Európai Parlament
2014-2019

ELFOGADOTT SZÖVEGEK

P8_TA(2019)0156

A kínai technológia fokozódó uniós jelenlétéhez kapcsolódó biztonsági fenyegetések és az ezek csökkentésére irányuló lehetséges uniós szintű fellépések

Az Európai Parlament 2019. március 12-i állásfoglalása a kínai technológia fokozódó EU-beli jelenlétéhez kapcsolódó biztonsági fenyegetésekről és az ezek csökkentésére irányuló lehetséges uniós szintű fellépésről (2019/2575(RSP))

Az Európai Parlament,

– tekintettel az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, 2018. december 11-i (EU) 2018/1972 európai parlamenti és tanácsi irányelvre[1],

– tekintettel a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvre[2],

– tekintettel az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelvre[3],

– tekintettel az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló európai parlamenti és tanácsi rendeletre („kiberbiztonsági jogszabályra”) irányuló, 2017. szeptember 13-i bizottsági javaslatra (COM(2017)0477),

– tekintettel az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról szóló rendeletre irányuló, 2018. szeptember 12-i bizottsági javaslatra (COM(2018)0630),

– tekintettel az új nemzeti hírszerzési törvény Kínai Nemzeti Népi Kongresszus általi 2017. június 28-i elfogadására,

---

1 HL L 321., 2018.12.17., 36. o.
2 HL L 194., 2016.7.19., 1. o.
3 HL L 218., 2013.8.14., 8. o.

– tekintettel a Tanács és a Bizottság által a kínai technológia fokozódó EU-beli jelenlétéhez kapcsolódó biztonsági fenyegetésekről és az ezek csökkentésére irányuló lehetséges uniós szintű fellépésről tett 2019. február 13-i nyilatkozatokra,

– tekintettel arra, hogy az ausztrál kormány elfogadta a kormányzati távközlési ágazat biztonsági reformját, amely 2018. szeptember 18-án hatályba lépett,

– tekintettel az Európai Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról szóló, 2019. február 14-én első olvasatban elfogadott álláspontjára[1],

– tekintettel az EU és Kína közötti kapcsolatok helyzetéről szóló korábbi állásfoglalásaira, különösen a 2018. szeptember 12-i állásfoglalására[2],

– tekintettel az „5G Európa számára: cselekvési terv” című, 2016. szeptember 14-i bizottsági közleményre (COM(2016)0588),

– tekintettel „A növekedést, a versenyképességet és a kohéziót célzó internetkapcsolatról: a gigabitalapú európai társadalom és az 5G” című, 2017. június 1-i állásfoglalására[3],

– tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletre[4] (általános adatvédelmi rendelet),

– tekintettel az Európai Hálózatfinanszírozási Eszköz létrehozásáról, a 913/2010/EU rendelet módosításáról és a 680/2007/EK és 67/2010/EK rendelet hatályon kívül helyezéséről szóló, 2013. december 11-i 1316/2013/EU európai parlamenti és tanácsi rendeletre[5],

– tekintettel a Digitális Európa programnak a 2021–2027 közötti időszakra történő létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló, 2018. június 6-i bizottsági javaslatra (COM(2018)0434),

– tekintettel eljárási szabályzata 123. cikkének (2) és (4) bekezdésére,

A. mivel az EU-nak elő kell mozdítania a kiberbiztonsági menetrendjét, hogy kihasználja képességét a kiberbiztonság terén a vezető szerep megszerzésére, és ezt saját iparának előnyére fordítsa;

B. mivel az 5G hálózatok sebezhetősége kihasználható az informatikai rendszerek meggyengítésére, ami rendkívül súlyos károkat okozhat mind az európai és a nemzeti gazdaságoknak; mivel a kockázatok minimálisra csökkentése érdekében a teljes értékláncban kockázatelemzésen alapuló megközelítésre van szükség;

---

1 Elfogadott szövegek, P8_TA(2019)0121.
2 Elfogadott szövegek, P8_TA(2018)0343.
3 HL C 307., 2018.8.30., 144. o.
4 HL L 119., 2016.5.4., 1. o.
5 HL L 348., 2013.12.20., 129. o.

C. mivel az 5G hálózat digitális infrastruktúránk gerincét fogja képezni, bővítve a különböző eszközök hálózathoz csatlakoztatásának (dolgok internete stb.) módjait, és új előnyökkel jár, illetve a társadalom és a vállalkozások számára lehetőségeket teremt számos területen, többek között a gazdaság kritikus fontosságú ágazataiban, például a közlekedési, energetikai, egészségügyi, pénzügyi, távközlési, védelmi, űrtechnológiai és biztonsági ágazatban;

D. mivel a biztonsági kihívások kezelésére szolgáló mechanizmus létrehozása lehetővé tenné az EU számára, hogy aktívan lépéseket tegyen az 5G-re vonatkozó normák meghatározása terén;

E. mivel aggodalmak merültek fel harmadik országbeli berendezésforgalmazókkal kapcsolatban, amelyek származási országuk jogszabályai miatt biztonsági kockázatot jelentenek az EU számára, különösen – a nemzetbiztonság fogalmának meglehetősen tág értelmezésével összefüggésben valamennyi polgárt, vállalatot és egyéb szervet az állambiztonság megőrzése érdekében az állammal való együttműködésre kötelező – kínai állambiztonsági törvények hatálybaléptetése után; mivel nincs garancia arra, hogy e kötelezettségeket nem alkalmazzák az ország területén kívül, és mivel a kínai törvényekre a különböző országok eltérően reagáltak – a biztonsági értékelésektől a teljes körű tilalmak bevezetéséig;

F. mivel 2018 decemberében a kiberbiztonságért felelős cseh nemzeti hatóság figyelmeztetett a Huawei és a ZTE kínai vállalatok által nyújtott technológiák jelentette biztonsági fenyegetésekre; mivel ezt követően, 2019 januárjában a cseh adóhatóság kizárta a Huaweit egy, az adózási portál létrehozására irányuló pályázatból;

G. mivel alapos vizsgálatra van szükség annak tisztázásához, hogy akár az érintett eszközök, akár más eszközök vagy szolgáltatók jelentenek-e biztonsági kockázatot olyan jellemzők miatt, mint például a rendszerekhez vezető hátsó ajtók;

H. mivel a megoldásokat európai uniós szinten kell koordinálni és kezelni, a különféle biztonsági fokozatok kialakításának és az esetleges kiberbiztonsági hiányosságoknak az elkerülése érdekében, a határozott reakcióhoz pedig globális szintű koordináció szükséges;

I. mivel az egységes piac előnyei az európai uniós normáknak és az uniós jogi keretnek való megfelelés kötelezettségével járnak együtt, és mivel a beszállítókat nem szabad származási országuk alapján megkülönböztetett módon kezelni;

J. mivel a közvetlen külföldi beruházások átvilágításáról szóló, 2020 végén hatályba lépő rendelet erősíti a tagállamok azon képességét, hogy biztonsági és közrendi kritériumok alapján átvilágítsák a külföldi befektetéseket, továbbá kialakít egy olyan együttműködési mechanizmust, amelynek köszönhetően a Bizottság és a tagállamok együtt dolgozhatnak a külföldi beruházások jelentette biztonsági – ezen belül kiberbiztonsági – kockázatok felmérésén, és amely olyan, EU-s érdeknek minősülő projektekre és programokra is kiterjed, mint például a transzeurópai távközlési hálózatok és a Horizont 2020;

1. úgy véli, hogy az Uniónak vezető szerepet kell vállalnia a kiberbiztonság terén az európai uniós, tagállami és ipari szakértelem hatékony és eredményes kihasználásán

alapuló közös megközelítés révén, minthogy az egymástól eltérő nemzeti határozatok sokfélesége ártana a digitális egységes piacnak;

2. mélységes aggodalmának ad hangot azon közelmúltbeli állítások miatt, amelyek szerint a kínai vállalatok által kifejlesztett 5G berendezésekben beépített hátsó ajtók vannak, amelyek lehetővé teszik a gyártók és a hatóságok számára az európai uniós magán- és személyes adatokhoz, illetve a távközléshez való jogtalan hozzáférést;

3. hasonlóképpen aggodalmát fejezi ki az említett gyártók által kifejlesztett 5G berendezések esetleges komoly hiányosságai miatt, amennyiben e berendezéseket az elkövetkező években az 5G hálózatok kiépítésekor üzembe helyezik;

4. hangsúlyozza, hogy a hálózatok és berendezések biztonságával kapcsolatos következmények világszerte hasonlóak, és kéri az Uniót, hogy vonja le a rendelkezésre álló tapasztalatok tanulságait annak érdekében, hogy a legmagasabb színvonalú kiberbiztonságot tudja biztosítani; felhívja a Bizottságot egy olyan stratégia kidolgozására, amely vezető pozícióba helyezi Európát a kiberbiztonsági technológiák terén, és amely Európa külső technológiáktól való függőségének mérséklését tűzi ki célul a kiberbiztonság területén; úgy véli, hogy megfelelő intézkedéseket kell alkalmazni minden olyan esetben, amikor a biztonsági követelményeknek való megfelelés nem garantálható;

5. felhívja a tagállamokat, hogy a legmagasabb színvonalú kiberbiztonság egész Unióban történő biztosítása céljából, az Unió válaszlépéseinek koordinálása érdekében tájékoztassák a Bizottságot minden olyan nemzeti intézkedésről, amelyet elfogadni szándékoznak, és ismételten hangsúlyozza, hogy fontos tartózkodni az aránytalan, egyoldalú, az egységes piac széttagoltságát eredményező lépésektől;

6. megismétli, hogy minden, az Unióban berendezéseket vagy szolgáltatásokat nyújtó szervezet származási helyétől függetlenül eleget kell tennie az alapvető jogokkal összefüggő kötelezettségeknek, valamint az Unió és a tagállamok jogszabályainak, ezen belül a magánélet védelmére, az adatvédelemre és a kiberbiztonságra vonatkozó jogi keretnek;

7. felhívja a Bizottságot, hogy végezze el az Unió jogi keretrendszerének értékelését a stratégiai ágazatokban és a gerinchálózati infrastruktúrában található sebezhető berendezésekkel kapcsolatos aggályok kezelése érdekében; sürgeti a Bizottságot, hogy terjesszen elő kezdeményezéseket, adott esetben jogalkotási javaslatokat is, az észlelt hiányosságok időben történő megválaszolása érdekében, miután a kiberbiztonsági kihívások számbavétele és megválaszolásuk, valamint az EU kibertámadásokkal szembeni ellenálló képességének erősítése soha véget nem érő folyamat az Unió számára;

8. sürgeti azokat a tagállamokat, amelyek még nem ültették át teljes mértékben a kiberbiztonsági irányelvet, hogy késedelem nélkül tegyék ezt meg, és felhívja a Bizottságot, hogy szorosan kövesse nyomon az átültetést annak biztosítása érdekében, hogy az irányelv rendelkezései megfelelő módon alkalmazhatók legyenek és érvényre jussanak, és az európai polgárok nagyobb védelemben részesüljenek a külső és belső biztonsági fenyegetésekkel szemben;

9. sürgeti a Bizottságot és a tagállamokat, hogy gondoskodjanak a kiberbiztonsági irányelvben bevezetett jelentéstételi mechanizmusok megfelelő alkalmazásáról; megállapítja, hogy az észlelt rések kezelése érdekében a Bizottságnak és a tagállamoknak szorosan nyomon kell követniük minden biztonsági incidenst vagy a szolgáltatók minden nem megfelelő reagálását;

10. felhívja a Bizottságot, hogy mérje fel az irányelv hatálya más, ágazatspecifikus jogszabály hatálya alá nem tartozó kritikus ágazatokra és szolgáltatásokra való további kiterjesztésének szükségességét;

11. üdvözli és támogatja kiberbiztonsági jogszabállyal kapcsolatban elért megállapodást, valamint az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) mandátumának megerősítését a kiberbiztonsági fenyegetések és támadások elhárítása terén a tagállamoknak nyújtott támogatás javítása érdekében;

12. sürgeti a Bizottságot, hogy bízza meg az ENISA-t az 5G-berendezésekre vonatkozó tanúsítási rendszer prioritásként történő kidolgozásával annak biztosítása érdekében, hogy az 5G Unióban történő bevezetése megfeleljen a legszigorúbb biztonsági normáknak, és ellenálló legyen a hátsó ajtókkal vagy nagyobb sebezhetőségekkel szemben, amelyek veszélyeztetnék az Unió távközlési hálózatainak és arra támaszkodó szolgáltatásainak biztonságát; javasolja, hogy fordítsanak külön figyelmet a széles körben használt folyamatokra, termékekre és szoftverekre, amelyek pusztán nagyságrendjük miatt jelentős hatást gyakorolnak az állampolgárok és a gazdaság mindennapi életére;

13. melegen üdvözli a kiberbiztonsági kompetenciaközpontok és a digitális egységes piac biztonságához szükséges uniós kiberbiztonsági technológiai és ipari kapacitások megőrzésének és fejlesztésének elősegítése céljából kialakított nemzeti koordinációs központok létrehozására irányuló javaslatokat; emlékeztet azonban arra, hogy a tanúsítás nem zárja ki, hogy az illetékes hatóságok és a gazdasági szereplők ellenőrizzék az ellátási láncot annak érdekében, hogy biztosítsák a kritikus környezetben és a távközlési hálózatokon működő eszközeik sértetlenségét és biztonságát;

14. emlékeztet arra, hogy az eredményes kiberbiztonság szigorú biztonsági normákat követel; kéri egy alapértelmezetten és beépítetten biztonságos hálózat létrehozását; sürgeti a tagállamokat, hogy a Bizottsággal együttesen tárják fel mindazon eszközöket, amelyek rendelkezésre állnak a magas szintű biztonság szavatolása érdekében;

15. felhívja a Bizottságot, hogy az ENISA-val együttműködésben adjon iránymutatást arra vonatkozóan, hogy miként lehet kezelni a kiberfenyegetéseket és -sebezhetőségeket az 5G berendezések beszerzése során pl. a különböző forgalmazók berendezéseinek diverzifikálása vagy a többfázisú közbeszerzési eljárások kialakítása révén;

16. megerősíti álláspontját a Digitális Európa programmal kapcsolatban, amely biztonsági követelményeket vezet be, és előírja az Unióban székhellyel rendelkező, de harmadik országokból irányított szervezetek Bizottság általi felügyeletét, különösen a kiberbiztonsággal összefüggő tevékenységekkel kapcsolatban;

17. felhívja a tagállamokat annak biztosítására, hogy a kritikus hálózati infrastruktúrák – például távközlés, energia, egészségügyi és szociális rendszerek – megfelelő működésének biztosításában részt vevő állami intézmények és magánvállalatok

végezzenek megfelelő kockázatelemzési értékelést, figyelembe véve az adott rendszer műszaki jellemzőihez vagy a hardver- vagy szoftvertechnológiák külső szállítóitól való függőséghez kapcsolódó sajátos biztonsági fenyegetéseket;

18. emlékeztet arra, hogy a telekommunikáció jelenlegi jogi kerete a tagállamokra bízza annak biztosítását, hogy a távközlési szolgáltatók tiszteletben tartsák a nyilvános elektronikus hírközlő hálózatok integritását és rendelkezésre állását, beleértve adott esteben a végponttól végpontig terjedő titkosítást; kiemeli, hogy az Európai Elektronikus Hírközlési Kódexnek megfelelően a tagállamok kiterjedt hatáskörrel rendelkeznek a vizsgálatok lefolytatására és jogorvoslati lehetőségek széles körének alkalmazására az EU piacán található termékek meg nem felelése esetén;

19. felhívja a Bizottságot és a tagállamokat, hogy uniós és nemzeti szinten egyaránt tegyék kötelező szemponttá a biztonságot minden érintett infrastruktúrára vonatkozó közbeszerzési eljárásban;

20. emlékezteti a tagállamokat az uniós jogi keret – az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv – értelmében fennálló azon kötelezettségükre, hogy szankciókat szabjanak ki azokra a jogi személyekre, amelyek bűncselekményt, például ilyen rendszerek elleni támadást követtek el; hangsúlyozza, hogy a tagállamoknak élniük kell azzal a lehetőségükkel, hogy más szankciókat – például a kereskedelmi tevékenységek folytatásától való ideiglenes vagy állandó eltiltást – is alkalmazzanak e jogi személyekkel szemben;

21. felhívja a tagállamokat, a kiberbiztonsági ügynökségeket, a távközlési szolgáltatókat, a kritikus infrastruktúra-szolgáltatások gyártóit és szolgáltatóit, hogy jelentsék be a Bizottságnak és az ENISA-nak a távközlési hálózatok integritását és biztonságát veszélyeztető, illetve az uniós jogot és az alapvető jogokat sértő hátsó ajtók vagy más jelentős sebezhetőségek bizonyítékait; elvárja a nemzeti adatvédelmi hatóságoktól, valamint az európai adatvédelmi biztostól a külső szolgáltatók által elkövetett, személyes adatokkal kapcsolatos adatvédelmi incidensek alapos kivizsgálását és a megfelelő szankciók európai adatvédelmi jogszabályokkal összhangban történő kiszabását;

22. a biztonság és a közrend szempontjából üdvözli a közvetlen külföldi befektetések átvilágítási keretének létrehozásáról szóló rendelet közelgő hatálybalépését, és hangsúlyozza, hogy ez a rendelet az első, amely felsorolja a biztonság és a közrend szempontjából uniós szinten lényeges területeket és tényezőket, többek között a távközlést és a kiberbiztonságot;

23. felhívja a Tanácsot, hogy gyorsítsa fel a javasolt elektronikus adatvédelmi rendelettel kapcsolatos munkáját;

24. ismételten hangsúlyozza, hogy az EU-nak támogatnia kell a kiberbiztonság magasabb szintre emelését a teljes értéklánc mentén, a kutatástól a kulcsfontosságú technológiák bevezetéséig és elterjesztéséig, terjesztenie kell a vonatkozó információkat, és elő kell mozdítania a kiberhigiéniát és a kiberbiztonságot is magukban foglaló tanterveket, továbbá úgy véli, hogy a Digitális Európa program ennek hatékony eszköze lesz;

25. sürgeti a Bizottságot és a tagállamokat, hogy tegyék meg a szükséges lépéseket – többek között erőteljes beruházási rendszerek révén – egy olyan innovációbarát

környezet kialakítására az Unión belül, amely az EU digitális gazdaságának valamennyi vállalkozása, többek között a kis- és középvállalkozások (kkv-k) számára is hozzáférhető; szorgalmazza továbbá, hogy ez a környezet tegye lehetővé az európai szolgáltatók számára a versenyképességüket elősegítő új termékek, szolgáltatások és technológiák kifejlesztését;

26. felkéri a Bizottságot, hogy az EU–Kína stratégiával kapcsolatos soron következő megbeszélések során tartsa szem előtt a fenti kéréseket mint annak előfeltételeit, hogy az EU versenyképes maradjon, és szavatolva legyen digitális infrastruktúrájának biztonsága;

27. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a Tanácsnak és a Bizottságnak.