IOT eszközök és 5G hálózat biztonsági lehetőségei

Dr. habil. Garai-Fodor Mónika

Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar,
fodor.monika@kgk.uni-obuda.hu

Viktor Patrik

Egyetemi tanársegéd, Óbudai Egyetem, Keleti Károly Gazdasági Kar,
viktor.patrik@kgk.uni-obuda.hu

A Jelen tanulmány keretében az 5 G hálózat megjelenésével foglalkoztunk, annak is IT biztonság szempontjából elemeztük várható hatásait. generáció-specifikus aspektusból. Feltételeztük, hogy az egyes generációk általános értékrendje, magatartásformája visszatükröződik az IT biztonság megítélésében és az 5 G hálózatokkal szembeni hozzáállásban is. A tanulmányban releváns szekunder források mellett primer kutatás konklúzióit mutatjuk be. A primer vizsgálat keretében kvantitatív kutatást valósítottunk meg, előtesztelt sztenderdizált kérdőív használatával. Az alanyok rekrutálása hólabda mintavételi eljárással történt, mely során első bázist saját aktív hallgatóink jelentették. A mintavétel eredményeként 391 értékelhető kérdőívet kaptunk. A kutatás eredményei szerint az informatikai támadások ismerete és az emberi tényező IT biztonságban betöltött szerepének megítélése generáció-specifikus elemeket hordoz. Ugyanakkor az 5 G házatok megítélése nem differenciált, erősebb bizonytalanság jellemzi valamennyi vizsgált generációt.

5G, IOT, biztonság, generáció.

1 Bevezetés

Hálózatok kötik össze a gépeket, számítástechnikai eszközöket, kisebb-nagyobb vállalati, ipari, információs rendszereket, hálózatok kötik össze az embereket, vesznek körül minket napi szinten. A hálózatok szerepe egyre fontosabbá vált a digitalizációnak köszönhetően, ami annak feltételeként és folyományaként is értelmezhető (Csiszárik-Kocsir, 2022; Dobos et al, 2022; Mizser et al, 2022; Tóth-

Csiszárik-Kocsir, 2022). Hálózatban élünk egymással, bármilyen megközelítésből is nézzük a témakört, a hálózat fogalma mindig is ott volt az emberek életében valamilyen formában. A választásom ezért esett erre a témára. Bármivel is foglalkozunk, bármilyen számítástechnikával vagy élettel kapcsolatos helyzetet vizsgálunk, bármilyen helyzetben vagyunk, meglátásom szerint, a hálózat kérdésköre minden bizonnyal jelen van, hiszen az ember egy társas lény, saját egzisztenciájának fenntartása érdekében nem tud teljes mértékben elzárkózni ettől.

Mit ér egy fénykép, ha nem oszthatjuk meg valakivel? Mit ér egy szó, ha másnak erről nem adhatunk tudomást? Mi a jelentősége egy sikerélménynek, ha nem mondhatjuk el a tőlünk messze élő családtagjainknak, vagy mit kezdünk a negatív élményeinkkel egyedül, ha senkit sem tudnánk segítségül hívni a hálózat hiánya miatt?

A hálózatok rengeteg előnnyel rendelkeznek, azonban nem szabad figyelmen kívül hagyni a számos jelentős hátrányt sem, mely megjelenésükhöz köthető. Az esetek nagy részében szükség van arra, hogy megosszunk adatokat vagy információkat. Azonban néhány esetben, az érzékenyebb információtartalommal rendelkező üzeneteknél ezzel ellentétben éppen az az érték, hogy kevés ember tud róla. Ezeknél az üzeneteknél fontos, hogy ne kerüljön olyan emberek kezébe, olyan emberek szeme elé, akik erre nem jogosultak, mert ez felmérhetetlen károkat képes okozni (pl. egy üzleti titok, személyes információk, egy jelszó stb.). Az informatika témaköreit böngészve, napjaink egyik lehető legaktuálisabb, legtöbb szakembert foglalkoztató témája az ötödik generációs mobilhálózat és annak kihatása az élet különböző területeire. Az 5G mára elindult a legtöbb erre alkalmas országban, jelen van az emberek köztudatában, nagyon sok kérdést vet fel, sokan beszélnek róla, de viszonylag kevesen tudják, hogy valójában ez a kifejezés mit is takar. Mikor az 5G-ről beszélünk, legfőbbképpen a jövőről beszélünk és az ebben rejlő lehetőségekről és nem a jelenről, mert a jelenben még nem érezzük ennek a hatását komolyabb szinten, illetve még nagyon sok kiaknázatlan lehetőséget tartogat ez a hálózat. Az új generációs hálózat rengeteg kaput nyit meg a technológia számára, de vajon a társadalomnak több előnye, haszna származhat ebből, mint amennyi kár érheti ennek kapcsán? Vajon az 5G mennyire lesz hatással az ember saját privát szférájának megtartására, mennyire veszélyezteti annak fennmaradását? Elegendőek az eddigi internethasználattal kapcsolatban megfogalmazott szabályozások, korlátozások, vagy esetleg új lehatárolásokra is szükség van ezen a téren? Az adataink mennyire lesznek kitéve nagyobb biztonsági kockázatnak az 5G-re váltás során? Vajon ez a fajta hálózat mennyire ad teret a kibertámadások fellendüléséhez? Kutatásunkban ilyen -és ezekhez hasonló kérdésekre szeretnék választ keresni.

2 Szakirodalmi feldolgozás

2.1 5G Biztonsága

Az mobilkommunikációs evolúció jelenlegi lépcsőfoka, az 5.generációs mobilhálózat bevezetése rengeteg biztonsági kérdés és megoldás megfogalmazását követeli. Az 5G számtalan új szolgálatatás használatát teszi lehetővé a korábbi elődje, a 4G után, azonban ezek biztonságos használatához szükséges a biztonsági rendszerek és védekezési protokollok fejlesztése is.(Balogh et al., 2020) Az 5G fő jellegzetességei közé tartozik többek között a magasabb kapacitás, az eszközök közötti kommunikáció (D2D- device-to-device) támogatása, az MMTC (Massive Machine-Type Communication), a nagyon alacsony látencia (válaszidő), az alacsonyabb energiafelhasználás, a gyorsabb letöltési és feltöltési sebesség. Az eddigieket összefoglalva az 5G képes akár a 10Gbps-os sebesség elérésére, 1 ms-os válaszidő mellett, valamint területenként sokkal szélesebb sávot tud biztosítani a kommunikáció számára. A hálózathoz jóval több eszköz csatlakozhat egyszerre, a hálózat csökkentett energiafelhasználása jellemzi. (K.-D. et al., 2019) Ahhoz, hogy mindezt el lehessen érni különféle technológiák bevezetésére volt szükség az 5G rendszerekben, mint a heterogén hálózatok (HetNet) kialakítása, a massive multiple-input multiple-output (MIMO) technológia, a D2D kommunikáció, a szoftver definiált hálózat (software defined network SDN), a hálózati funkciók virtualizációja (network functions virtualization- NFV) és a network-slicing, azaz a „hálózat-szeletelés”. Az 5G-s rendszer új hálózati architektúrája, az új felhasználási területek számos biztonsági kihívás elé állították a hálózatfejlesztőket a biztonság és adatvédelem terén. Az 5G evolúciós létrájának végső lépcsőfokai közé tartozik az elérhetőség és lefedettség minden eddigi szintnél nagyobb körben való kiterjesztése, illetve a hálózatok teljes konvergenciájának megvalósítása. A működő hálózatok „egybeolvasztása” egy sokkal gördülékenyebb kommunikáció megteremtését válthatja valóra, azonban ahhoz, hogy ez az egység kialakuljon és biztonságosan használni lehessen, még jó néhány biztonsági kérdés pontosítása szükséges.(Michelberger et al, 2012)

Az 5G-s hálózat természete miatt nehéz a különböző biztonsági funkciók megvalósítása, mint az autentikáció, integritás és a ’titoktartás’. Az eddig mobilhálózatokban is vannak biztonsági sebezhetőségek, adatvédelmi kockázatok a hálózat különböző rétegeiben pl.: a media access control (MAC) rétegben és a fizikai rétegben (PHY- physical layer), melyek az 5G bevezetésével még nagyobb teret nyerhetnek.(Fang et al.,2017) A hang és adatszolgáltatások biztonsági védelme a hagyományos biztonsági architektúrán alapszik, - több biztonsági funkció együttes működésével karöltve, mint a felhasználói identitás menedzsment, a kölcsönös autentikációs folyamat a hálózat és az UE (User Equipment – felhasználó eszköze) között, a kommunikációs csatorna védelme - azonban a tradícionális módszerek alkalmazása nem biztos, hogy elegendő az 5G-

s hálózat védelméhez. (Shafique et al., 2020) Az LTE hálózatok fejlesztése során megvalósult a magasszintű biztonság és megbízhatóság kialakítása, mely a felhasználói adatforgalom titkosításával és az autentikáció alkalmazásával volt elérhető az UE és a központi állomás között, ami létfontosságú szerepet játszik a kiberbiztonságban.(Cao et al.,2020) A korábbi hálózatban ezeken a biztonsági funkciókon kívül a hozzáférés és mobilitás menedzsment biztonságát egy kulcs hierarchia és a „handover key management" biztosította, de mindezek jelenléte mellett is szükséges a biztonsági és adatvédelmi technológiák korszerűsítése, implementálása, hogy azok kompatibilisek legyenek az 5G adta új felhasználási területekkel és technológiákkal is. (Li et al., 2020) Ezek az újtechnológiák nem csupán új szolgáltatások megjelenését ösztönzik, hanem új biztonsági sebezhetőségeket is hoznak magukkal, melyek megoldásra várnak. (Zhang et al., 2019)

Az új sérülékenységek megjelenése mellett az 5G bevezetése néhány biztonsági szempontból előrelépést is jelent. Ezek a következők:

- Titkosított adatátvitel biztosítása és állandó felhasználói azonosító struktúra
- Megerősített autentikációs mechanizmusok
- Adatok integritásvédelme
- Lehetővé teszi a titkosított csatornán való hozzáférést nem 3GPP-rendszerek felől is
- Lehetőség van a TLS titkosításra a hálózati funkciók között a maghálózaton
- Nyomon követhetőség biztosítása, mely a műveletek regisztrálását, biztonsági elemzések futtatását megkönnyíti.

2.2 Adatvédelem 5G hálózatban

A spanyol adatvédelmi hatóság (AEPD) 2020 májusában közzétett jelentésében több 5G- vel kapcsolatos kockázatot azonosított. A kockázatok egy része nem új, már a korábbi mobilhálózatoknál is jelen volt, viszont ezek a kockázatok az 5G bevezetésével megnőhetnek.(Garcia et al., 2019)

- Precízebb helymeghatározás
- Profilalkotás és automatizált döntéshozatal: Az 5G megjelenésével egyre több eszköz lesz a hálózatra csatlakoztatva, egyre több adat fog rendelkezésre állni, így még kiterjedtebb profilalkotásra és automatizált döntéshozatal alkalmazására nyílhat lehetőség.(Morocho-Cayamcela et al., 2019)

- A szolgáltatási láncban jelen lévő szolgáltatók száma jelentős mértékben megnövekedik, így az 5G-s új szolgáltatások kapcsán a felelősségvállalás több részre osztódhat (gyártók, szolgáltatók, hálózat üzemeltetők).
- A különböző szereplők által megfogalmazott adatvédelmi célok egymástól eltérhetnek, a szereplők növekedésével különböző érdekek ütközhetnek, illetve egyes szereplőkre speciális szabályok vonatkozhatnak.
- Az 5G hálózat nem rendelkezik egységes biztonsági modellel, így a biztonsági megoldások és szabványok tekintetében is több szereplőre lehet számítani
- A korábban használatba vett rendszerek adatvédelmi sérülékenységei továbbra is fennmaradnak és az új szolgáltatásokat is érinthetik.
- A hálózat jelenlévő problémái a hálózati szeletekre öröklődhetnek
- A hálózat üzemeltetése, a rendszer menedzselésre dinamikusabbá fog válni és ez instabil rendszert eredményezhet
- Felhasználói kontroll lehetséges elvesztése: Az adatok határokon átnyúló mozgása és a különböző jogi környezetek problémákat okozhatnak.(Hassan et al.,2019)

2.3 Biztonsági funkciók az 5G-ben

1. Autentikáció

Kétféle autentikáció létezik, az egyik az entitás autentikációja a másik pedig az üzenet autentikációja és mindkét fajta hitelesítés fontos szerepet játszik az 5G hálózatok támadásainak kivédése ellen. A mobilhálózatokban a kölcsönös azonosítás az UE - felhasználói eszközök között és az MME (Mobility Management Entity) között végbemegy mielőtt maga a kommunikáció megkezdődne.(Shafique et al.,2020)

Az autentikáció és a kulcs kezelés a 4G/LTE hálózatokban szimmetrikus kulcs alapú, azonban az 5G esetében az azonosításra nem csak az UE és MME között lesz szükség, hanem további harmadik feles szereplők is részt kell, hogy vegyenek a folyamatban, ami további komplikációkat okoz. Mivel más szolgáltatók is jelen lesznek, ezért szükség van az 5G esetében egy hibrid, rugalmas autentikációs menedzselés kialakítására. Ezt a hibrid hitelesítési folyamatot háromféleképpen lehet kialakítani: hitelesítés kizárólag a hálózat által, hitelesítés csak a szolgáltatást nyújtó által, vagy hitelesítés mind a hálózat és szolgáltatást nyújtó által. Az 5G által biztosított alacsony válaszidő és magas adatátviteli sebesség miatt az autentikációs folyamat sokkal gyorsabban végbemehet hálózatváltás során. A hibák kiszűrésére több technológiát is javasolnak a fejlesztők, mint az SDN által

aktivált autentikációs séma, publikus kulcs alapú hitelesítés, CRC (Cyclic Redundancy Check). (Ghosh,2019)

2. Titoktartás

Az adatok titoktartása segíti az adatokat megvédeni a passzív támadásoktól, amit az adatok hozzáférésének limitálásával tesz. Ez a funkció továbbá segíti megelőzni az adatok elemzésével járó támadást (traffic analysis), melyekre különös figyelmet kell fordítani az 5G esetében, ugyanis egyre több érzékeny adat fog potenciális veszélybe kerülni (forgalmi adatok, egészségügyi adatok stb.).(Pirinen,2014)

Az adatok titkosítása széles körben használatos az adatok védelmére, azonban a hagyományos kriptográfiai modellek nem elegendőek a kellő biztonság kialakítására, mert nem számolnak azzal, hogy néhány támadó rendelkezhet magas számítási kapacitásra alkalmas eszközzel. Az adatvédelmi szolgáltatásoknak nagy szerepe van az 5G során, ugyanis egy érzékeny adat kiszivárgása felmérhetetlen károkat tud okozni. (Liu et al,2019)

3. Elérhetőség

Az elérhetőség azt jelenti, hogy a szolgáltatásnak mindig, mindenhol, mindenki számára elérhetőnek kell lenni. A leggyakoribb elérhetőség elleni támadás a korábban említett DoS és DDoS támadás. Mivel az 5G-s mobilhálózatban rengeteg IoT eszköz lesz egy hálózatra csatlakoztatva, ezért ez komoly problémákat okozhat a jövőben. Az elérhetőség biztosítására a fizikai rétegben a korábban említett DSSS-t és FHSS-t használják. (Wu et al., 2020)

4. Integritás

Az integritás megakadályozza, hogy az információ módosítva legyen támadók által. A hangszolgáltatást és adatszolgáltatást összehasonlítva az adatok nagyobb veszélyben vannak, mer ezeket könnyebb módosítani, ezért van szükség az integritás védelemre. (Li et al., 2017)

Saját véleményünk szerint az 5G megnövelheti a kibertámadások számát. Az új hálózat számos új sérülékenységgel jár együtt, így potenciális veszélyforrás lehet személyes adatainkra. Az 5G még jelenleg is fejlődő stádiumában áll, mégis már elérhető a kereskedelemben is, azonban a bevezetésre szükség volt, mert e nélkül nehezebb lenne azonosítani a hálózat új sérülékenységeit. Az 5G elterjedésével az IoT eszközök is még szélesebb körben fognak terjedni és a több hálózatra csatlakoztatott eszköz több veszélyforrást generál. Személyes adataink védelmének tekintetében, meglátásom szerint a legnagyobb veszélyt a pontosabb geolokáció, illetve az IoT eszközök növekedő száma okozhatja. (Fang et al.,2017)

3 Anyag és módszertan

A tanulmányban ismertetett szekunder elemzések mellett primer kutatásunk eredményeit kívánjuk bemutatni. A primer vizsgálat keretében kvantitatív kutatást valósítottunk meg, előtesztelt sztenderdizált kérdőív használatával.

A kvantitatív adatfelvétel online megkérdezés formájában zajlott. Az alanyok rekrutálása hólabda mintavételi eljárással történt, mely során első bázist saját aktív hallgatóink jelentették. Amintavétel eredményeként 391 értékelhető kérdőívet kaptunk. A kutatási segédeszköz kizárólag zárt kérdéseket tartalmazott, nominális mérési szinten (egy- és többválasztásos kérdések formájában), továbbá metrikus skálákat (Likert-skála és szemantikus differenciál skála).

A sztenderdizált kérdőív összesen 21 kérdésből állt, témakörei az alábbiak voltak: általános IT biztonság, az % megjelenésének megítélése IT biztonsági aspektusból,, általános IT ismertek, szocio-demográfiai kérdések.

A kvantitatív eredmények feldolgozása során leíró statisztikát, kettő- és többváltozós elemzéseket alkalmaztunk SPSS 22.0 szoftvert felhasználásával. Jelen tanulmányban a leíró statisztikai eredmények mellett a nominális és metrikus skálán mért eredmények összefüggésének vizsgálatához használt variancia-analízis módszerét alkalmaztuk, azon belül is az egyszempontos, több mintaátlag összehasonlítására alkalmas ANOVA módszert. Egy metrikus függő változó átlagát hasonlítottuk össze kettőnél több csoport között. A post-hoc teszt alapján állapítottuk meg, hogy mely csoportpárok között volt szignifikáns eltérés Ennek során a szignifikancia-értékeket vettük alapul az összefüggések meglétének megállapításához (sig<= 0,05). A csoportátlagok összevetése mentén elemeztük a belső összefüggéseket az F-statisztikát alkalmazva, azaz a mintákon belüli átlagok varianciájának a varianciahányadosát figyelembe véve (Sajtos & Mitev, 2007; Malhotra,Simon, 2017). A tanulmányban ismertetésre kerülő összefüggés-vizsgálatok esetén, ahol az ANOVA- tábla szerinti szignifikancia érték 0,05 alatti volt, ott igazolttá vált, hogy az életkor-csoport (generáció) és a vizsgált változók között az összefüggés fennáll, így az SPSS poszt-hoc teszt eredményei közül ezen adatokat emeltük ki és szemléltettük a kutatásban.

A kvantitatív kutatási fázis során fő célunk az alábbi hipotézis elemzése volt:

H1: Az IT biztonság megítélése generáció-specifikus elemeket hordoz

H1/a) Az IT támadások ismerete generáció-specifikus elemeket hordoz

H1/b) Az IT biztonságban az emberi tényező szerepének megítélése generáció-specifikus elemeket hordoz

H2: Annak megítélése, hogy az 5G hálózat az IT támadásoknak nagyobb teret ad generációs sajátosságokat hordoz.

4 Eredmények

Első számú hipotézisünk vizsgálata céljából elemeztük, hogy az informatikai támadások ismerete tekintetében vannak e generációk között megmutatkozó különbségek. A variancia-analízis szignifikancia értéke alapján (0,01) megállapíthattuk, hogy a két változó között szignifikáns kapcsolat van (H1/a beigazolódott):

Az eredmények fényében azt láthattuk, hogy az X és a Z generáció a leginkább tájékozott az IT biztonság tekintetében.

Tudom, hogy milyen jellegű informatikai támadások léteznek	N	Mean*	Std. Deviation	szignifikancia
X generáció	141	4,37	0,959	0,01
Y generáció	22	3,73	1,162	
Z generáció	177	4,43	0,896	
Baby boom generáció	50	4,26	0,944	
Összesen	390	4,35	0,952	
1=egyáltalán nem értek egyet, 5= teljes mértékben egyetértek; variancia-analízis; One Way Anova, Post Hoc Test				

1. táblázat: Az informatikai támadások ismerte az egyes generációk körében
Forrás: saját kutatás, N=390, *átlag, ahol 1=egyáltalán nem értek egyet, 5= teljes mértékben egyetértek; variancia-analízis; One Way Anova, Post Hoc Test

További hipotézis-vizsgálat érekében elemeztük, hogy az emberi tényező IT biztonságban betöltött szerepét az egyes generációk eltérően ítélik e meg.

Az eredmények szerint az egyes generációk között szignifikáns különbség mutatkozott (H1/b beigazolódott).

Az X generáció tartotta az emberi tényező szerepét a legfontosabbnak az IT biztonság tekintetében.

Az informatikai védelem az emberi tényezőn múlik	N	Mean*	Std. Deviation	szignifikancia
X generáció	141	2,57	1,064	0,04
Y generáció	22	2,45	0,912	
Z generáció	177	2,21	1,131	
Baby boom generáció	50	2,42	1,247	
Összesen	390	2,38	1,120	

2. táblázat: Az informatikai védelem generáció-specifikus megítélése
Forrás: saját kutatás, N=390, *átlag, ahol 1=egyáltalán nem értek egyet, 5= teljes mértékben egyetértek; variancia-analízis; One Way Anova, Post Hoc Test

Külön kérdésben elemeztük az 5G hálózatok IT biztonság szempontjából történő megítélését. E tekintetben is megnéztük, hogy az egyes generációk véleménye eltérést mutat e. Az eredmények fényében elmondható, hogy az 5 G megjelenését nem ítélték meg differenciáltan (sig>=0,05) az egyes generációk (H2 nem igazolódott be).

Az átlagok abszolút értékét tekintve azt láthatjuk, hogy az Y generáció a leginkább szkeptikus az 5G megjelenését tekintve. Összességben a bizonytalanság jellemezte a mintát.

Generációk	N	Mean*	Std. Deviation	szignifikancia
X generáció	141	2,88	1,045 Ft	0,181
Y generáció	22	2,95	1,174 Ft	
Z generáció	177	2,67	0,991 Ft	
Baby boom generáció	50	2,60	1,245 Ft	
Összesen	390	2,75	1,059 Ft	

3. táblázat: 5G megjelenésének IT biztonságra gyakorolt hatása generáció-specifikus aspektusból

Forrás: saját kutatás, N=390, *átlag, ahol 1=egyáltalán nem értek egyet, 5= teljes mértékben egyetértek; variancia-analízis; One Way Anova, Post Hoc Test

Összefoglalás

Jelen tanulmány keretében az 5 G hálózat megjelenésével foglalkoztunk, annak is IT biztonság szempontjából elemeztük várható hatásait. Azt gondoljuk ,hogy az IT biztonságkérdése önmagában és az 5G megjelenésének IT biztonságra gyakorolt hatásának generáció-specifikus elemei vannak. Ennek érdekében primer vizsgálatot folytattunk le, ahol az IT biztonsággal és az 5Gmegítélésével kapcsolatos kérdések elemzését folytattuk le az egyes generációk körében. A primer vizsgálat keretében kvantitatív kutatást valósítottunk meg, előtesztelt sztenderdizált kérdőív használatával. Az alanyok rekrutálása hólabda mintavételi eljárással történt, mely során első bázist saját aktív hallgatóink jelentették. A mintavétel eredményeként 391 értékelhető kérdőívet kaptunk.

A kutatás eredményei szerint az informatikai támadások ismerete eltérő az egyes generációk között: az X és a Z generáció a leginkább tájékozott az IT biztonság tekintetében. Az emberi tényező IT biztonságban betöltött szerepét is differenciáltan ítélték meg az egyes generációk: az X generáció tartotta az emberi tényező szerepét a legfontosabbnak az IT biztonság tekintetében. Ugyanakkor az 5G hálózatok IT biztonság szempontjából történő megítélése nem mutatott szignifikáns különbséget az egyes generációk között, e tekintetben egy általános bizonytalanság volt jellemző a minta alanyaira.

Azt gondoljuk, hogy az IT biztonság tekintetében megmutatkozó generációs sajátosságokra érdemes koncentrálni az 5 G hálózatok kapcsán is. Azok bevezetését szorgalmazók számára azon generációk jelenthetik az ún. influencer/véleményvezér csoportot, aki kellően tájékozottak és ismereteik alapján

hiteles források lehetnek a többiek számára is. Így eredményeink alapján mindenképpen generációnként eltérő kommunikációs stratégiát javasolnánk az 5 G hálózatok népszerűsítése kapcsán hazánkban.

A kutatás korlátait tekintve fontos megemlíteni, hogy annak eredményei a mintavételi eljárásból fakadóan helyi értékűek. A kutatás folytatásában tervezzük poszt kvalitatív kutatás lefolytatását mini-fókuszcsoportos interjúk formájában, az egyes, 5 G hálóztok irányában tapasztalt bizonytalanság és szkepticizmus valós okainak szofisztikáltabb feltárása és megismerése céljából.

Hivatkozások

[1] Á. Csiszárik-Kocsir „The Present and Future of Banking and New Financial Players in the Digital Space of the 21st Century” ACTA POLYTECHNICA HUNGARICA 19 : 8, 143-160, 2022

[2] O. Dobos, I.M. Tóth, Á. Csiszárik-Kocsir, M. Garai-Fodor, and L. Kremmer „How Generation Z managers think about the agility in a world of digitalization” In: Szakál, Anikó (szerk.) IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics SAMI (2022) :Proceedings Poprad, Szlovákia : IEEE (2022) 207-212., 2022

[3] Cs. Mizser, M. Garai-Fodor, and Á. Csiszárik-Kocsir „Key competences of young entrepreneurs in the world of digitalisation based on the results of a Hungarian questionnaire research” In: Szakál, Anikó (szerk.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022 Budapest, Magyarország : IEEE Hungary Section. 281-286, 2022

[4] I.M. Tóth, and Csiszárik-Kocsir „Teleworking and the home office – the digital possibilities in work organization” In: Szakál, Anikó (szerk.) IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems ICCC 2022 Budapest, Magyarország : IEEE Hungary Section. 277-280., 2022

[5] A. Balogh, B. Gyenge, Á. Szeghegyi, and T. Kozma, “Advantages of simulating logistics processes,” ACTA POLYTECHNICA HUNGARICA, vol. 17, no. 1, pp. 215–229, 2020.

[6] M. E. Morocho-Cayamcela, H. Lee and W. Lim, "Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential, Limitations, and Future Directions," in IEEE Access, vol. 7, pp. 137184-137206, 2019, doi: 10.1109/ACCESS.2019.2942390.

[7] N. Hassan, K. A. Yau and C. Wu, "Edge Computing in 5G: A Review," in IEEE Access, vol. 7, pp. 127276-127289, 2019, doi: 10.1109/ACCESS.2019.2938534.

[8] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios,"

in IEEE Access, vol. 8, pp. 23022-23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[9] A. Ghosh, A. Maeder, M. Baker and D. Chandramouli, "5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15," in IEEE Access, vol. 7, pp. 127639-127651, 2019, doi: 10.1109/ACCESS.2019.2939938.

[10] P. Pirinen, "A brief overview of 5G research activities," 1st International Conference on 5G for Ubiquitous Connectivity, 2014, pp. 17-22, doi: 10.4108/icst.5gu.2014.258061.

[11] X. Liu, M. Jia, X. Zhang and W. Lu, "A Novel Multichannel Internet of Things Based on Dynamic Spectrum Sharing in 5G Communication," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 5962-5970, Aug. 2019, doi: 10.1109/JIOT.2018.2847731.

[12] T. -Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar and C. -M. Chen, "An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks," in IEEE Access, vol. 8, pp. 28096-28108, 2020, doi: 10.1109/ACCESS.2020.2969986.

[13] R. Li et al., "Intelligent 5G: When Cellular Networks Meet Artificial Intelligence," in IEEE Wireless Communications, vol. 24, no. 5, pp. 175-183, October 2017, doi: 10.1109/MWC.2017.1600304WC.

[14] Fang, D., Qian, Y. and Hu, R., Security for 5G Mobile Wireless Networks. IEEE Access, [online] 6, pp.4850-4874.2017 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125684

[15] K.-D. Anita, Z. R. Regina, and S. Ágnes, “Transport habits and preferences by generations - does it matter regarding the state of the art?,” ACTA POLYTECHNICA HUNGARICA, vol. 16, no. 1, pp. 29–44, 2019.

[16] P. Michelberger and C. Lábodi, “After Information Security – Before a Paradigm Change,” ACTA POLYTECHNICA HUNGARICA, vol. 9, no. 4, pp. 101–116, 2012.

[17] Fang, D., Qian, Y. and Hu, R., Security for 5G Mobile Wireless Networks. IEEE Access, [online] 6, pp.4850-4874.2017 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125684

[18] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," in IEEE Access, vol. 8, pp. 23022-23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[19] Y. Cai, Z. Qin, F. Cui, G. Y. Li and J. A. McCann, "Modulation and Multiple Access for 5G Networks," in IEEE Communications Surveys &

Tutorials, vol. 20, no. 1, pp. 629-646, Firstquarter 2018, doi: 10.1109/COMST.2017.2766698.

[20] Y. -N. R. Li, B. Gao, X. Zhang and K. Huang, "Beam Management in Millimeter-Wave Communications for 5G and Beyond," in IEEE Access, vol. 8, pp. 13282-13293, 2020, doi: 10.1109/ACCESS.2019.2963514.

[21] L. Zhang et al., "A Survey on 5G Millimeter Wave Communications for UAV-Assisted Wireless Networks," in IEEE Access, vol. 7, pp. 117460-117504, 2019, doi: 10.1109/ACCESS.2019.2929241.

[22] M. H. C. Garcia et al., "A Tutorial on 5G NR V2X Communications," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1972-2026, thirdquarter 2021, doi: 10.1109/COMST.2021.3057017.