Az 5G-hálózat és a közlekedés információbiztonsági kihívásai

BÓDI ANTAL, MAROS DÓRA
KTI Közlekedéstudományi Intézet Nonprofit Kft.
bodi.antal@kti.hu, maros.dora@kvk.uni-obuda.hu

Kulcsszavak: Európai Adatstratégia, mobilitási adattér, 5G, Trust Space, ITS-ökoszisztéma

A közös európai mobilitási adattér tudatos kialakítása alapvető infrastrukturális és kiberbiztonsági kérdéseket vet fel. Magyarország ebben a folyamatban vezető szerepet tölthet be, amennyiben innovatívan és kreatívan hasznosítjuk az eddig elért eredményeinket az intelligens közlekedési rendszerek kifejlesztésében – beleértve a hálózatba kapcsolt autókat és más innovatív közlekedési megoldásokat is. A jövő közlekedése szempontjából elengedhetetlen a legújabb távközlés- és informatika-technológiai fejlesztések felhasználása, beleértve az 5G-hálózat kialakulását és a mesterséges intelligencia alkalmazásszintű elterjedését. Ez az adattér meg fogja könnyíteni a meglévő és jövőbeli közlekedési és mobilitási adatbázisokból származó adatokhoz való kontrollált hozzáférést, azok összevonását, megosztását és közhiteles tanúsíthatóságát, kapcsolódva az ENISA által meghatározás alatt levő kiberbiztonsági keretrendszerhez és a NIST által kialakítás alatt levő „Zero Trust Architecture" elvekhez. Ezen felhasználási igény kielégítése pedig elvezethet a Trust Space adattér-absztrakció megvalósulásához.

1. Bevezetés

A közlekedésben jelentkező lehetőségek és kihívások megkövetelik a kiterjedt digitalizáció lehetőségét. Létrejönnek olyan intelligens közlekedési rendszerek (ITS, Intelligent Transport System), amelyek megteremtik annak lehetőségét, hogy az általuk előállított és kezelt adatokra épülve kialakuljon a közlekedési adatok felhasználásával a mobilitási adattér. A lehetőségek kiaknázása azonban jelentős kockázatot is hordoz magában, mivel az ITS kialakítása során olyan IT-rendszereket vagyunk kénytelenek használni, amelyek jelenleg jelentős kitettséget és kiberfizikai kockázatot jelentenek. Azzal, hogy adatvezérelt hálózati rendszerek közvetlen emberi kontroll nélkül képesek legyenek a közlekedésben meghatározó szerepet játszani, nagyon komoly kihívást jelentenek a jogalkotás és jogértelmezés számára a felelősség meghatározásában és a jogkövető magatartás kikényszerítésében. A kiterjedt digitalizáció eredményeként sok eddigi, közlekedést érintő jogszabályt újra kell értelmezni a kor elvárásainak megfelelően, összhangban az EU-szintű szabályozásokkal.

A technológiai fejlődés olyan új lehetőségeket ad a kezünkbe, amelyek segítségével képesek leszünk a kialakuló helyzetet kezelni és a kockázatokat megszüntetni vagy legalább jelentősen mérsékelni. A legfontosabb, hogy ne különálló szigetszerű alkalmazásokban gondolkozzunk, hanem az egész ökoszisztémát próbáljuk meghatározni, amely hosszútávon képes lesz kezelni a folyamatosan változó és fejlődő környezeti hatásokat. A Közlekedéstudományi Intézet a több éve elkezdett kutatás és fejlesztés eredményeként meghatározó szerepet játszik az intelligens közlekedési rendszerek kifejlesztésében és az ehhez kapcsolódó biztonságos adattér létrehozásában.

Alapvető elvárás, hogy a közlekedésbiztonság jelentősen megnövekedjen. Általános tapasztalat, hogy egy részterületen végbemenő digitalizáció törvényszerűen megteremti annak a pontos és gyors elszámoltathatóságát, és visszahat a részterületre vagy akár az egész területre. Itt például elegendő arra gondolni, hogy a Magyarországon kiépült VÉDA Közúti Intelligens Kamerahálózat rendszer hatásaként ma már az autópályákon jelentősen visszaszorulóban van a gyorshajtás, és az előírt sebesség betartása többnyire beépült a tudatos közlekedési viselkedési normák közé. A közlekedés kiterjedt digitalizációjának folyamata törvényszerűen együtt fog járni a közlekedés hatékonyságának és az információk mennyiségének növekedésével is. Ezzel a technológiai fejlődés fő sodrában kialakuló legújabb lehetőségek felhasználásával számolunk. Az egyik fontos feltétel az úthálózat egészén elérhető 5G-hálózati lefedettség kialakítása és annak, különösen a közlekedésre kifejtett hatásainak kérdései, amelyek jelentősen befolyásolhatják Magyarország fejlődését az elkövetkező években.

A járművek és az egész közlekedési tér közötti kommunikációhoz, az adatfeldolgozáshoz és a nagy tömegű adattal való közlekedésirányításhoz a mesterséges intelligenciát hívjuk segítségül, ahogy erre már nemzetközi példákat és működő pilot rendszereket lehet találni. Jó példa erre a 8,5 millió lakosú Csingtao (Kína), ahol a forgalmat 900 ezer okos kamera figyeli folyamatosan és a képek feldolgozásával komplex városirányítási rendszer jött létre *(1. ábra)*.

Az e-Mobilitás célja a fosszilis energiahordozóval működő gépjárművek elektromos meghajtással való kiváltása. Ebből a szempontból is az egyik legfontosabb tényező, hogy minden időpillanatban pontos információval rendelkezzünk a járműről. Az önvezető rendszerek

1. ábra
A Csingtao-i városirányítási rendszer modellkörnyezete (Bódi Antal saját felvétele, 2019. november 1.)

elterjedése sem jöhet létre a digitalizáció nélkül, akár a kötöttpályás, akár nem kötöttpályás közlekedésről van szó.

Általános probléma, hogy miként tud majd a közlekedésben kialakulni biztonságosan az az átmeneti állapot, amikor a hagyományos járműveknek és az önvezető járműveknek egy adott közös közlekedési térben kell tudniuk biztonságosan közlekedni. További kihívásként jelennek meg új innovatív közlekedési formák, mint például a drónok. Elegendő csak arra gondolni, amikor egy drón megzavarhatja a légikikötők forgalmát, vagy zavarokat okozhat a közúti- vagy a vasúti közlekedésben.

A közlekedés digitalizációja további lehetőséget adhat a környezeti terhelés csökkentésének optimalizálására, és ezáltal hatékonyabbá tehető a közlekedési környezet, amely komoly környezetvédelmi elvárásokat és jelentős klímavédelmi kérdéseket vet fel.

2. Európai Adatstratégia[1], mobilitási adattér

Az Európai Adatstratégia fogalmazza meg, hogy a 21. századi innovatív átalakulás középpontjában az adatok állnak. Az adatgyűjtés és az adatok felhasználásának módja tekintetében elsősorban az egyén érdekeit kell előtérbe helyezni, összhangban az európai értékekkel, az alapvető jogokkal és a szabályokkal. Az EU-ban az állampolgárok csak akkor fognak megbízni az adatvezérelt innovációban és csak akkor fogadják el azt, ha meggyőződhetnek arról, hogy az adatok megosztása során maradéktalanul érvényesülnek a szigorú uniós adatvédelmi szabályok (GDPR).

A közös európai mobilitási adattér tudatos és tervszerű kialakításánál szem előtt kell tartani azt a célt, hogy a közös európai intelligens közlekedési rendszer kifejlesztésében – beleértve a hálózatba kapcsolt autókat és más közlekedési módokat is –, olyan adattér jöjjön létre, amely meg fogja könnyíteni a meglévő és jövőbeli közlekedési és mobilitási adatbázisokból származó adatokhoz való hozzáférést, azok összevonását és megosztását.

Napjainkban a korszerű gépjárművek jellemzően óránként mintegy 25 gigabájtnyi adatot generálnak, az önvezető autók pedig több terabájtnyi adatot fognak előállítani, amelyeket a mobilitással kapcsolatos innovatív szolgáltatásokhoz, valamint a javítási és karbantartási szolgáltatásokhoz lehet majd felhasználni. Az innovatív alkalmazások működéséhez szükség van a gépjárművek adatainak biztonságosan, jól szervezetten és a szabályokkal összhangban történő megosztására számos különböző szereplő között. A járművek fedélzeti adataihoz való hozzáférést az uniós jármű-jóváhagyási jogszabályok már 2007 óta szabályozzák, annak érdekében, hogy a független javítóműhelyek számára méltányos és kielégítő hozzáférést biztosítsanak bizonyos gépjármű-adatokhoz. Elkerülhetetlen lesz a területet érintő jogszabályok folyamatos frissítése annak érdekében, hogy figyelembe vegye az összekapcsolt rendszerek terjedését, vagy akár a konfliktusmentes átalakulás szükségességét.

A távközlésben gyors fejlődésnek lehetünk szemtanúi, amely a távdiagnosztikai és felügyeleti rendszerek számára egyre biztonságosabb és egyre nagyobb kapacitást képes biztosítani. Az 5G-rendszerek[2] kialakítása már megkezdődött, és több országban már a 6G[3] rendszerek kísérleti fejlesztése is folyik. A távközlési fejlődés és a biztonságos szoftverrendszerek fogják biztosítani az adatokat generáló gépjárműtulajdonosok jogainak és érdekeinek tiszteletben tartását, valamint az adatvédelmi szabályok betartását.

3. Az EU Bizottság kezdeményezései

Az Európai Adatstratégián belül a mobilitási adattér létrejöttéhez a Bizottság felülvizsgálja a gépjárművekre vonatkozó hatályos uniós típusjóváhagyási jogszabályokat azzal a céllal, hogy azok hatálya több, a gépjármű-adatokon alapuló szolgáltatásra is kiterjedjenek. Ennek várható határideje 2021. első negyedéve. A felülvizsgálat keretében többek között arra keresik a választ, hogy a gépjárműgyártók miként tegyék hozzáférhetővé az adatokat, valamint milyen eljárások szükségesek ahhoz, hogy az ilyen adatok lehívása az adatvédelmi szabályok, a gépjárműtulajdonosok, valamint a gépjárművezetők jogainak maradéktalan tiszteletben tartása mellett történjen.

2021-ben fogják felülvizsgálni az intelligens közlekedési rendszerekről szóló irányelvet is és az ahhoz kapcsolódó felhatalmazáson alapuló rendeleteket. Az ITS-adatok rendelkezésre állásának, újrafelhasználásának és interoperabilitásának további elősegítésére erősebb

1 COM(2020) 66: European strategy for data
2 https://www.visualcapitalist.com/visualizing-the-state-of-5g-networks-worldwide/ (2021.01.30.)
3 https://www.oulu.fi/6gflagship/ (2021.01.30.)

koordinációs mechanizmust hoznak létre. Az egész EU-ra kiterjedő CEF-program támogatásával és keretében egyesítésre és egységesítésre kerülnek az ITS-irányelv alapján már korábban létrehozott nemzeti hozzáférési pontok (NHP-k).

2020-ban módosították az egységes európai égboltról szóló rendeletre irányuló javaslatot, amely új rendelkezésekkel lett kibővítve az adatok rendelkezésre állására és az adatszolgáltatók piaci hozzáférésére vonatkozóan. Ez előmozdítja a légiforgalmi szolgáltatás digitalizálását és automatizálását 2021-től. Ennek köszönhetően javulni fog a légi közlekedés biztonsága, hatékonysága és kapacitása. Nemzeti szinten kiadásra kerültek például a drónok működését szabályzó rendeletek.

Ugyanígy felülvizsgálják a vasúti közlekedés területén alkalmazott interoperábilis adatmegosztásra vonatkozó szabályozási kereteteket 2022-ig.

Az elektronikus áruszállítási információkról szóló rendeletekben kerülnek szabályozásra (2022 végéig) az előírt közös adatkészletek a vállalkozások és a közigazgatási szervek közötti digitális adatcserére, az adatok újra felhasználására és az adatok másodlagos felhasználásának megkönnyítésére.

4. Kiberbiztonsági tanúsítás közlekedési vonatkozása

Az EU Bizottság felismerte, hogy az informatikai kitettség kezelésének fokozott figyelmet kell szentelni. A 2019/881 rendelettel megbízta az ENISA-t (az Európai Uniós Kiberbiztonsági Ügynökséget), hogy dolgozza ki az információs és kommunikációs technológiák kiberbiztonsági tanúsítását, mivel a hálózati és információs rendszerek és a távközlési hálózatok és szolgáltatások létfontosságú szerepet töltenek be a társadalom működésében, és a gazdasági növekedés gerincét képezik. Ez az irányelv a 2025. június 28. után a fogyasztóknak nyújtott, alábbi szolgáltatásokra lesz majd alkalmazandó a közlekedés vonatkozásában.

A légi, az autóbuszos, a vasúti és a vízi személyszállítási szolgáltatások következő elemei:

– honlapok;
– mobileszköz-alapú szolgáltatások, ideértve a mobilalkalmazásokat is;
– elektronikus menetjegyek és elektronikus menetjegy-értékesítési szolgáltatások, a személyszállítási szolgáltatásokkal kapcsolatos tájékoztatásnyújtás;
– a valós idejű utazási információkat is beleértve; ez az információs képernyők tekintetében az EU területén található interaktív képernyőkre korlátozódik;
– az EU területén található interaktív önkiszolgáló terminálok, kivéve a járművek, a repülőgépek, a hajók és a vasúti járművek szerves részeként beépített, az említett személyszállítási szolgáltatások bármely részének nyújtásához használt ilyen terminálokat.

A fenti felsorolásból kitűnik, hogy itt nem találkozunk sem adatstratégiával, sem a mobilitási adattér fogalmával. Ennek a kialakítására adott határidő sokkal később fogja követni a korábbi intézkedéseket, amelyek valóban a mobilitási adattér kialakíthatóságához kapcsolódnak.

5. A legfontosabb rendeletek

A GDPR, az EU 2016/679 rendelete, a természetes személyek személyes adatainak kezeléséről és azok védelméről szól. Ezt tekintjük az általános adatvédelmi rendeletnek. Ez az európai jogintézmény, amely nem csak az EU-tagországok állampolgárainak, hanem az egész világ számára meghatározó mintaként szolgált az adatvédelem fontosságát illetően.

Az eIDAS, az elektronikus azonosítási és bizalmi szolgáltatásokról szóló 910/2014/EU rendelet egy szabványosítási előírás, amely minden EU-tagországra vonatkozik, amely konzisztens jogi kereteket biztosít az elektronikus azonosítók és aláírások elfogadására. Az eIDAS digitális pecséteket is bevezet az üzleti egységek számára, és ezekkel válik lehetővé az európai szervezetek számára az üzleti folyamataik teljes körű digitalizálása. Azonban ennek bevezetését nem sikerült minden tagországnak egyenlő szinten teljesíteni. Magyarország élen jár ezen a területen, mivel az e-személyi igazolványunk eIDAS-konform eszköz és már a magyar lakosság körében 50% körüli elterjedtséggel rendelkezik.

A NIS-direktíva az EU 2016/1148 irányelve, amely a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedések kidolgozását irányozza elő. Igazodva a technológiai fejlődéshez, ennek is megkezdődött az átdolgozása. Az új NIS2 irányelvtervezet főbb szempontjai a következők:

- a jelenlegi irányelv hatályának jelentős kiterjesztése új szektorok hozzáadásával, mint például a távközlés, a közösségi média platformjai és a közigazgatás;
- annak megállapítása, hogy a NIS2-keretrendszer hatálya alá tartozó ágazatokban tevékenykedő összes közép- és nagyvállalkozásnak automatikusan be kell tartania a javaslatban előterjesztett biztonsági szabályokat – megszüntetve annak lehetőségét, hogy a tagállamok bizonyos esetekben testre szabják a követelményeket;
- az alapvető szolgáltatások (OES) üzemeltetői és a digitális szolgáltatók (DSP-k, amelyek jelenleg három kategóriába sorolhatók: online piacterek, keresőmotorok és felhőszolgáltatók) közötti különbségtétel megszüntetése;
- az IKT-ellátási lánc kiberbiztonságának kezelése;
- kétlépcsős eljárás bevezetése a jelentős biztonsági megsértések bejelentésére; és
- meg nem felelés esetén 10 millió euróig terjedő, vagy az egységek világszerte elért teljes forgalmának 2%-át kitevő adminisztratív bírságok kiszabása, attól függően, hogy melyik magasabb.

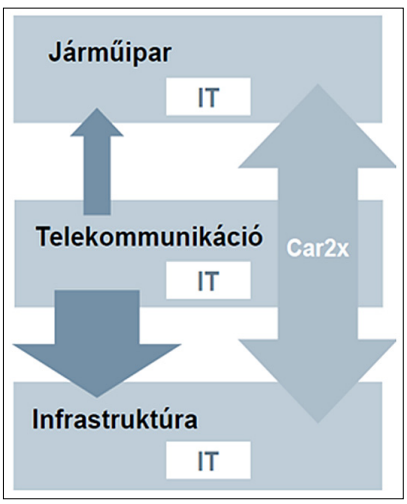
Politikai szinten a felülvizsgált NIS2-irányelv egy olyan uniós válságkezelési keretrendszert irányozna elő, amely előírná az uniós tagállamoknak, hogy fogadjanak el tervet a kiberbiztonsági események és válságok uniós szintű kezelésére, és jelöljenek ki nemzeti szintű illetékes hatóságokat, amelyek felelősek annak végrehajtásáért és betartatásáért.

Ez a három rendelet által meghatározott jogszabályi környezet jelentős támogatást ad az EU-szintű mobilitási adattér létrejöttének megalapozásához.

6. Hiányzó feltételek

A jövő közlekedésének kialakítására már nagyon jelentős fejlesztési eredmények születtek. A *2. ábra* bemutatja, hogy a fő együttműködő partnerek – Jármű, Infrastruktúra, Telekommunikáció – között milyen kapcsolódás, illetve logikai együttműködési modell képzelhető el. A legnagyobb probléma, hogy ebben a struktúrában még nincsenek kidolgozva és beépítve az alábbi szerepek:

1. hatósági, állami szerepek definiálása,
2. bűnüldözés, bűnmegelőzés, terrorelhárítás feltételrendszere,
3. az egész ökoszisztémát tanúsító szervezetek szerepe és lehetősége,
4. garanciát illetve a biztosítást nyújtó szereplők csatlakozási felülete,
5. különböző típusú járművek heterogén életkorának és felszereltségének a kezelése.



2. ábra
Az érintett iparágak együttműködése

(Forrás: Üveges P., Bogárdi P.: „Önvezető és vezetést támogató technológiák közúti infrastruktúrája” – SiemensMobility előadás, 2019.)

7. ITS ökoszisztéma – mint a közlekedés egészének a „security log”-ja

ITS alatt értjük a közlekedésben alkalmazott infokommunikációs technológiák alkotta egységes rendszert, amely segítségével optimalizálhatók a közlekedési módok, javítható a költséghatékonyság, csökkenthető a környezeti terhelés, javítható a közlekedés biztonsága, informáltsága és komfortja mind társadalmi, mind egyéni szempontból.

A hangsúlyt arra kell helyezni, hogy egyszerre kell teljesülnie mind a társadalmi, mind az egyéni szempontoknak. Ez alapján a hipotézisünk az, hogy a közhitelesen rögzített közlekedési adatokra épülve kell létrehozni az ITS adatokra épülő ökoszisztémáját. Ezzel biztosítanunk kell a közlekedés egészének „security log”-ját. Security log-on azt értjük, hogy digitálisan és közhitelesen, az eIDAS-konform eszközhöz rendelten rögzíteni kell magukat a közlekedési trajektóriákat és ezzel minden entitásnak az állapotváltozását, legyen az mozgó vagy nem mozgó résztvevője a közlekedési térnek.

Ennek eredményeként azt feltételezzük, hogy pozitívan meg fog változni a közlekedésben résztvevők viselkedése, mert minden mérhető és dokumentálható lesz, ezáltal jelentősen csökkenthető lesz a közlekedésből származó társadalmi veszteség és jelentősen javítható lesz a közlekedésbiztonság. Ezzel kialakítható – EU-konform módon – a közlekedés egészének közhiteles tanúsíthatósága. A gyakorlati megvalósításhoz a már elterjedt, flottakövető rendszerekhez hasonló rendszert kell kialakítani, amely integrált digitális hatósági rendszerként kerülne megvalósításra, és amely adatvédelmi szempontból az EU GDPR, az eIDAS és a NIS(2) rendeleteinek is megfelelne a létrejövő EU kiberbiztonsági tanúsítás szerint.

Az előző gondolatmenet alapján egy bizalmi modell jönne létre, az ún. *Trust Space,* amely olyan speciális adattér, amelynek elemei kiberbiztonsági szempontból garantáltan védettek és tanúsítottak. A Trust Space-ben lévő adatok megmásíthatatlanok, megőrzöttek, kompromittálhatatlanok, adott felhasználási célra érvényesek és elérhetők. A felhasználás ellenőrizhetőségének mind technikailag, mind törvényi szabályozás szerint biztosítottnak kell lennie a teljes életciklus alatt. Ez a bizalmi modell a bizalom két szintjén alapul:

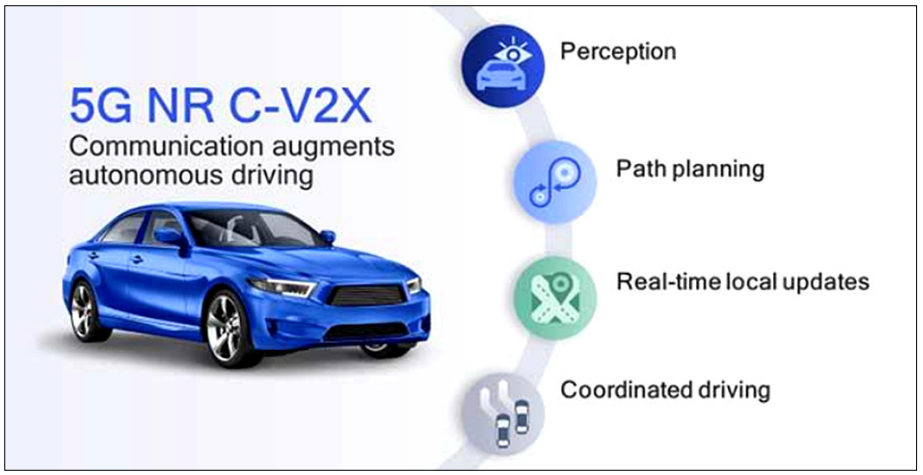
- *egyéni szintű bizalom,* amely a szereplők tevékenységének teljeskörű biztonsági logolását jelenti;
- *rendszerszintű bizalom,* amelynek alapja a rendszer egészén belüli Zero Trust elvre épülne, ki kell zárni minden olyan elemet, amelynek biztosítása egyéni hozzáálláson vagy ki nem kényszeríthető szabálykövetésen múlna.

  Ezt célozza meg a *Zero Trust Architecture*[4] szabvány NIST 800-207 külön kiadványa.

A mobilitási adattér részhalmazaként értelmezhetjük az ITS-ökoszisztémát, mint a közlekedés security logját. Ez azt jelenti, hogy az 5G-hálózat kialakítása előtt létre lehet hozni ezt a security logot, amely később a teljes mobilitási adattér kialakulását követően is fentartható és fentartandó lesz, mint közhiteles bizonyító digitális lenyomata a közlekedés egészének. Ennek kialakulása elő tudja segíteni az autonóm közlekedés kialakulását, és a korábban felsorolt hiányzó feltételek megalapozását azzal, hogy minden szereplőről képes lesz közhiteles mobilitási adatokat összegyűjteni.

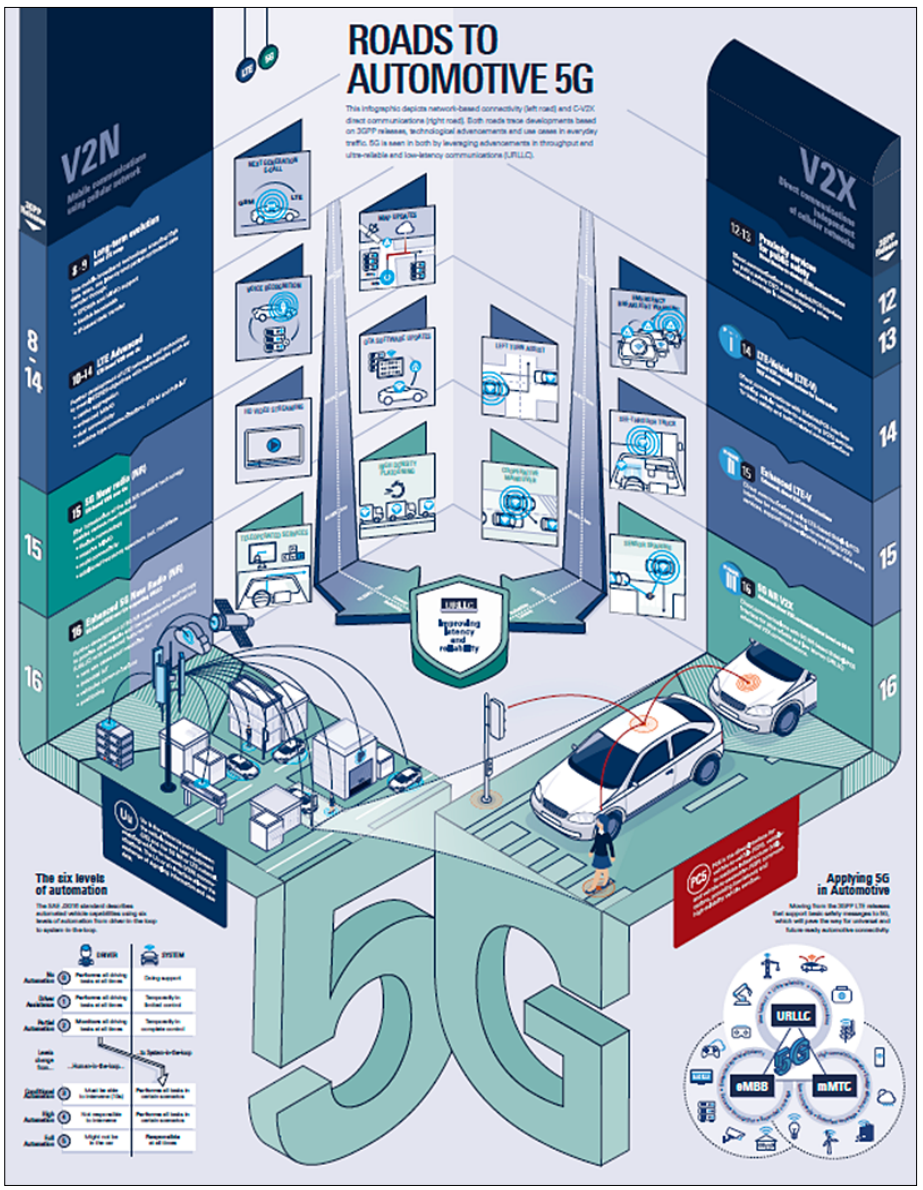
Magának az ITS-ökoszisztémának nem szükségképpen kell nagy sávszélességű, magas rendelkezésre ál-

4 *https://csrc.nist.gov/publications/detail/sp/800-207/final (2021.01.17.)*



3. ábra Az 5G és az autonóm közlekedés főbb kapcsolódásai
(Forrás: www.slideshare.net/qualcommwirelessevolution/power-point-messaging-5g-nr-based-cv2x, 2021.01.17.)

4. ábra 5G és az autonóm vezetés részletei
(Forrás: www.rohde-schwarz.com/au/solutions/test-and-measurement/automotive/connectivity/infographic-the-road-to-5g-in-automotive_253544.html, 2021.01.30.)



lású, mindenhol nagyon kiemelt biztonsági paraméterekkel rendelkező hálózati lefedettségi támogatás, mint például az 5G-hálózat, azonban az autonóm közlekedés hatalmas adatigényének kielégítéséhez kapcsolódó mobilitási adattérnek már igen. Ennek főbb szempontjai a *3. ábrán,* a részletes szempontok pedig a *4. ábrán* láthatóak.

8. Összefoglalás

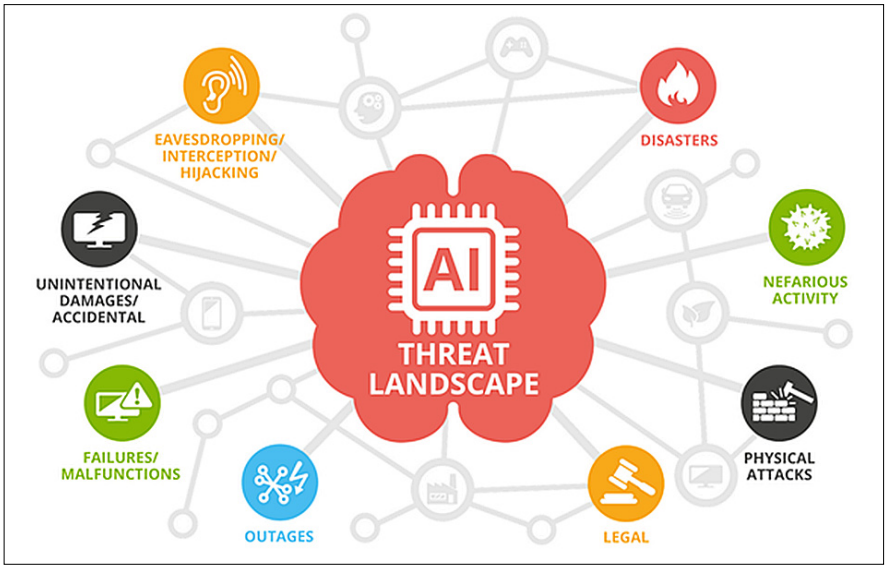
A közös európai mobilitási adattér és az ITS közlekedési rendszerek esetén kiemelt feladat a kiberfenyegetettség minimalizálása, kizárása. Ennek érdekében mielőbb ki kell alakítani a mindenhol elérhető 5G-hálózatot, mivel ennek kell szükségképpen megfelelő biztonsági megfelelőséggel rendelkeznie. Az adatok összegyűjtése és mozgatása során az adattér számára részben az 5G-hálózat fogja megteremteni az itt megosztott adatokból létrejövő Trust Space garantálását és az EU kiberbiztonsági keretrendszer szerinti tanúsíthatóságát is. Az ITS-ökoszisztéma esetén garantálni kell a közhitelességi és a GDPR-elvárások teljesülését. Ehhez az eIDAS szerint történő eID-hozzárendelhetőséget lesz érdemes kialakítani.

A jövőben meg kell vizsgálni kiberbiztonsági szempontból a már kialakult forgalomirányító és közlekedésbiztonság támogató rendszereket, illetve a járműveken belüli aktív közlekedésbiztonsági rendszerek esetén is a mesterséges intelligencia alkalmazhatóságát. A legacy- (örökölt) rendszerek integrálása a közös mobilitási adattérbe kiemelt kiberbiztonsági kockázati tényezőt jelentenek.

Külön vizsgálandó feladat a közösségimédia-alapú navigációs rendszerek és a közösségi közlekedési rendszerek között megteremthető kölcsönhatás és ezek együttes hatása az adatvezérelt közlekedési rendszerek kialakítására.

A közlekedési rendszerekben használt informatikai rendszerek átlagos felhasználóin kívül kiemelten kell kezelni elsősorban a privilegizált felhasználók, a rendszergazdák és az adatgazdák kiberbiztonsági tudatosságát, valamint a szabályok betartását és betartatását.

Az ENISA által publikált *5. ábrán* látható, hogy az adatrobbanás és a mesterséges intelligencia elterjedése is milyen kockázatokat hordoz a jövőben. Azonban napjainkban még az adatbiztonsági sérülékenységek és azok kihasználhatósága a legtöbb esetben emberi hibákra vezethető vissza, mint a napjainkban kirobbant eddigi legnagyobb világméretű kiberbiztonsági sérülékenység, ahol a legjelentősebb vállalatok IT-rendszereiben kialakított speciális szoftverek biztonsági frissítéseinél használt jelszó a „solarwinds123”[5] volt. Le kell vonnunk ebből azt a tapasztalatot, hogy a közlekedés egésze számára csak olyan ITS-rendszer alakítható ki, amely kizár minden kiberbiztonsági kockázatot, azaz megfelel az alapvető szolgáltatásokat nyújtó kritikus szereplők rezilienciájáról szóló NIS2-irányelvre irányuló javaslatnak. A cél a közlekedéssel szembeni kiberfizikai fenyegetések mérséklése és ezek preventív módon történő kizárása.



5. ábra ENISA – A mesterséges intelligencia kiberbiztonsági kihívásai

(Forrás: www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges, 2021.01.29.)

A szerzőkről

BÓDI ANTAL matematika-fizika-számítástechnika szakos tanári, anyagtudományi mérnök-fizikusi, valamint infokommunikáció menedzsment szakon szerzett MBA-oklevelet és 2017-től az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatója. 1990-től a BGyTF számítógépközpontját vezette és részt vett a Szab-I-Net Kht., később a UPC szélessávú internetszolgáltatásának kialakításában, majd az Antenna Hungária DVB-T-projektjében. 2002-től a Kopint-Datorgban a www.magyarorszag.hu és az Ügyfélkapu kialakításán dolgozott. A NISZ ZRt.-nél az eSZIG, AVDH, GovCA, Önkormányzati ASP IT biztonsági projekteket menedzselte. 2016-tól a KTI Közlekedéstudományi Intézet ITS tanúsítási irodavezetője. Az ITS-ökoszisztéma kialakításával és a közlekedés digitalizációjával foglalkozik. A HTE ISZB tagja.

MAROS DÓRA a Budapesti Műszaki Egyetemen, híradástechnika szakon végzett, ezt követően PhD-fokozatot szerzett a Zrínyi Miklós Nemzetvédelmi Egyetem Műszaki Doktori Iskolájában. Főbb kutatási területe a mobil távközlés és a kritikus infrastruktúra hálózatok. Nyolc éven át az Óbudai Egyetem Villamosmérnöki Karának tudományos dékánhelyettese volt és öt évig a Híradástechnika Intézet igazgatója. Számos magyar és nemzetközi tudományos konferencia szervezője és előadója. A Közlekedéstudományi Intézet vezető szakértője és tudományos tanácsadója 2014 óta.

Hivatkozások

[1] COM(2020) 66: European strategy for data.
[2] COM(2020) 65: On Artificial Intelligence – A European approach to excellence and trust.
[3] Pintér Róbert, Kis Gergely; Az információs társadalom és más versengő metanarratívák. In: BME–UNESCO, Információs Társadalom- és Trendkutató Központjának kutatócsoportja, Évtizedjelentés: ITTK Budapest, (2008), pp.5–62.
[4] Sallai Gy., Horváth P., Abos I., Bartolits I., Bódi A., Huszty G.; A hazai szélessávú infokommunikációs infrastruktúra fejlesztése. Híradástechnika: HÍRKÖZLÉS-INFORMATIKA, 2009:1-2, pp.4–17.
[5] A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), 2019, Országjelentés: Magyarország.
[6] Gigabit Hungary Stratégia (GHS) 2020–2030, Nemzeti Digitalizációs Stratégia (NDS) 2021–2030, Magyar 5G Stratégia szakmai tervezete (munkapéldány).
[7] Bódi A., Maros D.; A komplex ITS ökoszisztéma alapjai. In: Vigh, László (szerk.) Az infrastruktúra és a gazdaság távlatai 2020 előtt. Budapest, Edutus Egyetem, (2019), pp.48–70.
[8] Bódi A., Szabó T., Maros D., Gáspár L.; ITS ökoszisztéma – A közlekedés egészének digitalizációja. „Utazás a tudományban” konferencia a 70 éves Pálfalvi József tiszteletére. Konferenciakötet, Bp., Corvinus Egyetem, (2018), pp.82–84.
[9] Beke É., Bódi A., Takácsné Gy. K., Kovács T., Maros D., Gáspár L.; The role of drones in linking industry 4.0 and ITS Ecosystems. IEEE 18th International Symposium on Computational Intelligence and Informatics (CINTI 2018) Budapest: IEEE Hungary Section, (2018), pp.191–197.
[10] Charlotte Ducuing; Beyond the data flow paradigm: governing data requires to look beyond data, Technology and Regulation, 2020.006, pp.57–64, ISSN: 2666-139X, *https://doi.org/10.26116/techreg*

5 Security Researcher Reveals Solarwinds' Update Server Was 'Secured' With The Password 'solarwinds123': https://www.techdirt.com/articles/20201215/13203045893/security-researcher-reveals-solarwinds-update-server-was-secured-with-password-solarwinds123.shtml (2020.12.20.)