaking [16] és a prompt injection [17]. Az elkövetkező évtizedek nagy kihívása lesz a robusztus MI technikák kifejlesztése, melyek a fenti – és más hasonló – támadásoknak ellenálló modelleket eredményeznek.

A támadó oldal is masszívan kihasználja majd az MI adta lehetőségeket. A generatív modellek nagyszerűen alkalmazhatók például a felhasználók megtévesztésében, kártékony programok fejlesztésében, és új támadási stratégiák kidolgozásában. Az MI segítségével a jövőben automatizálhatóvá válik majd a sérülékenységek keresése és kihasználása, és a támadók hatékonysága olyan mértékben növekedhet, hogy azzal már nem lehet lépést tartani, csakis valamilyen MI-vel támogatott védekezési módszer segítségével. Hogy ez a spirális út hova vezet majd, azt nehéz megjósolni.

Hivatkozások

- [1] <https://www.technologyreview.com/2006/02/15/229667/the-internet-is-broken/>
- [2] <https://www.ibm.com/blog/malware-history/>
- [3] <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- [4] <https://www.netscout.com/ddos-attack-map>
- [5] <https://iotsecurityfoundation.org/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/>
- [6] <https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/>
- [7] <https://www.shodan.io/>
- [8] <https://www.newyorker.com/magazine/2022/12/19/the-world-changing-race-to-develop-the-quantum-computer>
- [9] <https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography>
- [10] <https://techmonitor.ai/hardware/quantum/harvest-now-decrypt-later-cyberattack-quantum-computer>
- [11] <https://en.wikipedia.org/wiki/BQP>
- [12] <https://csrc.nist.gov/projects/post-quantum-cryptography>
- [13] <https://defence.ai/ai-security/data-poisoning-ml/>
- [14] <https://defence.ai/ai-security/backdoor-attacks-ml/>
- [15] <https://datascientest.com/en/adversarial-examples-definition-and-importance-in-machine-learning>
- [16] <https://www.techopedia.com/what-is-jailbreaking-in-ai-models-like-chatgpt>
- [17] <https://www.techtarget.com/searchsecurity/tip/Types-of-prompt-injection-attacks-and-how-they-work>

Infotáció, az információ-vonzás konceptiója

BARANYI PÉTER

Budapesti Corvinus Egyetem

Az elmúlt évtizedben az internetfejlesztés céljai nagyrészt megvalósultak, a megoldások megerősödtek. A legdinamikusabb fejlődés a digitális valóság technológiák (kiterjesztett, virtuális és kevert valóság, AR/VR/MR) és a mesterséges intelligencia (AI) terén történt. Az emberek és tárgyak internetét egyesítő Internet of Everything (IoE) koncepcióján túl az Internet of Digital & Cognitive Realities (IoD) már a kognitív entitások leg szélesebb körének hálózatba szervezését is magában foglalja, és tudatosan épít az AI-ra és az AR/VR/MR-re, integrálja azokat [1]. De mi lesz ezután, mi van a látóhatáron, milyen új fogalmak megjelenésére számíthatunk?

A következő 30-40 évben az infotáció koncepciójára és fogalomkörére irányuló figyelem várhatóan jelentősen felerősödik és tudományos tárgyalásmódja megszilárdul. Ahogy a gravitáció tömegvonzást jelent, úgy az infotáció az információk egymáshoz való vonzódását jelenti, azaz az információ mintázatok vonzzák egymást, statisztikus és sztochasztikus folyamatokban az együttes megjelenésük – időbeli, tartalmi vagy mintázati értelemben – erősödik, távolságuk csökken. Ez egy olyan természeti jelenség, ami megjelenik a mindennapjainkban, sokan érzékelik is és az események, történetek, valamint a gondolatok szinkronságában egyfajta, a világot folyamatosan konstruáló rendező-elvet vélnek érzékelni. Feltételezem, hogy az infotáció természetes manifesztációjában egyre inkább megjelenik majd a mesterséges / digitális információs rendszerek tartalma, és annak mesterségesen kialakult infotációs képességei összeolvadnak majd a természetes infotációval, hiszen lényegében az infotáció független az információ fizikai manifesztációjától. A mesterséges intelligencia információkezelési képessége is jelentősen hozzájárul majd az infotáció természetének megértéséhez, különösen akkor, amikor a 3D digitális/virtuális környezetek egyre elterjedtebb használatának hatására

a mesterséges intelligencia térbeli intelligenciája, azaz geometrikus értelmezési képessége megjelenik és tudása felhalmozódik. Mindezt tovább erősítik az Internet of Digital & Cognitive Realities (IoD) tudományos témában az internet kiterjesztésére irányuló kutatások, és előrevetítik azt a feltételezést, hogy valójában a természetnek is van egy "Internet of Natural & Cognitive Realities" szerű szerkezete. Ami miatt az IoD is hatékony mint modellezési eszköz. Az infotációról bővebben a [2] tanulmányban olvashatunk.

Az infotáció koncepciójának evolúciója

A Higgs-bozon jelenség [3] igazolja az energia csomósodások közötti vonzás létezését. A tömeg és az energia közötti egyértelmű kapcsolatot Einstein elméleteiből ismerjük. Ezzel összhangban, a tömegsűrűségek közötti vonzás – a gravitáció – is létezik, amint azt a Newtoni dinamika fogalmazza meg. Ugyanezen logika alapján következtetni lehet arra, hogy egyfajta vonzás létezik az információs mintázatok között – feltéve, ha elfogadjuk az energia és az információ mintázatok között van valamiféle megfeleltetés, ahogy az energia és a tömeg között van. Az információ és az energia közötti kapcsolatnak a létezését, mint modellezési eszközt, néhány tudományos területen nagy hatékonysággal alkalmazzák még akkor is, ha ez még mindig csak kismértékben képezi jelenlegi fizikai vizsgálataink tárgyát. Bizonyos korlátok között több tudományos megközelítés is elérte az információ határait, azonban egységes álláspont még nem alakult ki. Ez az oka, hogy az információ és a kapcsolódó jelenségek kutatása nem volt jelen a fizikában, hanem inkább külön jelent meg, és más kutatási területek módszertanára támaszkodott. Ez hasonló ahhoz, ahogyan nagyon gyakran előbb fedezünk fel fizi-

kai tényeket a matematikában, mielőtt azok jelenlétét a fizikában megvizsgálánk. Fontos hangsúlyozni, hogy a fizika jelenlegi fogalmai és az ott alkalmazott mérési módszerek nem biztos, hogy alkalmasak az információ vizsgálatára, és kérdéses, hogy az energia és az információ közötti kapcsolat kizárólag a fizika területéhez tartozik-e. Az is fontos kérdés, hogy melyik tudományterület a legalkalmasabb arra, hogy eldöntse, létezik-e az infotáció vagy sem. Lehet, hogy új nézőpontokkal és módszertani alapokkal rendelkező tudományterületre van szükség az információt irányító elvek felfedezéséhez, amelyben az infotáció létezése bizonyítható vagy megcáfолható lenne, és az energia és az információ közötti kapcsolat tisztázható lenne. Így feltehetően az infotáció koncepciója nem elsősorban a fizikában használt koncepciókra támaszkodik majd. Például az emberi agy a legbonyolultabb és legérzékenyebb „információfeldolgozási eszköz”, amely a rendelkezésünkre áll (hasonlóan néhány kutatási területhez – például a pszichológiában – ahol szinte egyedi „mérőeszközként” használható) és az infotáció vizsgálatára különösen alkalmas (lásd az Oxfordi Egyetem híres ikerkísérleteit). Így tehát valószínű, hogy annak igazolása, hogy milyen kapcsolat létezik az energia és információ között egy új tudományterület megjelenését igényli, amit mai szemmel előzetesen fizikai informatikának vagy infofizikának nevezhetünk, ami az energiasűrűsödések és térerők, valamint az információk és mintázatai között tár fel kapcsolatokat, kommunikációs képességeket. Érdeemes megemlíteni, hogy az infotáció fogalmára számos tudományterület magas rangú tudósai, köztük W. Pauli és C. G. Jung is *implicit* módon támaszkodtak. Ha az infotáció fogalma akkoriban létezett volna, fontos szerepet játszott volna a tudományos megközelítéseikben és kutatásaikban. Jung munkája demonstrálja, hogy az információs halmazok közötti tértől és időtől független kapcsolatokról, a tartalmuk hasonlósága alapján létrejött vonzásokról lehet tudományos tárgyalásmódban értekezni. Talán azt is mondhatjuk, hogy Pauli-Jung munkája és módszertani megközelítése jelentős mértékben támogatja az infotáció fogalmának meghatározását és felhasználását. Ennek alapján arra következtetésre is juthatunk, hogy ha az infotáció létezését csak hipotézisként is kezeljük ma, bevezetése a tudományos párbeszédbe új diszkurzust és holisztikus modellezési reformot indíthat el.

Az internet megjelenésével az információ szó fogalomköre és jelentése radikálisan megváltozott. A szabad és helyfüggetlen (felhőalapú) tudáshozzáférés révén képesek vagyunk egy mesterséges kollektív tudásra támaszkodni, amely kiterjeszti a korábban ismert pszichikai és társadalmi alapú kollektív tudás formáit. Ez jelentősen hozzájárult magának az „információ” szónak a közéleti

megjelenéséhez. Érdeemes belegondolni, hogy 1950-es években mennyire és hogyan használták az információ szót a hétköznapiakban, szemben a mai értelmezéssel és használattal. Kommunikációs alkalmazásaink (beleértve a Facebookot, a Twittert stb.) és hatásaik a társadalomra egyaránt radikális változáson mentek és mennek keresztül. Mindezek következményeként új kutatási módszerek jelentek meg, amelyek az információ terjedését, kölcsönhatásait valamint csomósodásait – ami egyfajta vonzásként is értelmezhető – például közösségi információs rendszerekre és hírforrásokra támaszkodva elemzik. A ChatGP és hasonló nagy nyelvi modellekre épülő mesterséges intelligencia rendszerek már érzékelhetővé teszik, hogy tartalmak közötti távolságot miként lehet értelmezni és ennek alapján közeli tartalmakat generálni. Ez önmagában már egy mesterségesen előállított egyfajta tartalmi vonzásnak is tekinthető.

Az infotáció koncepciójának evolúciójában fontos megjegyezni, hogy míg eredetileg a tömeg-energia-információ triádban a legnagyobb hangsúly a tömegre helyeződött, ma – különösen a Higgs-bozon jelenség miatt – az *energia egyre inkább vált egy központi fogalomká, amely „irányítja” a tömeget.* Következő évtizedekben, de *már ma is létező feltevés, hogy az információ és az energia vonatkozásában kiderül, hogy az információra „irányító” energiaként kell tekinteni,* azaz az információ irányítja az energiát, vagy az energia követ egyfajta információs mezőt. Ez a fajta megközelítés is konvergál a fentiekben említett információ vonzás jelenségéhez.

A következőkben két különböző tudományterületi háttérből teszünk egy kicsit részletesebb áttekintést.

Energia és információ a fizikában és a filozófiában

A Higgs-bozon jelenség kapcsolatát az infotáció fogalmával már a fentiekben említettük. Érdeemes Heisenberg híres állítására is utalni, miszerint matematikai formulákat lehet találni a materiális világ legmélyebb szintjén, ami az infotáció szempontjából úgy fogalmazható újra, hogy a részecskék viselkedését meghatározó elvek „információs mezőkön alapulnak”, és így „szükségessé válik” az információ fogalmát, talán egy teljesen új, információ alapú keretrendszer kontextusában értelmezni. Heisenberg nézőpontját monista és dualista szempontból is meg lehet fogalmazni.

A monista esetben az energia és az információ „kiegészítő” és oszthatatlan egységet alkotnak, és csak azért érdemes megkülönböztetni őket, hogy új nézőpontokat

hozzunk létre egy hatékonyabb vizsgálati forma megalkotására. Itt említhető de Broglie „rejtett paraméterek” hipotézise is – amit Pauli egyáltalán nem szerezett. Eddington részben támogatta ezt a felfogást, és a finomszerkezeti állandó reciprokát, a 137-et, központi „szervező” és „információs”, kozmikus, archetipikus számnak tekintette. A monista perspektívában a prioritás kérdése is fontossá válik: éppúgy, ahogyan a tömeget visszavezethetjük az energiára, az energia potenciálisan visszavezethető lehetne egy információs mezőhöz, folyamathoz vagy hálózathoz – amelynek kondenzációja, egy kritikus szint elérése után, átalakulhat olyan energiává, amely képes az információ megőrzésére is.

A modern matematikai rendszerelmélet szempontjából egy dualista, „interakcionista” nézőpont lenne megfelelőbb, amelyben az információs világ „különálló” a fizikai világtól, még akkor is, ha folyamatos kölcsönhatás lehetséges a kettő között. David Bohm „kvantumelmélete” közel állt az információ posztulálásához, de inkább egy monista kísérlet volt, amely a kauzalitás elvének köszönhetően nagy sikert ért el az 1950-es években, még a szovjet „filozófusok” körében is.

Energia és információ a mélylélektanban

Sigmund Freud úttörő volt abban, hogy az energia fogalmát a fizikából átvegye és a pszichológiai vizsgálatokban (pszichoanalízis) alkalmazza. Az energiának ezt a különleges formáját libidónak nevezte. Freudnál a libidó pánszexuális jelleget kapott, és a mitológiai összehasonlításokat tekintve Erószhoz hasonlította. Később, Sabina Spielrein hatására, a destruktív (halál) ösztönre vonatkozó fogalmat is bevezette és a mitológiai Thanatoszhoz kapcsolta. Ebben a pontban azonban a különböző típusú ösztönös kényszerhatások már nem alkottak „harmonikus” egészet Freud eredeti pszichikai energia fogalmával, a libidó koncepciójával. Freud egykori tanítványa, Jung a libidót az általános pszichikai energia státuszába emelte. Jung azt állította, hogy „az energiát átalakító pszichológiai mechanizmus a szimbólum (és nem a jel)”. Bár a szimbólumok Jung esetében az energián keresztül értelmeződnek, archetipikus (azaz komplex információs) mintákat tükröznek. Így a szimbólum fogalma a mai szóhasználatunkban elválaszthatatlan az információtól. Jung hasonlóan értelmezte az értékrendszer fogalmát is, amikor azt öss-

szekapcsolta a libidó különböző fokozataival (azaz a pszichikai energiához), amelyek a szubjektív értékelést eredményezik. Jung ezeket a kifejezéseket az archetipikus képek, formák világához, valamint a kialakult viselkedési mintákhoz és komplexumokhoz rendelte. Így az energia és az információ nemcsak a szimbólumok esetében alkotnak rendszerbeli egységet, hanem az értékrendszerek esetében is.

Míg az empirikus és „gyakorlatias” Jung néha inkább a viszonylag monista megközelítést részesítette előnyben, leggyakrabban a dualista interakcionista nézőpontot alkalmazta, például amikor az archetipikus alapokat és a pszichét komplex, önszabályozó rendszereknek írta le. Az 1950-es évekre már valószínűségi mezők és térképek segítségével írta le az archetipusokat, amelyekből az információ világa, amelyet bonyolult sztochasztikus folyamatok határoznak meg, csak egy lépés volt.

Összefoglalás

Mindezek alapján úgy vélem, hogy függetlenül attól, hogy az infotáció jelensége mérhető-e vagy bizonyítható-e, bevezetése – még ha csak egy absztrakt fogalomként vagy modellként is – logikailag értelmes megközelítés, amely gazdagabb és a következő 20-40 évben holisztikusabb koncepciókhoz vezethet különböző tudományterületeken. Ehhez jelentős segítséget adnak a mesterséges intelligenciában megjelenő, az információk tartalmainak „vonzását” leíró matematikai eszközök vizsgálata, valamint ha az információt egyfajta IoT mintára az kognitív valóságok „internetén”, vagy természetes „felhőjében” megjelenő helyfüggetlen jelenségként közelítjük.

Hivatkozások

- [1] Baranyi, P., Csapó, A., Budai, T., Wersényi Gy.: „Introducing the Concept of Internet of Digital Reality”. Acta Polytechnica Hungarica, Vol. 18. No.7. 2021, pp. 225–240. DOI: 10.12700/aph.18.7.2021.7.12
- [2] Baranyi, P. and P. Várlaki, P.: “Introducing the concept of infotation,” 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Győr, Hungary, 2015, pp. 647–654, DOI: 10.1109/CogInfoCom.2015.7390663.
- [3] https://en.wikipedia.org/wiki/Higgs_boson

Kell-e félnünk a jövőtől?

RAB ÁRPÁD

NKE, Információs Társadalom Kutatóintézet

A kultúra az emberiség túlélési stratégiája, az intelligencia és az együttműködés teszi az emberiséget sikeressé. Rendkívül izgalmas időkben élünk, döbbenetes sebességű és mélységű események, lehetőségek, kihívások zajlanak egyéni és társadalmi szinten is. Sosem volt még ennyi lehetőségünk, ennyi eszközünk, és sosem voltak még ekkora nagy kihívásaink sem, gondoljunk akár a fenntartható fejlődésre, életszínvonalunk megtartására, vagy a transzhumanizmus mindennapiainkat formáló erejére.

Nem kell félnünk a jövőtől, mert az emberiség előtt mindig álltak kihívások, ezeket megoldotta, a megoldás során újabb kihívásokat teremtett, aztán egy újabb kulturális-technológiai-gazdasági hullámban ezeket oldotta meg.

Azért nem kell félnünk a jövőtől, mert az előttünk álló kihívás látszik, a megoldás eszközkészlete és a szemléletváltozás, az üzleti modellek felsorakozása zajlik, és ha okosan viselkedünk, a megfelelő időben lezajlik. Megvan az eszköz-tárunk a kihívások megoldására, de ez nem azt jelenti, hogy megnyugodhatunk, csak azt, hogy el tudjuk végezni a munkát. Nem lesz könnyű.

Ehhez többek között az emberi és a mesterséges intelligenciát kell ötvöznünk, alapvető fogyasztói értékeinket kell átformálnunk, a látóhatáron túli események iránti felelősséget kell növelnünk. A digitális kultúra nem (csak) egy üzleti modell, egy múlt divat, hanem egy hosszú fejlődési folyamat fontos lépése, melynek igazán mélyreható változásai még előttünk állnak. Nem választási lehetőség, hanem alapvető túlélési stratégia, ami lehetővé teszi, hogy az emberiség sikerrel válaszoljon az előtte álló kihívásokra.

Mint faj, a technológiai evolúció segítségével jól vizsgálunk. Az elmúlt kétszáz évben megdupláztuk, sőt, lassan megtriplázzuk biológiai eredetileg kódolt élet-tartamunkat, az 1880-as évek életminőség-növelő technológiáinak (és a fogyasztói társadalom kialakulásának)

köszönhetően 250szeresére nőtt a gazdaságunk. Hosszabban élünk, egészségesebben, tisztábban; a Földön a mélyszegénységet sikerült leszorítani 84%-ról 14%-ra közel százötven év alatt (1880–2018 között). Annak eredményeképpen, hogy egyre kevesebb ember tudja megtermelni az élelmiszert egyre több embernek, a történelme során javarészt vidéki Föld elvárosiasodott, ma már az emberiség fele városokban lakik, 2050-re várhatóan a kétharmada fog. A városok gazdaságunk, kulturális életünk, innovációink gyújtópontjai. A faji siker a lélekszám gyarapodását is hozta, jelenleg nyolc milliárd ember él a Földön.

Az életminőségjavító gépek tömeges gyártása, illetve a fogyasztói társadalom előretörése megoldotta az akkori kihívásokat, és termelt újakat. Ezt a szemléletet alapvetően mennyiség alapú, erőforrás-tékozló megközelítés jellemzi. Ennek a folyamatnak számos következménye lett - az egyik az, hogy nagyon gyorsan nagyon sokan lettünk. Nem azért gyorsult fel a világ, mert technológiát használunk, hanem azért, mert gazdagok lettünk és sokan. A technológiákat azért fejlesztjük, hogy ezt a nagyon összetett új világot kezelni tudjuk. Nem egy véletlenszerűen létrejött technológiai-démoni felhőre reagálunk, hanem azokat az emberiség igényei hozzák létre, majd megméri megoldóértéküket, elhelyezi és okosan használja nagyon változatos érdektérképek mentén.

Hatékonytalan gépeket használunk, a megtermelt élelmiszerek jelentős részét elvesztegetjük, a megfelelő erőforrás felhasználása a megfelelő mértékben a megfelelő helyen korunk legnagyobb kihívása. Ezen túl kell lépni. Az előttünk álló legnagyobb kihívás az, hogy képessé válunk-e ilyen nagy népesség mellett, a környezetünket megkímélve, hatékony és együttműködő módon fejlődni. Egy együttműködő, tudatosabb, intelligensebb emberi fajra van szükség.

Ahhoz, hogy hatékonyan megőrizhessük életszínvonalunkat, egyrészt tudatos fejlesztésre, viselkedésre, illetve a széles tömegek együttműködésére van szükség. Az utóbbihoz pedig bizalom kell, ráadásul egyre inkább városiasodó környezetben, ahol az idegenektől

való félelem pont ezt a bizalmat bontja le. A digitális kultúra létrejött, az okostelefonok, szeretetgépeink és kényelmi szolgáltatásaink pontosan ezt a bizalmat teremtik meg.

Az, hogy ezek az eszközök ilyen gyorsan, nemtől, kortól, vallástól, földrajzi helyzettől függetlenül mindenkinek kellett, nem véletlen. A digitális kultúra ősi vágyainkat valósította meg. Segítségével technológiai úton, és – nem szellemi tökéletesedéssel, hosszú évek tanulással, de – elértük azt, hogy mindent tudhatunk, a világ összes nyelvén beszélhetünk, nem tévedünk el, tudunk olyanokkal élő kapcsolatot tartani, akik nincsenek is a közelünkben. Annyira szeretjük ezen eszközeinket, hogy ezeken keresztül idegenekkel is együtt tudunk működni, ráadásul az automatizáció segítségével akár nagyon rövid időtartamú együttműködések is lehetségesek, nem igényelnek szervezést, például egy idegen hazavisz minket az autójával, vagy kölcsönkapjuk a fűnyíró, a sharing economy, illetve a szívességbank működési modellek hatása drasztikus mértékben növekszik, és működésüket a digitális kultúra teszi lehetővé. Ez az, amiért létrejött. A digitális kultúra nem a fiatalok szórakoztató környezeteként jött létre, hanem a középkorú és az idősebb generációk megoldáskészletének bővítésére.

A digitális transzformáció a fenntartható fejlődés egyetlen útja, egyben a legnagyobb kihívása is. Elvárás, hogy a digitális transzformáció segítségével ennyi ember esetében is fenntartsuk az elért életszínvonalat úgy, hogy közben a környezet élhetőségét is biztosítjuk. Ez a lehetetlennek látszó kettős cél a technológia által segített automatizált együttműködésekkel, a társadalom intelligens adatalapú döntéseivel, és tudatosabb, önkorlátozottabb mindennapi viselkedésével kivitelezhető.

Az éghajlatváltozás és a digitális transzformáció kétségtelenül jelenkorunk két legmeghatározóbb jellemzője. Mindkettő hatalmas kihívást jelent, amely elképzelhetetlen következményekkel járhat az emberi fajra nézve, és nagy jutalmat ígér azoknak, akik megtalálják a módját annak, hogy hatékonyan kezeljék negatív következményeiket. Ezért nem meglepő, hogy a digitális átalakulás és a környezeti fenntarthatóság évek óta a gazdasági világ két legforróbb témája. A digitális transzformáció a fenntartható fejlődés egyetlen útja, egyben a legnagyobb kihívása is növekvő energiaigénye miatt. A két terület sikert pedig csak a társadalom újraprogramozásával és az üzleti modellek átírásával érhet el.

A legfőbb kihívásunk és elvárásunk az, hogy a digitális transzformáció segítségével ennyi ember esetében is fenntartsuk az elért életszínvonalat úgy, hogy közben a környezet élhetőségét is biztosítjuk. Ez az elsősre lehetetlennek látszó kettősség azonban a technológia által segített automatizált együttműködésekkel, az (ön) megfigyelő társadalom intelligens adatalapú döntéseivel, valamint tudatos és (ön)korlátozottabb mindennapi viselkedéssel kivitelezhető.

A digitális transzformáció 2040-re a digitális tér komplexebb megjelenési formáját és megoldóértékét hozza majd. A helyhiány, a környezeti negatív hatások, az élményalapú társadalom és a digitális kultúra újraprogramozása miatt növekvő mértékben élünk majd társadalmi életet egyre összetettebb virtuális világokban. Ezek első körben a környezet terhelésének csökkenését hozzák magukkal, például a logisztika, vagy a megtermelendő fizikai javak számának csökkenésével, működtetésük azonban párhuzamosan egyre növekvő környezeti terhelést jelent, amelyet okos fejlesztésekkel ellensúlyozhatunk.

2040-re mind a gazdaság, mind a társadalom sokkal tudatosabban, adatvezéreltebben, algoritmus-vezéreltebben fog élni. Ez a mindennapokban rengeteg automatizált korlátozást, figyelmeztetést, javaslatot jelent majd kényelmi szolgáltatásokkal, a töredezett idő, tér és cselekvés kihasználásával. Természetes lesz számunkra az önmegfigyelés, az intelligens technológiák használata és a digitális tér, mint kommunikációs, élmény-, munka- és társadalmi tér használata. Ezek segítségével a környezeti változás negatív folyamatai megállíthatók, illetve megélhetőbbek lesznek. Mindennapjainkat uralja majd a technológia, mind elrejtőzve, mind szem előtt, ez azonban nem félelem vagy korlátozás lesz számunkra, hanem a megszokott élet része.

Az automatizáció legelőször a munka világában fejti ki hatásait, egyre jobban tudatosul a társadalomban, hogy a robotok nem úgy „ölnek meg”, hogy lelőnek lézerfegyverekkel, vagy elveszik a munkánkat, hanem úgy, hogy elveszik a pénzünket, pontosabban értéktelenné teszik az ipari társadalom ellentételezési logikáit. A monotóniátűrés és a hosszú időn át tartó precíz koncentrált munkavégzés, mint munkaerőpiaci validátor, a mennyiségi alapú megközelítés, a viszonylag lassan reagáló ipari termelési és értékesítési láncok egy utánpótló és automatizált gépekkel teli, gyorsan változó világban megkérdőjelezi az addigi értékek mértékét és ellentételezését. Az automatizáció legfontosabb társadalmi hatása, hogy mind az egyéneket, mind a társadalmi alrendszereket szintlépésre kényszeríti egy magasabb tudatosság felé.

Rövid távú, már érzékelhető hatása, hogy fragmentálja a karrier világot, elősegíti az „azt amikor kell, és csak azt” atipikus munkaformákat, ami számos szabályozási kihívással jár együtt a töredezett munkaviszonyok kezelésétől kezdve a munkavállalók védelméen át egészen az azonnali automatikus szerződéseikig.

Ezért fejlesztettük ki a mesterséges intelligenciát (MI), mert ezekben jó. Hatékony gép segítségével elérhetjük, hogy a megfelelő helyen és időben a megfelelő mennyiségű, és nem több erőforrást használjunk fel. Képesé tesz arra, hogy idegenek egymással együttműködve megosszák erőforrásaikat. Segítségével bérelni tudjuk a tudást, így bárki szert tehet arra az összetett tudásra, amire abban a pillanatban szüksége van. Az nem kérdés, hogy a mesterséges intelligenciára az emberiségnek szüksége van, és használni is fogja. A következő évek nagy kérdése és kihívása, hogy mennyire okosan tesszük majd ezt.

Bár az MI-alapú rendszereknek csak kis részét alkotják a generatív szolgáltatások, és hosszú távon jó eséllyel nem is ezek formálják majd a jövőnket, a munkaerőpiacot és a társadalmat jelenleg leginkább ezek a szolgáltatások tartják lázban. Nap, mint nap tükörbe nézünk, megmérjük azokat az emberi cselekvéseket és értékeket, melyeket egyre hatékonyabban, ügyesebben utánoz az adatvezérelt algoritmuskörnyezet.

Azt, hogy milyen lesz a világunk 10-15 év múlva, mi formáljuk. A kihívás látszik, az eszköztár létrejött, az okos felhasználás rajtunk múlik. Bár 10-15 év soknak hangzik, a fizikai környezet (épületek, utak, hálózatos infrastruktúrák), a nagyobb értékű eszközeink (akár csak az autók) esetében azonban rövid, ha már ma léteznének is ezek letisztult formái, ennyi idő alatt akkor sem cserélődnek le. 10-15 év múlva viselkedésünk, értékkészletünk, döntéshozatali folyamataink, megoldási stratégiáink a maitól nagyon különbözni fognak a mindennapi, a gazdasági és a kulturális életben egyaránt. A mesterséges intelligencia szuperexponenciális növekedési lehetősége (ebben nem a processzorok száma, hanem az a lényeges, hogy az emberiség történetében először kapcsoltuk ki a tudástermelés területén a biológiai kódot) számtalan kutatási eredményt fog hozni például az orvostudomány, az életmeghosszabbító technológiák területén. A gyors kutatás-fejlesztést lassú üzleti modell változások és terjedés követi, még ha létre is jött a megoldás.

A klímaváltozás hatásait egyre inkább érezni fogjuk, a levegőminőségben, a szélsőséges időjárási körülmények növekvő számában, a nagyobb hidegben, a nagyobb melegben, a nem egyenletesen érkező vízutánpótlásban, az erőforrás láncok rövidülésében és változásában. Ezek azonban mind-mind az együttműködő, egyre okosabb, egyre hatékonyabban döntő emberiség felé terelik a jövőnket, és valószínűleg a megoldás során egy olyan új kihívás formálódik, ahol már az irracionális, az emberi megőrzése lesz a fő feladat a racionális, a gépi vezérlés és utánpótlás felett.

Összegzés, a trendek összefonódása, feladataink

BARTOLITS ISTVÁN

Nemzeti Média- és Hírközlési Hatóság

Hét előrejelzést olvashattunk az előzőekben az infokommunikáció egyes területeinek a jövőjére vonatkozóan és a szakértők szerint – amint azt többen is megfogalmazták – nagy bátorság volt a tizenöt éves előrejelzést felvállalni. Nyilván, az egyre gyorsuló technológiai fejlődés mellett is ez egy nehéz műfaj, de már régebben is annak számított. Erre utal a Nobel-díjas Niels Bohr mondása is: „Prediction is very difficult, especially about the future”, azaz „Az előrejelzés nagyon nehéz dolog, különösen, ha a jövőre vonatkozik”. Ugyanakkor teljesen természetes igény, hogy szakavatott, az illető szakterületet aktívan művelő szakemberek véleményére vagyunk a leginkább kíváncsiak a várható jövőt illetően.

A kétezres évek elején volt már egy igen alapos kísérlet a jövő felvázolására, amikor az NHIT (Nemzeti Hírközlési és Informatikai Tanács) égisze alatt Dömölki Bálint vezetésével elindult az IT3 (Információs Társadalom Technológiai Távlatai) projekt. A célja az volt, hogy a hírközlés és az informatika területén összesen 27 résztémában adjon 15 éves előrejelzéseket a várható fejlődésről. A 2005-2008 között a kutatásait végző projekt eredményét az „Égen-földön informatika” című vastkos kötetben tették közzé a szerzők [1], így a 15 éves előrejelzések határideje éppen tavaly járt le. Már akkor is nagy bátorság volt a projekt eredményeinek a publikálása, de a szerzők most legfeljebb mosolyogva veszik tudomásul a tévedéseiket vagy éppen örülnek a bevált előrejelzéseknek, de senkit nem ért negatív kritika az esetleges tévedések, melléfogások miatt.

Természetesen a most publikált előrejelzések nem ilyen részletesek és mélységűek, de az átfogó víziók mégis jól mutatják, hogy a nagyító alá vett területeken mi a fejlődés iránya, mi várható a jövőben a digitalizáció megatrendje mentén. Ez a széles, szinte mindent átha-

tó megatrend határozza meg az utóbbi évtizedekben az életünket – előbb észrevétlenül, majd egyre észrevehetőbben – és ennek a részeként fejlődnek a kiválasztott infokommunikációs részterületek is, tovább alakítva a digitalizáció megatrendjét.

Összegzés

Az infokommunikáció jövőjének a hálózati technológiák fejlődése adja meg a keretet, hiszen ezek a rendszerek adják a kommunikáció alapját. Összességében itt egyértelmű a fejlődés iránya, hiszen az egyre nagyobb mennyiségű információ mozgatása kikényszeríti a hálózatok fejlődését, azonban itt is vannak izgalmas kérdőjelek, ahogy az előrejelzésben olvashattuk.

A kvantumkommunikáció témája első pillanatra talán meglepőnek látszik, két okból is. Egyrészt a kvantumszámítógépeket gyakrabban emlegetik, azonban ezeknek a mindennapi igénybevétele még nagyon távolinak látszik. A kvantumkommunikáció vagy napjainkra már inkább kvantum-infokommunikáció, mint fogalom, kevésbé van jelen a köztudatban, de az előrejelzésből kiderül, hogy ennek alapvető szerepe van a jövő kommunikációjának biztonságossá tétele szempontjából, ráadásul a technológia is részint már rendelkezésre áll. Ezért került a kvantumkommunikáció témája a nagyító alá. Ráadásul lényeges is, hogy a kvantumkommunikáció egyes alkalmazásai hamarabb kerüljenek bevezetésre, mint a kvantumszámítógépek, mert addigra már át kell térnünk a biztonságos, kvantum alapú kulcselosztó rendszerekre az adataink titkosítása terén.

A blokklánc technológiát sokan még mindig a kriptopénzek világával azonosítják, azonban pontosan látni kell, hogy ez ugyan valóban a kriptopénzek kezelésé-

nek egy kifinomult eszköze, azonban a létjogosultsága ennél sokkal szélesebb körű, általánosabb. Ez a technológia az elosztott főkönyv – vagy ha jobban tetszik, akkor a kollektív nyilvántartás – különleges eszköze, mely komoly informatikai háttérre és komplex matematikai modellekre épül. Ezt a tulajdonságát használja fel a kriptopénzek világa is, hogy kiküszöbölje a központi nyilvántartást, azonban a blokklánc technológia más területeken is magas szinten képes a hitelesség és a meghamisíthatatlanság garantálására. Az előrejelzés jól mutatja, hogy itt még vannak nyitott, megoldatlan problémák, de már így is egyre több helyen alkalmazzák a blokklánc technológiát a beszállítói láncoktól kezdve a biztosításokon át egészen a közigazgatásig.

A mesterséges intelligencia témáját nem kell megindokolni, ez a több évtizede kutatott témakör – bár a legutóbbi időig csak a szűk szakma ismerte – berobbant a mindennapjainkba az elmúlt néhány évben, indokolt és indokolatlan félelmeket kiváltva a társadalomban. Azt azonban látni kell, hogy nincs visszaút, a mesterséges intelligencia be fog épülni az eszközeinkbe és rengeteg segítséget fog tudni nyújtani a jövőben az egyes embereknek és a társadalomnak egyaránt, csak megfelelő módon kell használnunk hihetetlen képességeit. Ezen a területen most annyira gyors a fejlődés, hogy itt valóban nehéz 10-15 évre előre látni, de éppen a félelmek eloszlátása, a veszélyek megelőzése miatt létkérdés a jövő víziójának a felvázolása.

A kiberbiztonság témája szükségszerűen szerepel az előrejelzések között, hiszen mindannyian érezzük – és sokan már tapasztalták is – hogy az adataink védelme egy igen fontos kérdés ebben az infokommunikációval átszőtt világban. Akár azt is mondhatjuk, hogy ezen áll vagy bukik, mennyire lesz élhető az egyre inkább digitalizálódó világunk. Az előrejelzésből kiderül, hogy ebben a véresen komoly rabló-pandúr játékban sosem lesz meg a megoldás, a komplex védelmi rendszerek legfeljebb enyhíteni tudják a problémákat. Persze ez is lényeges eredmény, hiszen tudjuk, a behatoló mindig a legkönnyebben támadható rendszereket keresi, mert ott tudja a legtöbb kárt tenni és a legtöbb információhoz hozzájutni. A jövőkép kiemelt pontjai, a kiber-fizikai rendszerek, a posztkvantum titkosítás és a mesterséges intelligencia sokat segíthet a jövőben a kiberbiztonság emelésében, de nem szabad elfelejteni, hogy a hackerek oldalán is rendelkezésre állnak ugyanezek az eszközök, tehát itt „örök fejlődésre” vagyunk ítélve.

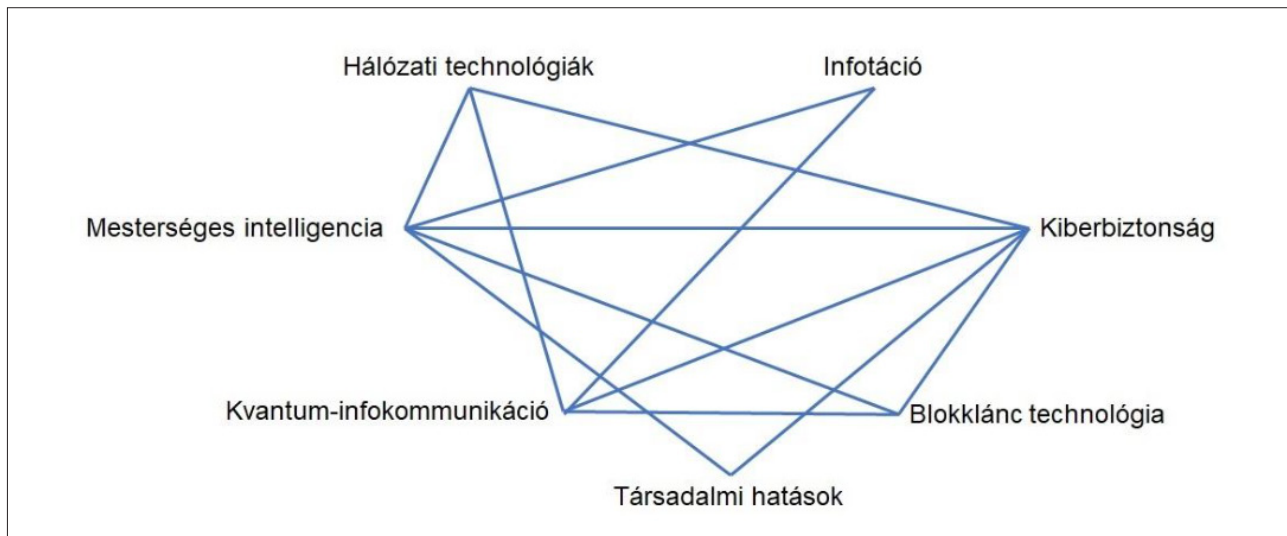
Különösen érdekes téma az előrejelzések között az infotáció, az információ-vonzás víziója, ahol bizony nehéz kapaszkodót találni egy összegzésben, hiszen maga a fogalom is meglehetősen futurisztikus.

Az azonban tény, hogy az információ mibenléte – mint látszólag anyagtalan entitás – nagyon sok kérdést vet fel, ugyanakkor keveset tudunk róla. Mi történik az információval, ha megsemmisítjük, mi lesz vele, ha beszippantja a fekete lyuk? Stephen Hawking eredeti feltételezése szerint a fekete lyuk teljesen megsemmisíti az információkat, a róla elnevezett Hawking-sugárzás teljesen független a fekete lyuk korábbi életétől, de ezt az elméletét később egy elvesztett fogadás keretében kénytelen volt megváltoztatni [2]. Vannak más elméletek is az információra vonatkozóan – mint pl. Vijay Balasubramanian paradoxona [3] – melyek szerint az információ teljes megsemmisülése ellentmond a kvantumrendszerek tulajdonságainak. Sokan a termodinamika és az információ jellege között vonnak párhuzamot, erre igyekeznek elméletet felépíteni. Ebben a sorban most új elméletnek tűnik az infotáció gondolata, ahol a gravitációs hatás mintájára lép fel az információ vonzása; izgalmas lenne, ha erre lehetne végül felépíteni egy új elméletet.

Az infokommunikáció fejlődésének, az elének táruló újabb és újabb lehetőségeknek természetesen társadalmi hatása is van és erről nem szabad elfelejtkezni a trendek előrejelzésénél sem. Ezért készült el a feldolgozott témák sorában hetedik anyagként a társadalmi hatásokat vizsgáló előrejelzés, aminek a fókuszában a most legtöbbször felmerülő kérdés áll: kell-e félnünk a jövőtől? A kérdés már nyilván sokszor felmerült a történelem során, de most – a technológiai fejlődés egyre gyorsuló szakaszában – még élesebben jelentkezik ez a félelem. Az előrejelzés mértéktartóan optimista, és felhívja a figyelmet arra, hogy ezért a pozitív kimenetelért még sokat kell tennünk.

A trendek összefonódása

Az elemzett trendek – bár nem fedik le az infokommunikáció minden részét – lényegében jól reprezentálják a jövő fejlődési irányát, mintegy kifeszítik a jövőt. A bemutatott víziók azonban nem függetlenek egymástól, fejlődésük együttesen fejt ki a hatását, ami további szinergikus lehetőségeket teremt az infokommunikáció egészének a fejlődése szempontjából. A trendek ilyen értelmű összefonódása már megjelenik egyes víziók elemzésében, így például a kvantumkommunikációnak szükségszerű összefonódása van a hálózatokra vonatkozó vízióval, a mesterséges intelligencia már szintén megjelent a hálózatokban, de a blokklánc technológiában is szerepe lesz, a kiberbiztonság pedig szinte mindegyik víziót érinti valamilyen szinten. A víziókban már kitapintható összefonódásokat legjobban egy ábrán szemléltethetjük.



2. ábra – Az infokommunikációs trendek kapcsolódásai

A 2. ábrából jól látható, hogy jelenleg a mesterséges intelligencia és a kiberbiztonság van kulcsszerepben, ami jól összevág a tapasztalatainkkal. Az összefonódás azonban további izgalmas fejleményeket hozhat és amikor pl. a mesterséges intelligencia és a kvantumkommunikáció – ebben az esetben már a kvantumszámítógép – trendje válik dominánssá és fonódik egybe; akkorra már egészen megjósolhatatlan dolgokra képes számítási és döntési kapacitás lesz a segítségünkre, feltételezve persze a pozitív társadalmi hatásokat. Ez a hatás vélhetően már a vizsgált 15 éves időszak után fog megjelenni és erősen egybeesik a Ray Kurzweil által előre jelzett technológiai szingularitás időpontjával. Ezt az időpontot a „Singularity is near” című, 2005-ben megjelent könyvében [4] 2045-re prognosztizálta. 2005 óta persze sok minden változott, de 2024-ben megjelentette a „Singularity is Nearer” könyvét [5], ahol következetesen fenntartja ezt a dátumot. Elképzelhető tehát, hogy éppen ezek az összefonódások hozzák meg a technológiai szingularitás időszakát, amikor a technológia fejlődése olyan gyorsá válik, amelyet az emberek már nem lesznek képesek felfogni, és megjósolhatatlanná válik a jövő.

Feladataink

Természetesen a jövő vízióinak a beteljesüléséhez még számos feladatot kell megoldani, ahogy arra a legtöbb előrejelzés is rávilágított. A technológiai fejlődés ugyan töretlen és ez jó alapot ad a célok eléréséhez, azonban a világ különböző régiói más-más módon vesznek részt ebben a folyamatban. Miközben tehát globálisan erőteljes a fejlődés, arra is figyelni kell, hogy ebben az

intenzív fejlődésben a tágabb és a szűkebb régiók milyen mértékig tud részt venni, mennyire tudjuk kiaknázni az infokommunikáció fejlődésében rejlő előnyöket. Sajnos Európa ebben a folyamatban lemaradóban van, világosan látszik, hogy egyes területeken – pl. a mesterséges intelligencia fejlesztése terén – az USA került vezető szerepbe, és egyre jobban zárkózik fel hozzá Kína, miközben Európa erőteljesen lemaradt. Több más területen is ez figyelhető meg, ami tendenciájában már veszélyezteti az európai életminőség megtartását is. Már is adódik tehát egy feladat, fel kell zárkóznunk az élvonalokhoz a jövő technológiái terén.

Ezt ismerte fel az Európai Unió, ezért jelentette meg a versenyképesség emelését célzó vitaanyagát 2024 februárjában, a „How to master Europe’s digital infrastructure needs?” című Fehér Könyvet [6]. A vitaanyag – sok más kérdés mellett – már felveti a legkorszerűbb technológiákban való előrelépés szükségességét és céljaiban jól illeszkedik a szakembereink által megfogalmazott víziókhoz. Lemaradást állapít meg olyan területeken, mint az 5G rendszer, az optikai hálózatok és a pereminformatikai infrastruktúra kiépítése, a kvantumkulcsszétosztó hálózatok, a mesterséges intelligencia és a LEO műholdas rendszerek fejlesztése. Erősíteni javasolja az 5G standalone rendszerek kiépítését, a 6G rendszer kutatás-fejlesztését, a hálózati konnektivitást, a tenger alatti kábelinfrastruktúra védeltségét, a felhőinfrastruktúrák és a pereminformatika fejlesztését, a kvantumkommunikáció kutatás-fejlesztését.

A vitaanyaghoz 2024. június 30-ig lehetett véleményeket küldeni és jól mutatja a vita szükségességét, hogy a megadott határidőig 357 vélemény érkezett a Fehér

Könyv felvetéseihez. A vitában a legtöbb vélemény vállalkozói szövetségektől (116), vállalatoktól (103), hatóságoktól és közigazgatási szervektől (32), civil szervezetektől (26) és egyetemektől (21) érkezett, de jöttek vélemények, hozzászólások uniós állampolgároktól és Európán kívüli területekről is. A vélemények feldolgozása és beépítése után van remény egy intenzívebb sebességű fejlődésre Európa részéről is, ez az első nagyobb lépés lehet a megoldandó feladatok terén.

Szűkebb környezetünket, Magyarországot tekintve ugyancsak komoly feladatok látszanak. Kiváló, magasan képzett szakembereink vannak, azonban ezeket a szakmai közösségeket helyzetbe kell hozni az európai vérkeringésbe való bekapcsolódással, mert ez tudást is hoz és bevételt is termel. Ezzel párhuzamosan meg kell kezdeni az Európához való felzárkózást több innovatív területen. Új irányba kell állítani és magasabb szintre kell hozni az oktatást egészen az alapoktól a posztgraduális képzésig. A lehető legtöbb olyan projektbe, nemzetközi munkamegosztásba be kell kapcsolódni, ahol tapasztalatot lehet nyerni és egyben hozzájárulhat a hazai értékteremtéshez.

Természetesen ezzel a folyamattal az Nemzeti Média- és Hírközlési Hatóságnak, az NMHH-nak, mint infokommunikációs szabályozó hatóságnak is együtt kell mozognia. A jelenlegi piac szabályozása mellett lényeges feladata az új technológiák azonosítása, elemzése és az ismeretek disszeminációja az NMHH-n belül és a hazai szakmában egyaránt. A teljesen új technológiák esetében lényeges a megfelelő szakembergárda kiképzése és/vagy felvétele ezek mélyebb megismerésére, a várható szabályozási kérdések azonosítására és megoldására. A folyamat eredményeként az NMHH egészének képesnek kell lennie az új technológiák, a hozzájuk tartozó üzleti modellek és innovatív szolgáltatások magas szintű kezelésére, ami sok esetben a korábbiaktól eltérő, teljesen új gondolkodásmódot igényel.

Végül, de nem utolsó sorban a HTE-nek is vannak, lesznek feladatai ebben a folyamatban. A 75 éves szervezet szakértő tagjaival, a felhalmozódott tapasztalatokkal és szervezőkészségével sokat tud segíteni az új technológiákkal kapcsolatos szaktudás szélesebb körben való terjesztésében, például innovatív konferenciák, nagyrendezvények megszervezésével, szakmai közösségein keresztül egyes részterületek ismereteinek elmélyítésével. Fontos szerepe lehet abban is, hogy az új technológiákkal kapcsolatos indokolatlan félelmeket eloszlassa, de ugyanakkor a valós veszélyekre felhívja a figyelmet. Független, szakértő szerepkörében meg tudja világítani a jövő fejlődésének az útját a következő időszakban, ahogy most ezekkel a víziókkal is tette. Ez ad alapot az Egyesület egészének arra, hogy a 75 éves évfordulón is bátran előre tekintsen a következő 75 évre.

Hivatkozások

- [1] Dömölki Bálint (szerk.): „Égen-Földön informatika – az információs társadalom technológiai távlatai”, TYPOTEX, 2008. ISBN: 978-963-2790-24-4
- [2] „Thorne – Hawking – Preskill bet”, Wikipedia; letöltve: 2024. augusztus 10. https://en.wikipedia.org/wiki/Thorne-Hawking-Preskill_bet
- [3] Vijay Balasubramanian, Bartłomiej Czech: „Quantitative approaches to information recovery from black holes”, Classical and Quantum Gravity, 2011. Vol. 28. Number 16. <https://arxiv.org/pdf/1102.3566>
- [4] Ray Kurzweil: „The Singularity is Near: When Humans Transcend Biology”; New York, Viking Books, 2005, ISBN 978-0-670-03384-3.
- [5] Ray Kurzweil: „The Singularity is Nearer: When we merged with AI”; Vintage Publishing, June 2024, ISBN 978-0-399-56276-1
- [6] European Commission: „White Paper – How to master Europe’s digital infrastructural needs?” 21 February 2024, <https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs>

A HTE-ről dióhéjban

A **Hírközlési és Informatikai Tudományos Egyesület** tekintélyes, 75 éves múltjával hazánk infokommunikációs szektorának legpatinásabb szervezetévé vált. Munkássága a távközlési és az informatikai iparágtól, a hagyományos postai szolgáltatásokon át, az internetig és a média-világig terjed. Az egyesület közel 70 jogi tagot, valamint több mint 700 magánszemélyt számlál. Berkein belül közel 20 szakmai közösség munkálkodik meghatározott célok érdekében, a legjobb tudása szerint.

A HTE mellett, hogy kiemelt, véleményformáló szerepet tölt be a magyar infokommunikációs szakterület szabályozásában, működésében, fejlődésében, hazai és nemzetközi szakmai rendezvények elismert szervezőjeként is jegyzett.

A HTE naptárában nem telik el hét szakmai találkozók, előadások, kerekasztal beszélgetések és egyéb szervezett események nélkül, de házigazdája többek között olyan **országos szakmai nagyrendezvényeknek**, mint

- a projektmenedzsment találkozóját és információcseréjét segítő **Projektmenedzsment Fórum**,
- a **HTE Infokom**, amely az infokommunikációs hálózatok és alkalmazások legfrissebb piaci, műszaki és szabályozási kérdéseinek egyik legelismertebb rendezvénye.

Az egyesület az utóbbi években számos **nemzetközi tudományos konferencia és workshop** magyarországi megvalósítását nyerte el pályázati úton, így öregbíthette hazánk szerepét a világ infokommunikációs szakmájában (bővebb információ a HTE nagyrendezvényeiről: <http://www.hte.hu/nagyrendezvények>).

Az egyesület szerteágazó kapcsolatrendszerének, valamint szakmai taglistájának (amely lefedi az infokommunikációs szektor szinte teljes területét) köszönhetően teret ad a különböző vélemény- és információcseréknek, professzionális párbeszédnek, közös cél érdekében folytatott kollektív munkásságnak. Lehetőséget biztosít arra, hogy az iparág valamennyi képviselője – akár a mindennapi konkurálást is háttérbe szorítva – kommunikáljon fontos kérdéskörökben, kifejtse a jelen nehézségeit illetve jövőbeli elképzeléseit. Mindeközben az egyének szakmai kiemelkedésének, véleményformálásának is utat enged.

A HTE megkérdőjelezhetetlen erőssége, és így több évtizedes elismertségének egyik alapja, hogy mind munkásságában, mind véleményformálásában **szakszerű, kiegyensúlyozott és független**, felülemelkedik az esetleges politikai vagy éppen vállalati érdekeken.

Bő hét évtizedet és két tucat szakterületet pár mondatban összefoglalni szinte lehetetlen lenne, ezért inkább vázlatpontokban szemléltetjük, mi minden érinti manapság a **HTE tevékenységi körét**:

- hazai és nemzetközi konferenciák szervezése, lebonyolítása
- szakmai fórumok az internet technológiák és szolgáltatások elterjesztéséhez
- műsorelosztási és tartalomipari technológiák népszerűsítése
- rádiótávközlési technológiák ismeretterjesztése
- projektmenedzsment módszerek terjesztése
- szakmai folyóiratok, nyomtatványok kiadása
- nemzetközi kapcsolatok: együttműködés az IEEE-vel és más társszervezetekkel
- szakmai díjak odaítélése (pl. Puskás Tivadar-díj, Kempelen Farkas-díj, Pollák Virág-díj, HTE Fekete László-díj)
- kiegyensúlyozott szakmapolitikai, szakmai véleményalkotás (minisztériumok felkéréseire és társadalmi egyeztetésekben)
- főiskolák és egyetemek képzési és kimeneti követelmények véleményezése
- külföldi infokommunikációs eredmények honosításának segítése
- kutatásfejlesztési tevékenység támogatása

A HTE ars poeticájában tradicionálisan hangsúlyos szerepet kap a fiatalokkal való kapcsolat ápolása, **a szakmailag széles látókörű és tudományos érdeklődéssel bíró diákok tanulásának és pályaindításának segítése** – hiszen ők alkotják majd a jövő szakembereit. Az egyesület mellett, hogy az arra érdemes hallgatóknak biztosítja a különböző rendezvényeken, konferenciákon, fórumokon való kedvezményes részvételt, és ezáltal a szakmai kapcsolatépítést is, különböző pályázatokat hirdet, amelyek díjazottai anyagi elismerésben is részesülnek. A HTE Diplomaterv és Szakdolgozat Pályázatára például az ország 15 egyeteméről nevezhetnek.

A HTE időszakos kiadványai mellett hagyományosan két folyóiratot jegyez: a **Híradástechnikát** és az **Infocommunications Journalt**. Míg előbbi a hazai szakmai élet történéseit, kérdéseit és működését elemzi, az Infocommunications Journal már nemzetközi elismertségre is szert tett, olyan nemzetközi adatbázisokban szerepelve, mint a Scopus, a Compendex és az Inspec. A lap kiadását a Nemzeti Média és Hírközlési Hatóság támogatja, szerkesztősege folyamatosan szervez keresztpublikációkat nemzetközi társlapokkal.

További információk:

www.hte.hu,
kérdéseit, észrevételeit pedig
az info@hte.hu
címmre várjuk!



