EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.1.29.
COM(2020) 50 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

Az 5G biztonságos kiépítése az EU-ban – Az uniós eszköztár alkalmazása

1. Bevezetés

A távközlési hálózatok ötödik generációja (5G) alapvető szerepet fog játszani az európai társadalom és gazdaság fejlődésében. A várakozások szerint hatalmas gazdasági lehetőségeket fognak kínálni, és fontos alapként fognak szolgálni a digitális és zöld átalakuláshoz olyan területeken, mint a közlekedés, az energia, a gyártás, az egészségügy, a mezőgazdaság és a média.

Az 5G ily módon potenciálisan hatással lesz az uniós polgárok életének csaknem valamennyi aspektusára. Az 5G hálózatok kiberbiztonsága ezért nemcsak gazdaságaink, társadalmaink és demokratikus folyamataink védelme, hanem az összes uniós polgár javát szolgáló megbízható digitális átalakulás biztosítása szempontjából is alapvető fontosságú.

Számos kritikus szolgáltatás 5G hálózatoktól való függése miatt a rendszerszintű és széles körű zavarok következményei különösen súlyosak lennének, és – tekintettel a digitális ökoszisztémák összekapcsolt jellegére – határokon átnyúló, jelentős hatásokkal járnának. Ennek következtében az 5G hálózatok kiberbiztonságának megvalósítása stratégiai fontosságú kérdés az Unió számára egy olyan időszakban, amikor a kibertámadások egyre gyakoribbak és kifinomultabbak, mint valaha, és a fenyegetést jelentő szereplők széles körétől – különösen az EU-n kívüli állami vagy valamely nem uniós állam által támogatott szereplőktől – érkeznek. Ami az olyan kritikus infrastruktúrák biztonságát illeti, mint az 5G, a választott megoldás az, hogy – most első alkalommal – meg kell határozni egy közös európai megközelítést. Ez a megközelítés teljes mértékben tiszteletben tartja az EU belső piacának nyitottságát mindaddig, amíg tiszteletben tartják a kockázatalapú uniós biztonsági követelményeket.

2019. március 22-i ülésén az Európai Tanács az 5G hálózatok biztonságát illetően összehangolt megközelítésre szólított fel. A Bizottság 2019. március 26-án elfogadta az 5G hálózatok kiberbiztonságáról szóló (EU) 2019/534 ajánlást[1]. Az ajánlásban felkérte a tagállamokat, hogy készítsenek nemzeti kockázatértékelést, vizsgálják felül nemzeti intézkedéseiket, valamint hogy uniós szintű együttműködés keretében vegyenek részt az összehangolt kockázatértékelés elvégzésében és dolgozzanak ki egy, a lehetséges kockázatcsökkentő intézkedéseket tartalmazó eszköztárat. Ez a közlemény az Európai Tanács kérésének megfelelően szerves részét képezi a Bizottság átfogó európai digitális stratégiájának.

2. Az 5G bevezetése az EU-ban

Az 5G hálózati infrastruktúra kiépítése Európában központi jelentőségű az európai ipari stratégia és versenyképesség szempontjából. A Bizottság a hálózati technológiák 5. generációjának (5G) kiépítését a jövőbeli digitális szolgáltatások egyik fő elősegítő tényezőjeként ismerte el. A Bizottság 2016-ban elfogadta az 5G cselekvési tervet[2] annak biztosítása érdekében, hogy az Unió 2020-tól rendelkezzen a digitális átalakulásához szükséges hálózati infrastruktúrával, 2025-ig pedig a városi területeken és a fő közlekedési útvonalakon történő átfogó bevezetéshez szükséges hálózati infrastruktúrával. A gigabitalapú

[1] A Bizottság (EU) 2019/534 ajánlása az 5G hálózatok kiberbiztonságáról (HL L 88., 2019.3.29., 42. o.).
[2] COM(2016) 588, 2016. szeptember 14., 5G Európa számára: cselekvési terv.

társadalomról szóló közlemény[3] azt a célt tűzi ki, hogy a mobil adatkapcsolatok mindenhol elérhetőek legyenek, beleértve a vidéki és távoli területeket is.

Ami a frekvenciakiosztást illeti, a tagállamok az 5G úttörő sávok 16 %-át osztották ki[4]. Tekintettel arra a jogi kötelezettségre, hogy az év végéig lehetővé kell tenni valamennyi 5G úttörő sáv használatát, az elkövetkező hónapokban több kiosztási eljárásról is várhatók konzultációk.

Európa a világ egyik legfejlettebb régiója az 5G szolgáltatások kereskedelmi bevezetése tekintetében[5]. A jelenlegi előrejelzések szerint az első 5G szolgáltatások 138 európai városban állnak majd rendelkezésre 2020 végéig. Az első 5G hálózatok a hálózati technológiák jelenlegi 4. generációjára (4G) épülnek, és az 5G szolgáltatások elsősorban vagy a 4G kapacitás és sebesség javításaként, vagy a vezetékes hálózatok költséghatékony vezeték nélküli alternatívájaként állnak a lakosság rendelkezésére[6].

Ami az új, vállalkozások közötti szolgáltatásokban – például az energia-, az élelmiszer- és a mezőgazdasági, az egészségügyi, a feldolgozóipari vagy a közlekedési ágazatban – rejlő lehetőségeket illeti, Európa jól halad a mintegy 1 milliárd EUR összegű beruházással, beleértve a Horizont 2020 égisze alatti 5G köz-magán társulás keretében megvalósuló 300 millió EUR összegű uniós finanszírozást is. Ez a beruházás több mint 160, Európában azonosított nagyszabású 5G tesztelést foglal magában, beleértve tíz, határokon átnyúló autópálya-folyosót az 5G-alapú összekapcsolt és automatizált mobilitási szolgáltatások nagyszabású tesztelésére. A tesztelések kiterjednek a fenntartható egészségügyi ellátástól és az automatizált mobilitástól az erőforrás-hatékony mezőgazdaságon át az intelligens villamosenergia-hálózatokig és az Ipar 4.0-ig a legkülönbözőbb területek 5G-alapú alkalmazásaira. Emellett az EBB az Európai Stratégiai Beruházási Alap támogatásával hiteleket nyújtott az 5G technológiával kapcsolatos kutatás-fejlesztés felgyorsításához.

A 2020. december 21-től alkalmazandó Európai Elektronikus Hírközlési Kódex (a továbbiakban: Kódex)[7] fontos alapot jelent az 5G hálózatok és az azon túlmutató infrastruktúrák beruházásbarát környezetének megteremtéséhez. Emellett az olyan közfinanszírozású programok, mint az Európai Hálózatfinanszírozási Eszköz[8] digitális ága vagy az európai strukturális és beruházási alapok szintén alapvető fontosságúak lesznek az 5G hálózatok jövőbeli kiépítésének támogatása szempontjából, különösen azáltal, hogy a közösségeket összekapcsolják az 5G-alapú szolgáltatásokkal, például az iskolákkal, kórházakkal, városokkal és helyi közigazgatási szervekkel.

[3] COM(2016) 587, 2016. szeptember 14., Az összekapcsoltság a versenyképes digitális egységes piac szolgálatában: Úton a gigabitalapú európai információs társadalom felé.

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Az 5G új funkcióinak egy részét szakaszos megközelítést követve vezetik be. Az első szakaszban (nagyon rövid vagy rövid távon) az 5G kiépítése elsősorban „nem önálló" hálózatokból fog állni, amelyek esetében csak a rádió-hozzáférési hálózatot korszerűsítik az 5G technológiára, és más tekintetben továbbra is a meglévő 4G gerinchálózatokra támaszkodnak, amelyek jobb széles sávú mobilszolgáltatásokat biztosítanak a végfelhasználók számára. Az ezt követő (rövid/közép- és hosszú távú) szakaszokban az „önálló" 5G hálózatok kiépítése – beleértve az 5G gerinchálózati funkciókat is – a hálózati architektúra sokkal szélesebb körű változását teszi szükségessé és fogja eredményezni.

[7] Az Európai Parlament és a Tanács (EU) 2018/1972 irányelve (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról (átdolgozás).

[8] COM(2018) 438, 2018. június 6., Rendeletjavaslat az Európai Hálózatfinanszírozási Eszköz létrehozásáról, valamint az 1316/2013/EU és a 283/2014/EU rendelet hatályon kívül helyezéséről.

Figyelembe véve Európa stratégiai lehetőségeit az 5G szolgáltatások terén a különböző ágazatok esetében, rendkívül fontos, hogy az üzemeltetők és szolgáltatók beruházásai fejlett 5G hálózati és szolgáltatási megoldásokra irányuljanak. Ehhez nemcsak új 5G rádióhálózatokra lesz szükség, hanem új, úgynevezett „önálló” 5G gerinchálózatokra is annak érdekében, hogy olyan fejlett 5G funkciókat biztosítsanak, mint a hálózati szeletelés[9] és a pereminformatikai alkalmazások[10].

A Bizottság továbbra is teljes mértékben támogatni fogja az 5G sikeres bevezetését az EU-ban, többek között azáltal, hogy a tagállamokkal és az érdekelt felekkel együttműködve megragadja az 5G nyújtotta lehetőségeket. Az érintett nemzetközi szervezetekkel és a tudományos közösséggel együttműködve az elővigyázatosság elve alapján kellő figyelmet kell fordítani a releváns egészségügyi szempontokra[11].

3. Az 5G hálózatokon belüli kiberbiztonságra vonatkozó összehangolt uniós kockázatértékelés

A Kiberbiztonsági[12] Együttműködési Csoport keretében együttműködve valamennyi tagállam elvégezte az 5G hálózati infrastruktúráira vonatkozó saját nemzeti kockázatértékelését, és az eredményeket 2019. július elejéig továbbította a Bizottságnak és az Európai Uniós Kiberbiztonsági Ügynökségnek, az ENISA-nak.

E nemzeti kockázatértékelések alapján a tagállamok, a Bizottság és az ENISA képviselőiből álló Kiberbiztonsági Együttműködési Csoport 2019. október 9-én jelentést tett közzé az 5G hálózatok kiberbiztonságára vonatkozó összehangolt uniós kockázatértékelésről[13]. A jelentés azonosítja az 5G hálózatokat érintő főbb fenyegetéseket és a fenyegetést jelentő szereplőket, a legérzékenyebb eszközöket és a főbb sebezhető pontokat (ideértve a technikai jellegű és az egyéb típusú sebezhetőségeket). Ennek alapján a jelentés az uniós szempontból stratégiai jelentőségű kockázatok számos kategóriáját is azonosította, amelyeket konkrét kockázati forgatókönyvek illusztrálnak, és amelyek tükrözik a különböző paraméterek (sebezhetőségek, fenyegetések és a fenyegetést jelentő szereplők) releváns kombinációit a különböző eszközök tekintetében (lásd a függeléket).

A jelentés kiegészítése céljából és az eszköztárhoz való további hozzájárulásként az ENISA elvégezte a fenyegetettségi helyzet célzott feltérképezését[14], amely egyes technikai szempontok – különösen a hálózati eszközök és az azokat érintő fenyegetések – részletes elemzéséből áll.

---

[9] Az 5G hálózati szeletelés lehetővé teszi ugyanazon fizikai hálózat különböző szolgáltatási rétegei közötti nagy fokú elkülönítést, ami növeli a differenciált szolgáltatások nyújtásának lehetőségeit a hálózat egészében.

[10] A pereminformatikai alkalmazások egy elosztott számítási paradigma, amely a válaszidők javítása és a sávszélesség megtakarítása érdekében közelebb hozza a számítást és az adattárolást ahhoz a helyhez, ahol arra szükség van.

[11] A Tanács 1999/519/EK ajánlása (1999. július 12.) a lakosságot érő (0 Hz – 300 GHz közötti) elektromágneses sugárterhelés korlátozásáról.

[12] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (kiberbiztonsági irányelv). A Kiberbiztonsági Együttműködési Csoportot a kiberbiztonsági irányelv hozta létre azzal a céllal, hogy biztosítsa az uniós tagállamok közötti stratégiai együttműködést és információcserét a kiberbiztonság területén.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] Az ENISA 5G hálózatokkal kapcsolatos fenyegetettségi helyzetjelentése: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

Az összehangolt uniós kockázatértékelésről szóló jelentés rávilágít számos, az 5G hálózatok szempontjából fontos szempontra. Ezek a következők:

a) Az 5G által előidézett technológiai változások összességében növelni fogják a támadási felületet és a támadók lehetséges belépési pontjainak számát:

- A jobb hálózatperemi funkcionalitás és a mobilhálózatok korábbi generációihoz képest kevésbé központosított architektúra révén a gerinchálózat egyes funkciói beépíthetők a hálózatok más részeibe, ami érzékenyebbé teszi a megfelelő berendezéseket (pl. bázisállomások vagy MANO-funkciók);

- Az 5G berendezések megnövekedett szoftveraránya növeli a szoftverfejlesztési és -frissítési folyamatokhoz kapcsolódó kockázatokat, új konfigurációs hibák lehetőségét hordozza magában, és emiatt fontosabb szemponttá válik, hogy az egyes mobilhálózat-üzemeltetők a hálózat kiépítési szakaszában a biztonsági elemzésben szereplő opciók közül melyeket választják;

b) Ezen új technológiai jellemzők miatt fokozódni fog a mobilhálózat-üzemeltetők harmadik fél beszállítóktól való függése, és az utóbbiak hangsúlyosabb szerepet fognak betölteni az 5G ellátási láncban.

Ez pedig növelni fogja azoknak a támadási útvonalaknak a számát, amelyeket a fenyegetést jelentő szereplők – különösen az EU-n kívüli állami vagy valamely nem uniós állam által támogatott szereplők – kihasználhatnak, figyelembe véve az uniós tagállamok távközlési hálózatai elleni támadások végrehajtására való képességüket (szándékukat és erőforrásaikat), valamint fokozni fogja az ilyen támadások következményeinek potenciális súlyosságát.

A harmadik fél beszállítók miatt könnyebbé váló támadásoknak való fokozott kitettséggel összefüggésben különösen fontossá válik az egyes beszállítók kockázati profilja, különösen akkor, ha a beszállító jelentős jelenléttel rendelkezik egyes hálózatokban vagy területeken.

c) Az egyetlen beszállítótól való nagy fokú függés növeli az adott beszállító esetleges kieséséből fakadó következményekkel szembeni kitettséget. A nagy fokú függőség súlyosbítja továbbá a gyengeségeknek és sebezhetőségeknek, valamint ezek támadók általi kihasználhatóságának potenciális következményeit, különösen abban az esetben, ha olyan beszállítóról van szó, amely magas szintű kockázatot jelent.

d) Ha az 5G-vel kapcsolatban tervezett új felhasználási forgatókönyvek némelyike megvalósul, az 5G hálózatok végül számos kritikus informatikai alkalmazás ellátási láncának fontos részét fogják képezni, és az nemcsak a titoktartási és adatvédelmi követelményeket fogja érinteni, hanem a hálózatok integritását és rendelkezésre állását érintő jelentős nemzetbiztonsági aggályok is fel fognak merülni, ami uniós szempontból jelentős biztonsági kihívást jelen majd.

Forrás: Összehangolt uniós kockázatértékelés

Az összehangolt uniós kockázatértékelésről szóló jelentés továbbá arra a következtetésre jut, hogy ezek a kihívások új biztonsági paradigmát hoznak létre, ami szükségessé teszi az 5G ágazatra és annak ökoszisztémájára alkalmazandó jelenlegi szakpolitikai és biztonsági keret

újraértékelését, és elengedhetetlenné teszi, hogy a tagállamok meghozzák a szükséges kockázatcsökkentő intézkedéseket.

Az azonosított kockázatok hatékony kezelése, valamint az 5G hálózatok biztonságának és ellenálló képességének megerősítése érdekében átfogó megközelítésre van szükség, ami azt jelenti, hogy olyan kulcsintézkedéseket és kapcsolódó támogató intézkedéseket kell életbe léptetni, amelyek egyszerre képesek kezelni a kockázatokat. Az összehangolt uniós kockázatértékelés alapul szolgált a nemzeti és európai szinten alkalmazható kockázatcsökkentő intézkedések meghatározásához.

2019. december 3-i következtetéseiben[15] a Tanács támogatta az összehangolt kockázatértékelés megállapításait, és hangsúlyozta, hogy „az egységes piac fragmentálódásának elkerülése érdekében fontos az ajánlással kapcsolatos koordinált megközelítés és az ajánlás tényleges végrehajtása". E célból a Tanács felszólította a tagállamokat, a Bizottságot és az ENISA-t, hogy „tegyenek meg a hatáskörükbe tartozó minden szükséges intézkedést az elektronikus hírközlő hálózatok, különösen az 5G hálózatok biztonságának és sérthetetlenségének biztosítása érdekében, továbbá folytassák [...] az 5G technológiákhoz kapcsolódó biztonsági kihívások kezelését célzó összehangolt megközelítés megszilárdítását".

4. Az 5G kiberbiztonsággal kapcsolatos uniós eszköztár

2020. január 29-én a Kiberbiztonsági Együttműködési Csoport közzétette a kockázatcsökkentő intézkedések uniós eszköztárát[16]. Az eszköztár az összehangolt kockázatértékelésről szóló jelentésben azonosított valamennyi kockázatra kitér.

Az uniós eszköztár meghatározza és leírja az azonosított kockázatok csökkentése érdekében bevezetendő stratégiai és technikai intézkedéseket, valamint a hatékonyságuk növelését célzó kapcsolódó támogató intézkedéseket. A **stratégiai intézkedések** a következőket foglalják magukban: a hálózatok beszerzésének és kiépítésének ellenőrzése területén a hatóságok kibővített szabályozói hatáskörével kapcsolatos intézkedések, a nem technikai jellegű sebezhetőségekhez kapcsolódó kockázatok kezelésére irányuló konkrét intézkedések, valamint adott esetben a rendszerszintű, hosszú távú függőségi kockázatok elkerülése érdekében a fenntartható és diverzifikált 5G ellátási és értéklánc előmozdítására irányuló kezdeményezések. A **technikai intézkedések** közé tartoznak az 5G hálózatok és berendezések biztonságának a technológiákból, folyamatokból, emberi és fizikai tényezőkből eredő kockázatok kezelése révén történő megerősítését célzó intézkedések. Az eszköztár ezen túlmenően a leghatékonyabb intézkedéseken alapuló **kockázatcsökkentési terveket** tartalmaz az összehangolt uniós kockázatértékelésben azonosított valamennyi kockázati területre vonatkozóan.

Az uniós eszköztár Kiberbiztonsági Együttműködési Csoport által elfogadott következtetései olyan **kulcsintézkedéseket** javasolnak, amelyeket valamennyi tagállamnak és a Bizottságnak is végre kell hajtania:

[15] A Tanács következtetései – „Az 5G jelentősége az európai gazdaság számára és az 5G-hez kapcsolódó biztonsági kockázatok enyhítésének szükségessége", 14517/19, 2019. december 3., https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/hu/pdf.

[16] Az 5G hálózatok kiberbiztonsága – A kockázatcsökkentő intézkedések uniós eszköztára, 2020. január 29., https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

Az uniós eszköztár következtetései

Az uniós eszköztár számos olyan intézkedést és fellépést határoz meg, amelyek – megfelelő ötvözésük és hatékony végrehajtásuk esetén – az összehangolt megközelítés alapját képezik ezen a területen. Tekintettel az összehangolt uniós kockázatértékelésben azonosított kockázati területek széles körére és eltérő jellegére, nem lesz elegendő egyetlen intézkedéstípus, hanem több, megfelelő kombinációban alkalmazott intézkedés szükséges az összes kulcsfontosságú kockázati terület kezeléséhez.

A lehetséges kockázatcsökkentési tervek értékelése és a leghatékonyabb intézkedések meghatározása alapján ez az eszköztár a következőket ajánlja:

1. Valamennyi tagállamnak gondoskodnia kell arról, hogy meghozza azokat az intézkedéseket (ideértve a nemzeti hatóságok hatáskörére irányulóakat is), amelyek révén megfelelő és arányos módon tud reagálni a már azonosított és a jövőbeli kockázatokra, különösen pedig arról, hogy kockázatalapú megközelítést követve és a biztonsággal kapcsolatos indokok alapján képes legyen az 5G hálózati berendezések szolgáltatását, kiépítését és üzemeltetését korlátozni, megtiltatni és/vagy egyedi követelményekhez vagy feltételekhez kötni.

Különösen a következő feladatokat kell ellátniuk:

- *a mobilhálózat-üzemeltetőkre vonatkozó **biztonsági követelmények** szigorítása (pl. szigorú hozzáférés-ellenőrzés, a biztonságos üzemeltetésre és nyomon követésre vonatkozó szabályok, bizonyos funkciók kiszervezésének korlátozása stb.);*

- *a beszállítók kockázati profiljának értékelése; következésképpen az összehangolt uniós kockázatértékelésben kritikusként és érzékenyként meghatározott **kulcsfontosságú eszközök** (pl. a gerinchálózati funkciók, hálózati MANO-funkciók, valamint a hozzáférési hálózati funkciók) **tekintetében megfelelő korlátozások – többek között a hatékony kockázatcsökkentéshez szükséges kizárások – alkalmazása a magas kockázatúnak tekintett beszállítók esetében**;*

- *annak biztosítása, hogy minden üzemeltető rendelkezzen megfelelő, több forgalmazóra kiterjedő stratégiával az egyetlen beszállítótól (vagy hasonló kockázati profillal rendelkező beszállítóktól) való **nagy fokú függés elkerülése vagy korlátozása** érdekében, a beszállítók közötti megfelelő egyensúly nemzeti szintű biztosítása és **a magas kockázatúnak tekintett beszállítóktól való függés elkerülése**; ehhez az egyetlen beszállító általi vevőfogvatartás-helyzetek elkerülésére is szükség van, többek között a berendezések fokozott interoperabilitásának előmozdítása révén.*

2. Az Európai Bizottságnak a tagállamokkal közösen hozzá kell járulnia a következőkhöz:

- ***diverzifikált és fenntartható 5G ellátási lánc** működtetése a hosszú távú függőség elkerülése érdekében, többek között az alábbiak révén:*

  - *a meglévő uniós alapok és eszközök teljes körű kihasználása, különösen az 5G kulcsfontosságú eszközeit érintő potenciális **közvetlen külföldi befektetések** átvilágításán és az 5G kínálati piacán az esetleges dömpingből vagy támogatásokból eredő **torzulások** elkerülésén keresztül; valamint*

  - *a **az 5G és az 5G utáni technológiákkal kapcsolatos uniós kapacitások** további erősítése a vonatkozó uniós programok és finanszírozás felhasználásával;*

- *a **szabványosítás** terén a tagállamok közötti koordináció elősegítése a konkrét biztonsági célkitűzések teljesítése érdekében, valamint a **vonatkozó uniós szintű tanúsítási rendszer(ek)** kidolgozása a biztonságosabb termékek és folyamatok előmozdítása érdekében.*

3. Annak biztosítása céljából, hogy a szóban forgó összehangolt megközelítés kiállja az idő próbáját, ki kell terjeszteni a Kiberbiztonsági Együttműködési Csoport megbízatását és az egyéb érintett szervekkel és szereplőkkel való együttműködést, különösen az alábbiak érdekében:

- *az 5G hálózatok és az 5G utáni hálózatok biztonságára vonatkozó **nemzeti és uniós kockázatértékelések** rendszeres felülvizsgálata a Bizottság és az ENISA támogatásával, kiegészítve a követett értékelési módszertan továbbfejlesztésével és finomításával, valamint annak a kialakulóban lévő 5G technológiához való hozzáigazításával;*

- *a tagállamok strukturált jelentéstétele alapján **az eszköztár alkalmazásának részletes és rendszeres nyomon követése és értékelése**;*

- *az uniós szintű együttműködést igénylő **támogató intézkedések** végrehajtásának koordinálása és támogatása, különös tekintettel a különböző intézkedésekre vonatkozó iránymutatások kidolgozására és bevált gyakorlatok cseréjére;*

- *adott esetben további uniós szintű koordináció támogatása, különösen **a hálózatüzemeltetőkre vonatkozó műszaki és szervezeti biztonsági követelmények** további közelítése érdekében.*

Forrás: Uniós eszköztár.

Az eszköztár következtetései azt mutatják, hogy a tagállamok határozott szándéka, hogy közösen reagáljanak az 5G hálózatok biztonsági kihívásaira. Ez alapvető fontosságú a tagállamokon és az egész EU-n belüli biztonság, a nemzeti gazdaságok, valamint az EU belső piaca és Európa technológiai szuverenitása szempontjából. Mind az összehangolt uniós kockázatértékelés, mind az uniós eszköztár azt mutatja, hogy a Kiberbiztonsági Együttműködési Csoport keretében a tagállamok, a Bizottság és az ENISA képviselőinek intenzív együttműködésével végzett közös munka nagy értéket képvisel.

Az eszköztár a belső piac egységességének az uniós szakpolitikákkal és koordinációval történő támogatása révén lehetővé teszi az 5G kiberbiztonságra vonatkozó közös uniós megközelítés alkalmazását, ugyanakkor azt is, hogy a tagállamok – különösen a nemzetbiztonság terén – továbbra is gyakorolhassák hatásköreiket. Az eszköztárban foglalt kockázatcsökkentő intézkedések és kockázatcsökkentési tervek lehetővé teszik, hogy az EU megfelelő, hatékony és arányos módon reagáljon a közös 5G kiberbiztonsági kihívásokra.

A Bizottság üdvözli az 5G kiberbiztonsággal kapcsolatos uniós eszköztár közzétételét, és teljes mértékben támogatja annak fenti következtetéseit.

A Bizottság felszólítja a tagállamokat és az érintett uniós intézményeket, ügynökségeket és egyéb szerveket, hogy:

i. az uniós eszköztárral összhangban Unió-szerte biztosítsák a hatékony és megfelelő kockázatcsökkentési stratégiák gyors végrehajtását, és

ii. az intézkedések hatékonyságának és a belső piac zavartalan működésének szavatolása érdekében tegyenek meg minden szükséges további lépést az uniós szintű koordináció biztosítása céljából, többek között a Kiberbiztonsági Együttműködési Csoporton belüli folyamatos munka, valamint az uniós eszköztár alkalmazásának nyomon követésére szolgáló szilárd mechanizmus létrehozása révén.

5. Az eszköztár alkalmazása

Az 5G biztonsággal kapcsolatos hiteles és sikeres európai megközelítéshez elengedhetetlen, hogy a tagállamok elkötelezettek legyenek az eszköztár teljes körű kihasználása mellett. Jóllehet a tagállamok a nemzeti körülmények alapján döntenek egy adott intézkedés megfelelőségéről, elengedhetetlen, hogy **a Kiberbiztonsági Együttműködési Csoport ajánlásának (lásd az eszköztár fenti következtetéseit) megfelelően valamennyi tagállamban, egyes intézkedések esetében pedig uniós szinten kulcsintézkedéseket vezessenek be** az azonosított kockázatok kezelése érdekében.

A Bizottság készen áll arra, hogy a következő szakaszokban továbbra is teljes körű támogatást nyújtson, és felszólítja a tagállamokat, hogy:

2020. április 30-ig tegyenek konkrét és mérhető lépéseket az uniós eszköztár következtetéseiben ajánlott kulcsintézkedések végrehajtására;

2020. június 30-ig a Kiberbiztonsági Együttműködési Csoport keretében állítsanak össze egy jelentést arról, hogy az egyes tagállamokban milyen szakaszban van e kulcsintézkedések végrehajtása, különösen a Kiberbiztonsági Együttműködési Csoport által a Bizottság és az ENISA támogatásával végzett rendszeres jelentéstétel és nyomon követés alapján.

5.1. Kockázatalapú, összehangolt megközelítés az 5G beszállítók tekintetében

Tekintettel arra a végső célkitűzésre, hogy biztosítani kell az 5G hálózatok biztonságát, ellenálló képességét és fenntarthatóságát, a tagállamok egyetértettek abban, hogy értékelni kell az egyes beszállítók kockázati profilját, és ennek szellemében – az eszköztárban foglaltaknak megfelelően – megfelelő korlátozásokat kell alkalmazni a magas kockázatúnak tekintett beszállítók esetében, ideértve a hatékony kockázatcsökkentéshez szükséges kizárásokat is a kulcsfontosságú eszközök tekintetében. A Bizottság kész támogatni a tagállamokat ezen intézkedések végrehajtásában.

Az EU-n belüli végrehajtásuk támogatása érdekében az összehangolt uniós kockázatértékelés és az uniós eszköztár iránymutatást nyújt 1. a beszállítók kockázati profiljának értékelésével[17], valamint 2. a hálózati elemek és funkciók, valamint az egyéb eszközök érzékenységével[18] kapcsolatban. Mind az összehangolt uniós kockázatértékelés, mind az eszköztár intézkedései kiterjednek az 5G hálózati berendezések és hálózati szolgáltatások beszállítóival kapcsolatos kockázatokra. Nem terjednek ki ugyanakkor egyéb olyan termékekre és szolgáltatásokra, amelyeket adott esetben ezek vagy más beszállítók nyújtanak.

Az összehangolt uniós kockázatértékelés 2.37. pontjában meghatározottak szerint az egyes beszállítók kockázati profilja több tényező alapján értékelhető.

A beszállítók kockázati profiljának értékelését kizárólag biztonsági okokból szabad és objektív kritériumok alapján kell elvégezni. Az ezen intézkedések végrehajtására vonatkozó összehangolt megközelítés elősegítése érdekében az eszköztár azt ajánlja, hogy a tagállamok osszák meg egymással a nemzeti megközelítéseikkel és a bevált gyakorlatokkal kapcsolatos információkat. A Bizottság továbbá úgy véli, hogy ennek a fellépésnek a Kiberbiztonsági

[17] Az összehangolt uniós kockázatértékelés 2.37. pontja.

[18] Az összehangolt uniós kockázatértékelés 2.21. pontja bemutatja az elemek és funkciók fő kategóriáit és azok általános érzékenységi szintjét, és felsorol néhány, a tagállamok által az egyes kategóriák tekintetében azonosított kulcsfontosságú elemet, a 2.28. és 2.29. pont pedig az érzékeny eszközök és területek számos egyéb típusát határozza meg (pl. konkrét szervezeteket vagy földrajzi területeket).

Együttműködési Csoport keretében a Bizottsággal és az ENISA-val közösen végzett munka következő szakaszának egyik fő prioritását kell képeznie.

Fontos, hogy a magas kockázatúnak tekintett beszállítókra vonatkozó korlátozásokat – beleértve a hatékony kockázatcsökkentéshez szükséges kizárásokat –, valamint az e beszállítóktól való függőség elkerülését célzó intézkedéseket időben meghatározzák. Ha ez már a legkorábbi szakaszban megtörténik – többek között az 5G frekvenciákra vonatkozó engedélyezési eljárások tekintetében is, amennyiben lehetséges –, az növelni fogja a kiszámíthatóságot a piaci szereplők számára és ezáltal felgyorsítja az 5G hálózatok kiépítését, valamint biztosítja az 5G hálózatok hosszú távú biztonságát és az 5G ellátási lánc ellenálló képességét.

Ugyanakkor ezen intézkedések nemzeti végrehajtása során – amennyiben szükséges és indokolt – eltérő időkeretek is meghatározhatók, különösen abban az esetben, ha a berendezések vagy szolgáltatások igénybevétele az adott pillanatban nagy kockázatot jelentőként értékelt beszállítóktól nagymértékben függ (pl. figyelembe véve a berendezések korszerűsítésének ciklusait, különösen a „nem önálló” 5G hálózatokról az „önálló” 5G hálózatokra való átállást). A tagállamok mérlegelhetik olyan végrehajtási tervek kidolgozását, amelyek megfelelő átmeneti időszakokat tartalmaznak az érintett hálózatüzemeltetők számára. Ebben az összefüggésben az átmeneti időszakokat úgy kell meghatározni, hogy az 5G cselekvési terv[19] célkitűzéseivel összhangban a modern hálózati berendezésekbe – többek között a teljes értékű (önálló) 5G gerinchálózatok kiépítésének felgyorsításába és a hálózatok más részeiben (pl. a rádió-hozzáférési hálózatban) meglévő 4G berendezések lecserélésébe – való beruházás ösztönzői megmaradjanak vagy akár erősödjenek.

Emellett az 5G szoftveralapú hálózatok összetettsége miatt a távközlési szolgáltatók valószínűleg egyre inkább arra kényszerülnek majd, hogy a hálózati berendezések biztosításán túlmenően bizonyos feladatok – például az 5G hálózatok és szoftverek karbantartása és korszerűsítése, valamint egyéb kiszervezett irányítású szolgáltatások – elvégzéséhez is harmadik felekre támaszkodjanak. Az összehangolt uniós kockázatértékelés szerint ez komoly biztonsági kockázatot jelent. Ezért különös figyelmet kell fordítani erre a szempontra. Alapvető fontosságú az e szolgáltatásokkal megbízott beszállítók kockázati profiljának alapos biztonsági értékelése is, különösen akkor, ha ezeket a feladatokat nem az EU-ban végzik. Az 5G infrastruktúra hosszú távú integritásának megőrzése érdekében megfelelő intézkedéseket kell hozni, ideértve különösen az 5G hálózatok érzékeny részeire vonatkozó korlátozások alkalmazását, illetve szükség esetén az eszköztár kockázatcsökkentő intézkedéseivel összhangban a nagy kockázatot jelentő szervezetek kizárását.

5.2. A Bizottság szerepe az eszköztár alkalmazásának támogatásában

A Bizottság továbbra is általános szinten támogatni fogja az 5G kiberbiztonságra vonatkozó uniós megközelítés végrehajtását, valamint konkrét kezdeményezéseket fog tenni az eszköztár intézkedései és célkitűzései tekintetében, amennyiben ez hozzáadott értéket teremthet. A Bizottság az azonosított biztonsági megfontolások kezeléséhez szükséges mértékben lehetőség szerint élni fog hatásköreivel és a vonatkozó eszközökkel. Ezáltal, valamint a tagállamokkal és a magánszektorral együttműködve a Bizottság olyan stratégiai intézkedéseket kíván támogatni, amelyek hozzájárulnak az EU technológiai szuverenitásának

[19] COM(2016) 588, 2016. szeptember 14., 5G Európa számára: cselekvési terv.

és vezető szerepének biztosításához a hálózati technológiák jövőbeli fejlesztése, a kiberbiztonsági technológiák és minden olyan releváns építőelem tekintetében, amelyektől egész gazdaságunk és biztonságunk függ.

Ezen belül a Bizottság a következőket vállalja annak érdekében, hogy biztosítsa az eszköztár megfelelő kockázatcsökkentő intézkedéseinek végrehajtását a hatáskörébe tartozó területeken:

Az 5G hálózatok és a diverzifikált 5G értéklánc kiberbiztonságának védelme:

- **Kiberbiztonsági együttműködés**: a Kiberbiztonsági Együttműködési Csoporton keresztül továbbra is támogatást nyújt a tagállamoknak nemzeti intézkedéseik hatékony, összehangolt és időben történő végrehajtásához.

- **Távközlési és kiberbiztonsági szabályok**: támogatja az eszköztár biztonsági követelményekkel kapcsolatos -intézkedéseinek végrehajtását, különös tekintettel az elektronikus hírközlésre vonatkozó európai szabályok vonatkozó rendelkezéseire, és mérlegeli a technikai és szervezeti biztonsági intézkedéseket részletesen meghatározó lehetséges végrehajtási jogi aktusok hozzáadott értékét a nemzeti szabályok kiegészítése és az üzemeltetőkre vonatkozó biztonsági intézkedések hatékonyságának és következetességének fokozása érdekében.

- **Szabványosítás**: Európa biztonsági és interoperabilitási célkitűzéseinek elérése céljából lépéseket tesz annak érdekében, hogy segítsen fenntartani és szükség esetén növelni az európai részvételt a megfelelő szabványügyi szervekben. Ennek keretében a Bizottság a tagállamokkal együtt értékelni és támogatni fogja különösen azokat a műszaki előírásokat és szabványokat, amelyek lehetővé teszik a hálózat – többek között a hagyományos hálózatok – különböző részeiben használt 5G berendezések beszállítói közötti interoperabilitást annak érdekében, hogy – például nyílt, interoperábilis interfészek révén – valódi több beszállítós környezetet teremtsen.

- **Tanúsítás**: támogatja az 5G hálózatok igényeinek megfelelő 5G tanúsítási rendszerek kidolgozását az EU kiberbiztonsági tanúsítási rendszere keretében.

- **A közvetlen külföldi befektetések átvilágítása**: támogatja az uniós átvilágítási keret végrehajtását azáltal, hogy feltérképezi az 5G értékláncot, beleértve az érzékeny hálózati eszközöket is, és rendszeresen nyomon követi a közvetlen külföldi befektetéseket az értéklánc mentén. A közvetlen külföldi befektetések átvilágítási ütemtervének megfelelően (2020 októberétől) a Bizottság az (EU) 2019/452 rendeletben meghatározott iránymutatásokkal összhangban ellenőrizni fogja a külföldi befektetéseket az 5G területén, figyelembe véve az összehangolt uniós kockázatértékelést és az uniós eszköztárat.

- **Piacvédelmi eszközök**: nyomon követi az EU-ban és a harmadik országokban bekövetkező valamennyi releváns piaci fejleményt, valamint a kereskedelemtorzító gyakorlatok (dömping vagy támogatás) kezelésére irányuló piacvédelmi intézkedésekkel védi az európai 5G piac uniós szereplőit, adott esetben előzetes vizsgálatok indítása révén.

- **Versenyszabályok:** figyelemmel kíséri az 5G hardver- és szoftverellátás piacainak működését annak biztosítása érdekében, hogy azok versenyképes eredményeket produkáljanak, többek között az esetleges szerződéses vagy műszaki függőségi helyzetekkel kapcsolatban.

- **Uniós finanszírozási programok**: biztosítja, hogy a vonatkozó technológiai területeken az uniós finanszírozási programokban való részvételt – a biztonsági feltételek teljes körű kihasználása és K+I-programokba, különösen az Európai horizont kutatási és innovációs keretprogramba, a Digitális Európa programba, az Európai Hálózatfinanszírozási Eszköz 2 programba, az európai strukturális és beruházási alapokba és más idevágó programokba való beépítése révén – a biztonsági követelményeknek való megfeleléshez kössék. Hasonló megközelítést kell alkalmazni az EU külső finanszírozási programjai és pénzügyi eszközei esetében is, többek között a nemzetközi pénzügyi intézményeken keresztül nyújtott finanszírozás tekintetében.

- **Közbeszerzés:** ösztönzi a közbeszerzéseket az 5G hálózatok területén a biztonság, a beszállítók diverzifikációja és az 5G hálózatok hosszú távú fenntarthatósága terén meghatározott célkitűzések támogatására; különösen pedig törekszik annak biztosítására, hogy az 5G hálózatokhoz kapcsolódó közbeszerzési szerződések odaítélésekor az uniós közbeszerzési szabályokkal összhangban kellő figyelmet fordítsanak a biztonsági szempontokra.

- **Eseményekre való reagálás és válságkezelés (tervezet) és kiberbiztonsági gyakorlatok**: teljes körűen kihasználja a nagyszabású kiberbiztonsági eseményekre való összehangolt reagálásról szóló tervezet[20] kidolgozásából eredő lehetőségeket. Továbbá az ENISA-val együtt mérlegeli egy 5G kiberbiztonsági gyakorlat lefolytatásának lehetőségét, amint azt a piac érettsége lehetővé teszi.

Ezen túlmenően az Unió külügyi és biztonságpolitikai főképviselőjének és a Bizottság alelnökének, valamint a Tanácsnak a felelőssége mellett:

- **A rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete („kiberdiplomáciai eszköztár”)[21]**: az EU integritását és biztonságát veszélyeztető rossz szándékú kibertevékenységek esetében a tagállamokat arra ösztönzi, hogy az együttműködés előmozdítása, a fenyegetések enyhítése és a potenciális támadók magatartásának befolyásolása érdekében alkalmazzák az uniós kiberdiplomáciai eszköztár részét képező releváns közös kül- és biztonságpolitikai intézkedéseket (ideértve szükség esetén a korlátozó intézkedéseket is).

Emellett számos program hozzá fog járulni a hosszú távú függőség kockázatának elkerülésére vagy korlátozására irányuló célkitűzések teljesítéséhez azáltal, hogy előmozdítja az 5G piac diverzifikációját és fenntarthatóságát, többek között oly módon, hogy az EU nemzetközi kötelezettségeivel összhangban fenntartja az 5G értékláncban meglévő uniós kapacitásokat és beruház az innovációba.

Az innováció előmozdítása, valamint beruházás a kiberbiztonságba és a hálózati infrastruktúra-technológiákba:

- **Uniós finanszírozási programok**: növeli a hálózati technológiákkal és a releváns építőelemekkel kapcsolatos kutatásba, innovációba és kiépítési tevékenységekbe való beruházások mértékét. A Bizottság a 2021–2027-es időszakra vonatkozó következő uniós

[20] A Bizottság (EU) 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról.
[21] A Tanács 2017. november 20-i következtetései, 9916/17.

költségvetésből közel 3 milliárd euró értékű beruházást javasolt a kiberbiztonsági technológiákba. Ez magában foglalja az Európai horizont égisze alatt végzett kutatást és innovációt, valamint a kiberbiztonsági képességeknek a Digitális Európa program keretében történő támogatását. Az InvestEU program szintén nyújthat pénzügyi támogatást az 5G területén folytatott kutatáshoz és fejlesztéshez, valamint az infrastruktúra kiépítéséhez.

Ezen túlmenően az 5G kiépítésének befejezése és főként a mobiltechnológia következő generációjára, **a 6G-re való felkészülés érdekében** a Bizottság javaslatot tett egy, az újgenerációs internettel/6G-vel (intelligens hálózatokkal és szolgáltatásokkal) kapcsolatos intézményesített uniós partnerség létrehozására a következő Európai horizont program keretében[22], az ágazattal partnerségben és a tagállamokkal együttműködve. Az uniós költségvetésből (2021–2027) több mint 2,5 milliárd EUR összegű uniós beruházást javasolt, amelyhez e kezdeményezés keretében legalább 7,5 milliárd EUR összegű magánbefektetés társulna.

- **Ipari fejlesztés és kiépítés**: értékeli az 5G értékláncon belüli potenciális piaci hiányosságokat és hibákat, amelyek célzott beavatkozásokat indokolnának a következő hosszú távú költségvetés keretében vagy egy esetleges, a kiberbiztonsággal kapcsolatos, közös európai érdeket szolgáló fontos projekt keretében, összhangban a közös európai érdeket szolgáló fontos projekt magas szintű fórumának javaslataival. A közös európai érdeket szolgáló fontos projektek kialakítására és létrehozására vonatkozó döntés a tagállamok és a vállalkozások kezében van. Az uniós szabályok támogató keretet biztosítanak, a Bizottság pedig készen áll arra, hogy megkönnyítse a szükséges kapcsolatok létrejöttét és iránymutatást nyújtson.

[22] Finanszírozás az Európai Hálózatfinanszírozási Eszköz 2 programon és a Digitális Európa programon keresztül is biztosítható.

6. Következtetés

Az 5G hálózatok egy sor lehetőséget teremtenek az európai polgárok, valamint az európai társadalom és gazdaság számára. Az 5G hálózatok biztonságának és ellenálló képességének biztosítása ezért alapvető fontosságú. Ugyanakkor a kiberbiztonsági fenyegetések (ideértve az EU-n kívüli állami vagy valamely nem uniós állam által támogatott szereplők általi beavatkozás kockázatát is) folyamatosan változó kihívást jelentenek, amely a technológiákra és az adatokra való támaszkodás fokozódásával párhuzamosan egyre nagyobb figyelmet követel. A kiberbiztonság elhanyagolása aláásná a digitális gazdaság és társadalom fejlődésébe vetett bizalmat, és megakadályozná, hogy az EU teljes mértékben kihasználja annak előnyeit. Ehhez megfelelő, folyamatosan fejlődő és határozott reakcióra van szükség.

A kritikus technológiák és hálózatok kiberbiztonságának uniós szinten összehangolt és következetes megközelítése elengedhetetlen az EU technológiai szuverenitásának biztosításához, valamint az ipari kapacitások fenntartásához és fejlesztéséhez. A Bizottság teljes mértékben támogatni fogja az 5G hálózatokra vonatkozó uniós kiberbiztonsági megközelítés végrehajtását, miközben biztosítja, hogy az uniós piacok továbbra is nyitottak maradjanak az olyan termékek és szolgáltatások előtt, amelyek megfelelnek a folyamatosan változó kiberbiztonsági és megbízhatósági követelményeknek.

E célból fontos, hogy az 5G biztonságban érintett valamennyi érdekelt fél elkötelezettsége szilárd maradjon, és folyamatos együttműködésre lesz szükség a tagállamok, a Bizottság és az ENISA között.

A fent vázoltaknak megfelelően következő lépésként a Bizottság felszólítja a tagállamokat, hogy tegyenek gyors lépéseket az eszköztár részeként elfogadott intézkedések hatékony és objektív végrehajtása érdekében, és a Bizottság és az ENISA támogatásával folytassák az együttműködést az uniós szintű koordináció biztosítása érdekében. Ezzel párhuzamosan a Bizottság a hatáskörébe tartozó minden releváns intézkedést meg fog hozni annak érdekében, hogy támogassa az eszköztár tagállamok általi alkalmazását és erősítse annak hatását.

Függelék: Kockázati kategóriák (forrás: az összehangolt uniós kockázatértékelés)

	Kockázati kategóriák
Az elégtelen biztonsági intézkedésekkel kapcsolatos kockázati forgatókönyvek	*K1: A hálózatok hibás konfigurációja*
	K2: A hozzáférési ellenőrzések hiánya
Az 5G ellátási lánccal kapcsolatos kockázati forgatókönyvek	*K3: Gyenge termékminőség*
	K4: Az egyes hálózatokon belül egyetlen beszállítótól való függés vagy a diverzifikáció hiánya országos szinten
A fenyegetést jelentő főbb szereplők működési módjával kapcsolatos kockázati forgatókönyvek	*K5: Állami beavatkozás az 5G ellátási láncon keresztül*
	K6: Az 5G hálózatok szervezett bűnözés általi kihasználása vagy a végfelhasználók szervezett bűnözői csoportok általi megcélzása
Az 5G hálózatok és más kritikus rendszerek közötti kölcsönös függőségekkel kapcsolatos kockázati forgatókönyvek	*K7: Jelentős fennakadás a kritikus infrastruktúrákban vagy szolgáltatásokban*
	K8: Súlyos hiba a hálózatokban a villamosenergia-ellátás megszakadása vagy más kiszolgáló rendszerek leállása miatt
A végfelhasználói berendezésekkel kapcsolatos kockázati forgatókönyvek	*K9: A dolgok internetével való visszaélés*