Eiropas Parlaments
2014-2019

PIEŅEMTIE TEKSTI

P8_TA(2019)0156

Drošības apdraudējumi saistībā ar aizvien lielāko Ķīnas tehnoloģiju klātbūtni ES un iespējama rīcība ES līmenī to mazināšanai

Eiropas Parlamenta 2019. gada 12. marta rezolūcija par drošības apdraudējumiem saistībā ar aizvien lielāko Ķīnas tehnoloģiju klātbūtni ES un iespējamo rīcību ES līmenī to mazināšanai (2019/2575(RSP))

Eiropas Parlaments,

– ņemot vērā Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīvu (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi[1],

– 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[2],

– ņemot vērā Eiropas Parlamenta un Padomes 2013. gada 12. augusta Direktīvu 2013/40/ES par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI[3],

– ņemot vērā Komisijas 2017. gada 13. septembra 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 Komisijas 2018. gada 12. septembra priekšlikumu regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (COM(2018)0630),

– ņemot vērā to, ka Ķīnas Nacionālā tautas kongresa Pastāvīgā komiteja 2017. gada 28. jūnijā pieņēma jauno nacionālās izlūkošanas likumu,

– ņemot vērā Padomes un Komisijas 2019. gada 13. februāra paziņojumus par drošības apdraudējumiem saistībā ar aizvien lielāko Ķīnas tehnoloģiju klātbūtni ES un iespējamu

---

1 OV L 321, 17.12.2018., 36. lpp.
2 OV L 194, 19.7.2016., 1. lpp.
3 OV L 218, 14.8.2013., 8. lpp.

rīcību ES līmenī to mazināšanai,

– ņemot vērā to, ka Austrālijas valdība apstiprināja valdības telekomunikāciju nozares drošības reformas, kas stājās spēkā 2018. gada 18. septembrī,

– ņemot vērā 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[1],

– ņemot vērā iepriekšējās rezolūcijas par stāvokli ES un Ķīnas attiecībās, jo īpaši 2018. gada 12. septembra rezolūciju[2],

– ņemot vērā Komisijas 2016. gada 14. septembra paziņojumu „5G Eiropai. Rīcības plāns” (COM(2016)0588),

– ņemot vērā Parlamenta 2017. gada 1. jūnija rezolūciju par interneta savienojamību izaugsmei, konkurētspējai un kohēzijai: Eiropas gigabitu sabiedrība un 5G[3];

– ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)[4],

– ņemot vērā Eiropas Parlamenta un Padomes 2013. gada 11. decembra Regulu (ES) Nr. 1316/2013, ar ko izveido Eiropas infrastruktūras savienošanas instrumentu, groza Regulu (ES) Nr. 913/2010 un atceļ Regulu (EK) Nr. 680/2007 un Regulu (EK) Nr. 67/2010[5],

– ņemot vērā Komisijas 2018. gada 6. jūnija priekšlikumu Eiropas Parlamenta un Padomes regulai, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu (COM(2018)0434),

– ņemot vērā Reglamenta 123. panta 2. un 4. punktu,

A. tā kā ES ir jāturpina īstenot savu kiberdrošības programmu, lai tā varētu realizēt savu potenciālu kļūt par vadošo dalībnieku kiberdrošības jomā un izmantot to savas nozares stiprināšanai;

B. tā kā 5G tīklu trūkumi varētu tikt izmantoti, lai apdraudētu IT sistēmas, un tas varētu radīt ļoti nopietnu kaitējumu ekonomikai gan Eiropas, gan valstu līmenī; tā kā, lai samazinātu riskus, visā pievienotās vērtības veidošanas ķēdē ir nepieciešama pieeja, kas paredz risku mazināšanu;

C. tā kā 5G tīkls kļūs par mūsu digitālās infrastruktūras pamatu, paplašinot iespēju savienot tīklā dažādas ierīces (lietu internets, utt.) un daudzās jomās radīs jaunus ieguvumus un iespējas sabiedrībai un uzņēmumiem, tostarp tādās svarīgās tautsaimniecības nozarēs

---

1 Pieņemtie teksti, P8_TA(2019)0121.
2 Pieņemtie teksti, P8_TA(2018)0343.
3 OV C 307, 30.8.2018., 144. lpp.
4 OV L 119, 4.5.2016., 1. lpp.
5 OV L 348, 20.12.2013., 129. lpp.

kā, piemēram, transports, enerģētika, veselība, finanses, telesakari, aizsardzība, kosmoss un drošība;

D. tā kā piemērota mehānisma izveide, lai risinātu drošības problēmas, dotu ES iespēju aktīvi rīkoties, nosakot standartus 5G jomā;

E. tā kā tika paustas bažas par trešo valstu aprīkojuma tirgotājiem, kas varētu radīt drošības risku ES to izcelsmes valstu tiesību aktu dēļ, jo īpaši pēc tam, kad ir stājušies spēkā Ķīnas valsts drošības likumi, kas paredz pienākumu visiem pilsoņiem, uzņēmumiem un citām struktūrām sadarboties ar valsti, lai nodrošinātu valsts drošību ļoti plašā interpretācijā; tā kā nav garantijas, ka šādi pienākumi netiek piemēroti eksteritoriāli, un tā kā vairākās valstīs reakcija uz minētajiem Ķīnas tiesību aktiem ir atšķirīga, sākot no drošības novērtējumiem līdz pilnīgam aizliegumam;

F. tā kā 2018. gada decembrī Čehijas Valsts kiberdrošības iestāde brīdināja par drošības apdraudējumu, ko rada Ķīnas uzņēmumu *Huawei* un *ZTE* piedāvātās tehnoloģijas; tā kā, ņemot to vērā, Čehijas nodokļu iestādes 2019. gada janvārī neļāva *Huawei* piedalīties konkursā par nodokļu portāla izveidi;

G. tā kā ir nepieciešama rūpīga izpēte, lai noskaidrotu, vai iesaistītās ierīces vai jebkuras citas ierīces vai piegādātāji nerada drošības riskus tādu iezīmju dēļ kā, piemēram, sistēmā iebūvētas iegultās lūkas;

H. tā kā risinājumi būtu jākoordinē un jāpārvalda ES līmenī, lai izvairītos no dažādu drošības līmeņu un potenciālo kiberdrošības trūkumu rašanās, vienlaicīgi atzīstot, ka ir nepieciešama koordinācija globālā līmenī, lai nodrošinātu nepārprotamu reaģēšanu;

I. tā kā priekšrocības, ko sniedz vienotais tirgus, ir saistītas ar pienākumu ievērot ES standartus un Savienības tiesisko regulējumu, un tā kā attieksmei pret piegādātājiem nevajadzētu būt atšķirīgai atkarībā no to izcelsmes valsts;

J. tā kā regula par ārvalstu tiešo ieguldījumu izvērtēšanu, kam būtu jāstājas spēkā līdz 2020. gada beigām, nostiprina dalībvalstu spēju izvērtēt ārvalstu ieguldījumus, pamatojoties uz drošības un sabiedriskās kārtības kritērijiem, un izveido sadarbības mehānismu, kas ļauj Komisijai un dalībvalstīm sadarboties drošības risku, tostarp kiberdrošības risku, novērtēšanā, ko rada sensitīvi ārvalstu ieguldījumi, un tā kā tā ietver arī projektus un programmas, kas ir ES interesēs, kā, piemēram, Eiropas telekomunikāciju tīkli un „Apvārsnis 2020”,

1. uzskata, ka Savienībai ir jāuzņemas vadošā loma kiberdrošības jomā, izmantojot vienotu pieeju, kuras pamatā ir efektīva un lietderīga ES, dalībvalstu un nozares pārstāvju zinātība, jo dažādi atšķirīgi valstu lēmumi varētu kaitēt digitālajam vienotajam tirgum;

2. pauž dziļas bažas par nesenajiem apgalvojumiem par to, ka Ķīnas uzņēmumu izstrādātajā 5G aprīkojumā varētu būt integrētas iegultās lūkas, kas varētu ļauj ražotājiem un iestādēm neatļauti piekļūt privātiem un personas datiem un telesakariem no ES;

3. pauž tikpat dziļas bažas par šo ražotāju izstrādāto 5G aprīkojuma iespējamiem būtiskajiem trūkumiem, ja tā būtu jāinstalē, ieviešot 5G tīklus turpmākajos gados;

4. uzsver, ka ietekme uz tīklu un iekārtu drošību visā pasaulē ir līdzīga, un aicina ES mācīties no gūtās pieredzes, lai spētu nodrošināt augstākos kiberdrošības standartus; aicina Komisiju izstrādāt stratēģiju, kas ļaus Eiropai ieņemt vadošu pozīciju kiberdrošības tehnoloģiju jomā un kuras mērķis ir samazināt Eiropas atkarību no ārvalstu tehnoloģijām kiberdrošības jomā; uzskata, ka tad, ja nav iespējams garantēt atbilstību drošības prasībām, ir jāpiemēro atbilstīgi pasākumi;

5. aicina dalībvalstis informēt Komisiju par visiem valsts līmeņa pasākumiem, kurus tās plāno pieņemt, lai koordinētu Savienības reaģēšanas pasākumus, tādējādi visā Savienībā nodrošinot visaugstākos kiberdrošības standartus, un atkārtoti norāda uz to, ka ir svarīgi atturēties no nesamērīgu vienpusēju pasākumu ieviešanas, kas sadrumstalotu vienoto tirgu;

6. atkārtoti norāda, ka jebkurai struktūrai, kas ES nodrošina aprīkojumu vai sniedz pakalpojumus, neatkarīgi no tās izcelsmes valsts, ir jāievēro ES un dalībvalstu tiesību akti un saistības pamattiesību jomā, tostarp tiesiskais regulējums, kas attiecas uz privātumu, datu aizsardzību un kiberdrošību;

7. aicina Komisiju novērtēt Savienības tiesiskā regulējuma noturību, lai novērstu bažas par neaizsargāta aprīkojuma esamību stratēģiski svarīgās nozarēs un pamata infrastruktūrā; mudina Komisiju vajadzības gadījumā iesniegt iniciatīvas, tostarp tiesību aktu priekšlikumus, lai laikus novērstu visus konstatētos trūkumus, jo Savienība visu laiku apzina un risina kiberdrošības problēmas un stiprina kiberdrošības noturību ES;

8. mudina dalībvalstis, kuras vēl nav pilnībā transponējušas Tīklu un informācijas sistēmu drošības direktīvu, nekavējoties to izdarīt, un aicina Komisiju cieši uzraudzīt transponēšanu, lai nodrošinātu, ka direktīvas noteikumi tiek pienācīgi īstenoti un ka Eiropas iedzīvotāji ir labāk aizsargāti pret ārējiem drošības apdraudējumiem;

9. mudina Komisiju un dalībvalstis nodrošināt, ka tiek pareizi piemēroti ar TID direktīvu ieviestie ziņošanas mehānismi; norāda, ka Komisijai un dalībvalstīm būtu rūpīgi jāseko līdzi jebkādiem drošības incidentiem vai piegādātāju neatbilstošai reakcijai, lai novērstu atklātos trūkumus;

10. aicina Komisiju izvērtēt, vai ir nepieciešams paplašināt minētās TID direktīvas darbības jomu, attiecinot to arī uz citām kritiskām nozarēm un pakalpojumiem, uz kuriem neattiecas īpaši konkrēto nozari regulējoši tiesību akti;

11. atzinīgi vērtē un atbalsta panākto vienošanos par Kiberdrošības aktu un ES Tīklu un informācijas drošības aģentūras (*ENISA*) pilnvaru pastiprināšanu, lai labāk atbalstītu dalībvalstu centienus novērst kiberdrošības apdraudējumus un uzbrukumus;

12. mudina Komisiju pilnvarot *ENISA* par prioritāti noteikt darbu pie 5G aprīkojuma sertifikācijas sistēmas, lai nodrošinātu, ka 5G izvēršana Savienībā atbilst visaugstākajiem drošības standartiem un ir noturīga pret apiešanas iespējām vai būtisku neaizsargātību, kas apdraudētu Savienības telesakaru tīklu un no tā atkarīgo pakalpojumu drošību; iesaka īpašu uzmanību pievērst biežāk izmantotajiem procesiem, produktiem un programmatūrām, kas to plašās pielietojamības dēļ būtiski ietekmē iedzīvotāju ikdienas dzīvi un tautsaimniecību;

13. ļoti atzinīgi vērtē priekšlikumus par kiberdrošības kompetences centriem un valsts

koordinācijas centru tīklu, kas izstrādāts, lai palīdzētu ES saglabāt un attīstīt tehnoloģiskās un rūpnieciskās spējas kiberdrošības jomā, kas nepieciešamas digitālā vienotā tirgus nodrošināšanai; tomēr atgādina, ka sertifikācijas dēļ kompetentās iestādes un operatori nebūtu jāizslēdz no piegādes ķēdes pārbaudes, ko veic nolūkā nodrošināt tāda aprīkojuma integritāti un drošību, kas darbojas kritiskā vidē un telesakaru tīklos;

14. atgādina, ka kiberdrošībai ir nepieciešami augsti drošības standarti; prasa izveidot tīklu, kas atbilst principiem „drošs atbilstoši iestatījumam" un „tehniski drošs"; mudina dalībvalstis kopā ar Komisiju izpētīt visus pieejamos līdzekļus, lai garantētu augstu drošības līmeni;

15. aicina Komisiju un dalībvalstis sadarbībā ar *ENISA* sagatavot norādījumus par to, kā novērst kiberdraudus un neaizsargātību, iegādājoties 5G aprīkojumu, piemēram, dažādojot aprīkojumu, iegādājoties to no dažādiem piegādātājiem vai ieviešot vairākposmu iepirkuma procesus;

16. atkārtoti apstiprina savu nostāju attiecībā uz programmu „Digitālā Eiropa", kas paredz drošības prasības un Komisijas uzraudzību pār uzņēmumiem, kuri veic uzņēmējdarbību ES, bet kurus kontrolē trešās valstis, jo īpaši attiecībā uz darbībām, kas saistītas ar kiberdrošību;

17. aicina dalībvalstis nodrošināt, ka publiskās iestādes un privātie uzņēmumi, kas ir iesaistīti tādu kritiskās infrastruktūras tīklu kā, piemēram, telekomunikāciju, enerģētikas, veselības un sociālo sistēmu pienācīgas darbības nodrošināšanā, veic attiecīgus riska analīzes novērtējumus, ņemot vērā drošības apdraudējumus, kas ir saistīti tieši ar attiecīgās sistēmas tehniskajām īpašībām, vai atkarību no ārējiem aparatūras un programmatūras tehnoloģiju piegādātājiem;`

18. atgādina, ka pašreizējā telesakaru tiesiskajā regulējumā dalībvalstīm ir uzdots nodrošināt, ka telesakaru operatori ievēro publisko elektronisko sakaru tīklu integritāti un pieejamību, tostarp vajadzības gadījumā veicot pilnīgu šifrēšanu; uzsver, ka saskaņā ar Eiropas Elektronisko sakaru kodeksu dalībvalstīm ir plašas pilnvaras izpētīt produktus ES tirgū un piemērot dažādus tiesiskās aizsardzības līdzekļus to neatbilstības gadījumā;

19. aicina Komisiju un dalībvalstis gan ES, gan valstu līmenī padarīt drošību par obligātu aspektu visās publiskā iepirkuma procedūrās, kas saistās ar attiecīgo infrastruktūru;

20. atgādina dalībvalstīm par to pienākumu saskaņā ar ES tiesisko regulējumu, jo īpaši Direktīvu 2013/40/ES par uzbrukumiem informācijas sistēmām, noteikt sankcijas juridiskām personām, kuras izdarījušas noziedzīgus nodarījumus, piemēram, uzbrukumus šādām sistēmām; uzsver, ka dalībvalstīm būtu arī jāizmanto situācija, ka tās spēj noteikt citas sankcijas šādām juridiskajām personām, piemēram, pagaidu vai pastāvīgs aizliegums veikt komercdarbību;

21. aicina ne tikai dalībvalstis un kiberdrošības aģentūras, bet arī telesakaru operatorus, ražotājus un kritiskās infrastruktūras pakalpojumu sniedzējus ziņot Komisijai un *ENISA* par pierādījumiem saistībā ar iegultajām lūkām vai par citiem būtiskiem trūkumiem, kas apdraudētu telesakaru tīklu integritāti un drošību vai kas radītu Savienības tiesību aktu un pamattiesību pārkāpumus; sagaida, ka valstu datu aizsardzības iestādes, kā arī Eiropas Datu aizsardzības uzraudzītājs rūpīgi izpētīs norādes par to, ka ārējie tirgotāji ir

pārkāpuši datu aizsardzības noteikumus, un piemēros atbilstošus sodus un sankcijas saskaņā ar Eiropas tiesību aktiem datu aizsardzības jomā;

22. atzinīgi vērtē to, ka drīzumā stāsies spēkā regula, ar ko izveido satvaru ārvalstu tiešo ieguldījumu (ĀTI) izvērtēšanai drošības un sabiedriskās kārtības apsvērumu dēļ, un uzsver, ka ar šo regulu pirmo reizi izveido sarakstu ar jomām un faktoriem, tostarp komunikācijām un kiberdrošību, kas attiecas uz drošību un sabiedrisko kārtību ES līmenī;

23. aicina Padomi paātrināt tās darbu pie ierosinātās e–privātuma regulas;

24. atkārtoti uzsver, ka ES ir jāatbalsta kiberdrošība visā pievienotās vērtības veidošanas ķēdē, sākot no pētniecības līdz svarīgāko tehnoloģiju izstrādei un ieviešanai, jāizplata attiecīga informācija un jāveicina kiberhigiēna un izglītības mācību programmas, ietverot tajās arī kiberdrošību, un uzskata, ka citu pasākumu starpā programma „Digitālā Eiropa" būs lietderīgs instruments šādam nolūkam;

25. mudina Komisiju un dalībvalstis veikt nepieciešamos pasākumus, tostarp paredzēt stabilas ieguldījumu shēmas, lai ES radītu inovācijai labvēlīgu vidi, kurai vajadzētu būt pieejamai visiem ES digitālās ekonomikas uzņēmumiem, tostarp mazajiem un vidējiem uzņēmumiem (MVU); turklāt vēlas, lai šāda vide ļautu Eiropas tirgotājiem izstrādāt jaunus produktus, pakalpojumus un tehnoloģijas, kas nodrošinātu tiem iespēju būt konkurētspējīgiem;

26. aicina Komisiju un dalībvalstis turpmākajās diskusijās ņemt vērā minētos pieprasījumus saistībā ar ES un Ķīnas stratēģiju kā nosacījumus, kas ir nepieciešami, lai ES saglabātu konkurētspēju un garantētu tās digitālās infrastruktūras drošību;

27. uzdod priekšsēdētājam šo rezolūciju nosūtīt Padomei un Komisijai.