Eiropas Parlaments
2014-2019

Sesijas dokuments

B8-0153/2019

6.3.2019

REZOLŪCIJAS PRIEKŠLIKUMS

iesniegts, noslēdzot debates par Padomes un Komisijas paziņojumiem

iesniegts saskaņā ar Reglamenta 123. panta 2. punktu,

par apdraudējumu drošībai saistībā ar pieaugošo Ķīnas tehnoloģiju klātbūtni ES un iespējamo rīcību ES līmenī, lai to samazinātu
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
EFDD grupas vārdā

B8-0153/2019

Eiropas Parlamenta rezolūcija par apdraudējumu drošībai saistībā ar pieaugošo Ķīnas tehnoloģiju klātbūtni ES un iespējamo rīcību ES līmenī, lai to samazinātu (2019/2575(RSP))

Eiropas Parlaments,

– ņemot vērā Komisijas 2016. gada 14. septembra paziņojumu „Konkurētspējīga digitālā vienotā tirgus savienojamība. Virzība uz Eiropas Gigabitu sabiedrību” (COM(2016)0587) un „5G Eiropai. Rīcības plāns” (COM(2016)0588),

– ņemot vērā Komisijas 2016. gada 29. janvāra grozīto priekšlikumu Eiropas Parlamenta un Padomes regulai par trešo valstu preču un pakalpojumu piekļuvi Savienības publiskā iepirkuma iekšējam tirgum un par procedūrām, kas atbalsta sarunas par Savienības preču un pakalpojumu piekļuvi trešo valstu publiskā iepirkuma tirgiem (COM(2016)0034),

– ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā[1] (Kiberdrošības direktīva),

– ņemot vērā priekšlikumu Eiropas Parlamenta un Padomes regulai par *ENISA* — ES Kiberdrošības aģentūru — un Regulas (ES) Nr. 526/2013 atcelšanu, un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju („Kiberdrošības akts”) (COM(2017)0477),

– ņemot vērā Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīvu (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi[2],

– ņemot vērā Komisijas 2018. gada 12. septembra priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (COM(2018)0630),

– ņemot vērā PTO 2018. gada 1. jūnija strīdu izšķiršanas lietu (WT/DS549/6) par dažiem Ķīnas noteiktajiem pasākumiem, kas attiecas uz ārvalstu tehnoloģiju nodošanu Ķīnai,

– ņemot vērā Parlamenta 2019. gada 14. februārī pirmajā lasījumā pieņemto nostāju par priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko izveido satvaru ārvalstu tiešo ieguldījumu Eiropas Savienībā izvērtēšanai[3],

– ņemot vērā pašreizējās sarunas starp ES un Ķīnu par visaptverošu nolīgumu par ieguldījumiem,

[1] OV L 194, 19.7.2016., 1. lpp.
[2] OV L 321, 17.12.2018., 36. lpp.
[3] Pieņemtie teksti, P8_TA(2019)0121.

– ņemot vērā Reglamenta 123. panta 2. punktu,

A. tā kā nesenie sasniegumi IKT, tostarp sasniegumi piektās paaudzes telekomunikāciju (5G) izstrādē, ir radījuši jaunus veidus preču un pakalpojumu ražošanai, izplatīšanai un īstenošanai, kā arī mijiedarbībai ierīču starpā un mijiedarbībai iedzīvotāju, valsts pārvaldes iestāžu un citu sociāli ekonomisko dalībnieku starpā, un tādējādi šīm tehnoloģijām ir potenciāls veicināt Eiropas ekonomiku;

B. tā kā kiberdrošība attiecībā uz IKT, sensitīvas informācijas aizsardzība, individuālo tiesību ievērošana un aizsardzība pret ārējiem kiberdraudiem ir priekšnosacījumi ES pilsoņu tehnoloģiskās suverenitātes nodrošināšanai un, visbeidzot, nes labklājību ES un atbalsta demokrātiju tajā;

C. tā kā 5G pētniecība un testēšana ar grūtībām var izturēt starptautisko spiedienu 5G ieviešanai un komercializācijai, savukārt vairāki zinātniski pētījumi ir izraisījuši bažas un neskaidrības gan attiecībā uz to drošību, gan drošumu, jo īpaši saistībā ar elektromagnētiskā piesārņojuma risku cilvēku veselībai un videi;

D. tā kā kiberdrošības garantēšana attiecībā uz 5G tīkliem ir jauna un sarežģīta problēma, ko rada 5G virtualizētais un decentralizētais raksturs un to sadrumstalotā un ļoti specializētā pievienotās vērtības veidošanas ķēde no ražošanas līdz nosūtīšanai, uzstādīšanai, konfigurācijai, ekspluatācijai, tehniskajai apkopei un programmatūras atjaunināšanai; tā kā ES ir jānovērš kiberdrošības nepilnības ES kritiskajā infrastruktūrā, cita starpā, telekomunikāciju, enerģētikas, transporta, veselības aizsardzības, aizsardzības un drošības nozarēs;

E. tā kā drošu 5G tīklu garantēšana ir uzdevums, ko nevar veikt atsevišķi ražotāji vai sistēmas operatori, bet ir vajadzīga visu attiecīgo valsts un starptautisko iestāžu efektīva koordinēta rīcība;

F. tā kā ES ir potenciāls vadīt kiberdrošības tehnoloģiju izstrādi, atbalstot Eiropas uzņēmumus šajā nozarē un veicinot visas tādas pārmaiņas pievienotās vērtības veidošanas ķēdē, kas varētu mazināt ES atkarību no ārvalstu tehnoloģijām;

G. tā kā ES, lai garantētu kiberdrošību, ir izstrādājusi pasākumu kopumu, tostarp Kiberdrošības direktīvu un Kiberdrošības aktu, kas būtu ātri jāīsteno un pastāvīgi jāuzrauga, lai, veicot nepieciešamos atjauninājumus un pārskatīšanas, nodrošinātu, ka tie joprojām ir efektīvi;

H. tā kā ES 5G tirgū ir kļuvusi redzama lielāka Ķīnas un citu trešo valstu tehnoloģiju piedāvātāju klātbūtne, jo īpaši attiecībā uz valsts uzņēmumiem vai uzņēmumiem, kuros trūkst pārredzamības;

I. tā kā savstarpīgums ir viens no efektīvākajiem veidiem, kā panākt vienlīdzīgus konkurences apstākļus globālā līmenī;

J. tā kā ārvalstu uzņēmumiem ir jārisina jautājums saistībā ar pašreizējo neatbilstību ES datu aizsardzības standartos, kas vērojama starp Vispārīgo datu aizsardzības regulu un dažādām prasībām saskaņā ar valstu tiesību aktiem;

K. tā kā kopš 2013. gada notiek sarunas starp ES un Ķīnu par visaptverošu nolīgumu par ieguldījumiem; tā kā ierosinātais nolīgums palīdzētu atrisināt problēmas saistībā ar piekļuvi tirgum, izveidotu satvaru ieguldījumu aizsardzībai un noteiktu darba un vides pamatstandartus;

L. tā kā pierādījumi, kaut arī nepārliecinoši, ir radušies saistībā ar trūkumiem attiecībā uz to iekārtu drošību, kas piegādātas no trešām valstīm, tostarp Ķīnas, un kas varētu apdraudēt individuālās tiesības uz privātumu un sensitīvas informācijas aizsardzību ES,

1. uzsver, ka 5G ieviešana un komercializācija būtu jāveic saskaņā ar piesardzības principu, ņemot vērā visu sociālekonomisko dalībnieku viedokli attiecībā uz drošumu un drošību un veicot samērīgus piesardzības pasākumus, tostarp tūlītēju informācijas atklāšanu par faktoriem, kas var apdraudēt sabiedrības veselību vai vidi;

2. uzsver, ka būtu rūpīgi jāizvērtē 5G, kā arī tehnoloģijas, ko tā nodrošina, — no lietiskā interneta līdz mākslīgajam intelektam — sociālā un ekonomiskā ietekme un ka būtu jāveic pasākumi, lai pāreja uz Eiropas Gigabitu sabiedrību notiktu taisnīgi un vienlīdzīgi attiecībā pret visiem, kā arī pamatojoties uz ētisku atbildību;

3. aicina Komisiju un dalībvalstis izveidot inovācijai labvēlīgu vidi ES piegādātājiem, lai tie varētu izstrādāt jaunus produktus, pakalpojumus un tehnoloģijas, un atbalstīt ES uzņēmējdarbību drošu 5G ieviešanā un komercializācijā, vienlaikus nodrošinot, ka to potenciāls ir pieejams visiem uzņēmumiem ES digitālajā ekonomikā, tostarp maziem un vidējiem uzņēmumiem;

4. atgādina, ka kiberdrošības garantēšana ir viens no galvenajiem uzdevumiem, kas pašlaik jāveic ES, un ka neveiksme šajā jomā varētu negatīvi ietekmēt ES patērētāju un ražotāju tiesības uz privātumu un pamattiesības, nopietni mazināt iedzīvotāju uzticēšanos IKT produktiem un pakalpojumiem un galu galā radīt nopietnu ekonomisku kaitējumu; prasa izveidot tīklu, kas atbilst principiem „drošs atbilstoši iestatījumam” un „tehniski drošs”;

5. aicina Komisiju un dalībvalstis cieši sadarboties, īstenojot ES kiberdrošības stratēģiju, un apvienot ES un valstu pasākumus, lai mazinātu drošības noteikumu pārkāpšanas risku un datu aizsardzības pārkāpumus visā pievienotās vērtības veidošanas ķēdē; uzskata, ka šādi pasākumi varētu ietvert ES kiberdrošības sertifikāciju, konfigurācijas prasības un darbības procedūras un praksi, kā arī kiberhigiēnas un digitālās izglītības veicināšanu;

6. uzskata, ka ES kiberdrošības aģentūrai (Eiropas Savienības Tīklu un informācijas drošības aģentūrai — *ENISA*) ir izšķiroša nozīme, analizējot iespējamos draudus, ko rada ārvalstu tirgotāji, tostarp Ķīna, un koordinējot kopīgu pieeju starp dalībvalstīm, lai novērstu kiberdrošības apdraudējumus un uzbrukumus tai;

7. aicina Komisiju un dalībvalstis strauji īstenot aprites ekonomikas tiesību aktu kopumu un visā izejvielu aprites ciklā veicināt to pārvaldību, kā arī atkritumu pārstrādi, lai uzlabotu ES piekļuvi kritiski svarīgām izejvielām, kas ir būtiskas augsto tehnoloģiju produktiem un jaunām inovācijām;

8. uzskata, ka, izmantojot vienotu pieeju drošībai un datu aizsardzībai starp dalībvalstīm, ir steidzami jārisina iespējamie tehnoloģiskās drošības apdraudējumi, ko rada pašreizējo

ārvalstu tirgotāju, tostarp Ķīnas, iespiešanās ES tirgū;

9. aicina Komisiju un dalībvalstis analizēt un uzraudzīt to IKT sistēmu drošību, kurās trešo valstu tehnoloģijas ir spēcīgi pārstāvētas, veicot arī stresa testus;

10. uzsver, ka trešo valstu piegādātājus nedrīkst diskriminēt to izcelsmes valsts dēļ, bet, lai nodrošinātu vienlīdzīgus konkurences apstākļus, būtu jāņem vērā šo uzņēmumu pārredzamība, to kiberdrošības standarti un apstāklis, ka tādi paši nosacījumi ir paredzēti Eiropas uzņēmumiem ārvalstu uzņēmumu izcelsmes valstī;

11. uzsver, ka Ķīnas vai citu trešo valstu piegādātāji un operatori nekādā gadījumā nedrīkst apdraudēt individuālās tiesības, kas garantētas ES tiesību aktos, pat ja to izcelsmes valstī pastāv atšķirīgas prasības saskaņā ar valsts tiesību aktiem;

12. aicina Padomi pozitīvā gaisotnē apsvērt sarunu atsākšanu par jauno pārskatīto Komisijas priekšlikumu par procedūru, ar kuru ierobežo ārvalstu produktu piekļuvi ES publiskā iepirkuma tirgum, ja nav savstarpējas pievienošanās;

13. atgādina, cik svarīgi ir turpināt uzlabot sarunas par regulatīvo sadarbību digitālās tehnoloģijas jomā ar trešām valstīm un nodrošināt lielāku līdzdalību starptautiskajās standartu noteikšanas struktūrās;

14. uzdod priekšsēdētājam šo rezolūciju nosūtīt Padomei un Komisijai.