Europos Parlamentas
2014-2019

PRIIMTI TEKSTAI

P8_TA(2019)0156

Grėsmės saugumui, susijusios su kiniškų technologijų plitimu ES, ir galimi ES lygmens veiksmai siekiant jas mažinti

2019 m. kovo 12 d. Europos Parlamento rezoliucija dėl grėsmių saugumui, susijusių su Kinijos technologijų plitimu ES, ir galimų ES lygmens veiksmų siekiant jas mažinti (2019/2575(RSP))

Europos Parlamentas,

– atsižvelgdamas į 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyvą (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas[1],

– atsižvelgdamas į 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[2],

– atsižvelgdamas į 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR[3],

– atsižvelgdamas į 2017 m. rugsėjo 13 d. Komisijos pasiūlymą dėl Europos Parlamento ir Tarybos reglamento dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (COM(2017)0477),

– atsižvelgdamas į 2018 m. rugsėjo 12 d. Komisijos pasiūlymą dėl reglamento, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (COM(2018)0630),

– atsižvelgdamas į 2017 m. birželio 28 d. Kinijos Nacionalinio Liaudies Kongreso priimtą naują Nacionalinės žvalgybos įstatymą,

– atsižvelgdamas į 2019 m. vasario 13 d. Tarybos ir Komisijos pareiškimus dėl grėsmių saugumui, susijusių su Kinijos technologijų plitimu ES, ir galimų ES lygmens veiksmų

---

1 OL L 321, 2018 12 17, p. 36.
2 OL L 194, 2016 7 19, p. 1.
3 OL L 218, 2013 8 14, p. 8.

siekiant jas sumažinti,

– atsižvelgdamas į Australijos vyriausybės patvirtintas valstybės telekomunikacijų sektoriaus saugumo reformas, kurios įsigaliojo 2018 m. rugsėjo 18 d.,

– atsižvelgdamas į savo 2019 m. vasario 14 d. pirmojo svarstymo metu priimtą poziciją dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatoma tiesioginių užsienio investicijų į Europos Sąjungą tikrinimo sistema[1],

– atsižvelgdamas į savo ankstesnes rezoliucijas dėl ES ir Kinijos santykių padėties, ypač į 2018 m. rugsėjo 12 d. rezoliuciją[2],

– atsižvelgdamas į 2016 m. rugsėjo 14 d. Komisijos komunikatą „Europos 5G veiksmų planas“(COM(2016)0588),

– atsižvelgdamas į savo 2017 m. birželio 1 d. rezoliuciją „Interneto ryšys siekiant augimo, konkurencingumo ir sanglaudos: Europos gigabitinė visuomenė ir 5G ryšys“[3],

– atsižvelgdamas į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)[4],

– atsižvelgdamas į 2013 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1316/2013, kuriuo sukuriama Europos infrastruktūros tinklų priemonė ir iš dalies keičiamas Reglamentas (ES) Nr. 913/2010 bei panaikinami reglamentai (EB) Nr. 680/2007 ir (EB) Nr. 67/2010[5],

– atsižvelgdamas į 2018 m. birželio 6 d. Komisija pasiūlymą dėl Europos Parlamento ir Tarybos reglamento dėl 2021–2027 m. Skaitmeninės Europos programos sudarymo (COM(2018)0434),

– atsižvelgdamas į Darbo tvarkos taisyklių 123 straipsnio 2 ir 4 dalis,

A. kadangi ES, siekdama realizuoti savo galimybes, kad taptų lydere kibernetinio saugumo srityje, ir panaudoti tai savo pramonės labui, privalo toliau įgyvendinti savo kibernetinio saugumo darbotvarkę;

B. kadangi siekiant pakenkti IT sistemoms galėtų būti naudojamasi 5G ryšio tinklų pažeidžiamumu, o tai galėtų padaryti labai didelę žalą ekonomikai Europos ir nacionaliniu lygmenimis; kadangi siekiant kuo labiau sumažinti riziką visoje vertės grandinėje būtina taikyti rizikos analize grindžiamą požiūrį;

C. kadangi 5G ryšio tinklas bus mūsų skaitmeninės infrastruktūros pagrindas, kuris padidins galimybę prijungti prie tinklų įvairius įrenginius (daiktų internetas ir kt.), taip pat suteiks visuomenei ir įmonėms naujų pranašumų ir galimybių daugelyje sričių, be

---

1 Priimti tekstai, P8_TA(2019)0121.
2 Priimti tekstai, P8_TA(2018)0343.
3 OL C 307, 2018 8 30, p. 144.
4 wOL L 119, 2016 5 4, p. 1.
5 OL L 348, 2013 12 20, p. 129.

kita ko, ypatingos svarbos ekonomikos sektoriuose, pavyzdžiui, transporto, energetikos, sveikatos, finansų, telekomunikacijų, gynybos, kosmoso ir saugumo sektoriuose;

D. kadangi, sukūrus tinkamą reagavimo į saugumo iššūkius mechanizmą, ES būtų sudaryta galimybė imtis aktyvių veiksmų nustatant 5G ryšio standartus;

E. kadangi buvo išreikštas susirūpinimas dėl trečiųjų šalių prekiautojų įranga, kurie dėl savo kilmės šalyse galiojančių įstatymų galėtų kelti pavojų saugumui ES, ypač po to, kai buvo priimti Kinijos valstybės įstatymai dėl saugumo, pagal kuriuos visiems piliečiams, įmonėms bei kitiems subjektams nustatomos prievolės bendradarbiauti su valdžios sektoriumi siekiant užtikrinti valstybės saugumą, taip pat kuriuose pateikta labai plati nacionalinio saugumo apibrėžtis; kadangi nėra jokių garantijų, kad šios prievolės nebus taikomos eksteritorialiai, ir kadangi įvairių šalių reakcija į šiuos Kinijos įstatymus skiriasi – pradedant saugumo vertinimais ir baigiant visišku draudimu;

F. kadangi 2018 m. gruodžio mėn. Čekijos nacionalinė kibernetinio saugumo institucija pateikė perspėjimą dėl saugumo grėsmių, kurias kelia Kinijos bendrovių „Huawei“ ir ZTE tiekiamos technologijos; kadangi vėliau, 2019 m. sausio mėn., Čekijos mokesčių institucijos neįtraukė bendrovės „Huawei“ pateikto pasiūlymo į konkursą mokesčių portalui sukurti;

G. kadangi reikia atlikti išsamų tyrimą, siekiant išsiaiškinti, ar susiję prietaisai arba bet kurie kiti prietaisai ar tiekėjai kelia saugumo riziką dėl tokių priemonių kaip užpakalinės durys į sistemas;

H. kadangi sprendimus reikėtų koordinuoti ir diegti ES lygmeniu, kad būtų išvengta saugumo lygio skirtumų ir galimų kibernetinio saugumo spragų, tuo pačiu metu siekiant užtikrinti tvirtą atsaką reikia koordinavimo pasauliniu lygmeniu;

I. kadangi bendrosios rinkos pranašumai taip pat reiškia prievolę laikytis ES standartų ir Sąjungos teisinės sistemos ir kadangi tiekėjams dėl jų kilmės šalies neturėtų būti taikomos skirtingos sąlygos;

J. kadangi Reglamentas dėl tiesioginių užsienio investicijų tikrinimo, kuris turėtų įsigalioti iki 2020 m. pabaigos, sustiprina valstybių narių gebėjimą tikrinti užsienio investicijas remiantis saugumo ir viešosios tvarkos kriterijais ir nustato bendradarbiavimo mechanizmą, kuris suteikia galimybę Komisijai ir valstybėms narėms bendradarbiauti vertinant saugumo riziką, įskaitant dėl jautrių užsienio investicijų kylančią kibernetinio saugumo riziką, ir taip pat apima ES svarbius projektus ir programas, pvz., transeuropinius telekomunikacijų tinklus ir programą „Horizontas 2020“;

1. mano, kad Sąjunga turi atlikti vadovaujamą vaidmenį kibernetinio saugumo srityje ir nustatyti bendrą požiūrį, grindžiamą efektyviu ir veiksmingu ES, valstybių narių ir pramonės ekspertinių žinių taikymu, nes skirtingų nacionalinių sprendimų sistema būtų žalinga bendrajai skaitmeninei rinkai;

2. yra labai susirūpinęs dėl neseniai pareikštų kaltinimų, kad Kinijos įmonių sukurtoje 5G ryšio įrangoje gali būti įdiegtos užpakalinės durys, kurios suteiktų gamintojams ir valdžios institucijoms neteisėtos prieigos prie privačių ir asmeninio pobūdžio duomenų bei telekomunikacijų Europos Sąjungoje galimybę;

3. taip pat yra susirūpinęs dėl to, kad šių gamintojų sukurta 5G ryšio įranga galės būti labai

pažeidžiama, jei ateityje ji būtų įrengta diegiant 5G ryšio tinklus;

4. pabrėžia, kad poveikis tinklų ir įrangos saugumui yra vienodas visame pasaulyje, ir ragina ES pasimokyti iš turimos patirties, kad būtų galima užtikrinti aukščiausius kibernetinio saugumo standartus; ragina Komisiją parengti strategiją, kurią įgyvendinant Europa pirmautų kibernetinio saugumo technologijų srityje ir kuria būtų siekiama sumažinti Europos priklausomybę nuo užsienio kibernetinio saugumo srities technologijų; laikosi nuomonės, kad visais atvejais, kai negalima užtikrinti saugumo reikalavimų laikymosi, būtina taikyti tinkamas priemones;

5. ragina valstybes nares informuoti Komisiją apie bet kokias nacionalines priemones, kurias jos ketina patvirtinti, kad būtų galima koordinuoti Sąjungos atsaką ir atitinkamai užtikrinti aukščiausius kibernetinio saugumo standartus visoje Sąjungoje, taip pat kartoja, kad svarbu nenustatyti neproporcingų vienašališkų priemonių, kuriomis būtų suskaidyta bendroji rinka;

6. pakartoja, kad visos įmonės, tiekiančios įrangą ir teikiančios paslaugas ES, nepriklausomai jų nuo kilmės šalies, privalo laikytis įsipareigojimų dėl pagrindinių teisių ir ES bei valstybių narių teisės, įskaitant su privatumu, duomenų apsauga ir kibernetiniu saugumu susijusią teisinę sistemą;

7. ragina Komisiją įvertinti Sąjungos teisinės sistemos tvirtumą, siekiant spręsti rūpestį keliančius klausimus dėl strateginiuose sektoriuose ir pagrindinėje infrastruktūroje įdiegtos pažeidžiamos įrangos; primygtinai ragina Komisiją pateikti iniciatyvų, įskaitant, kai tinka, pasiūlymus dėl teisėkūros procedūra priimamų aktų, kurios padėtų laiku pašalinti bet kokius nustatytus trūkumus, nes Sąjungoje nuolat nustatoma kibernetinio saugumo problemų ir jos sprendžiamos, taip pat ES vykdomas kibernetinio atsparumo didinimo procesas;

8. primygtinai ragina valstybes nares, kurios dar visapusiškai neperkėlė TIS direktyvos į savo nacionalinę teisę, nedelsiant tai padaryti, ir ragina Komisiją nuodugniai stebėti, kai ši direktyva perkeliama, siekiant užtikrinti, kad jos nuostatos būtų tinkamai taikomos ir vykdomos ir kad Europos piliečiai būtų geriau apsaugoti nuo išorės ir vidaus grėsmių saugumui;

9. primygtinai ragina Komisiją ir valstybes nares užtikrinti, kad būtų tinkamai taikomi Kibernetinio saugumo (TIS) direktyvoje nustatyti ataskaitų teikimo mechanizmai; pažymi, kad Komisija ir valstybės narės turėtų atidžiai stebėti visus saugumo incidentus ar netinkamas tiekėjų reakcijas, kad būtų pašalintos nustatytos spragos;

10. ragina Komisiją įvertinti poreikį toliau plėsti TIS direktyvos taikymo sritį, į ją įtraukiant kitus svarbius sektorius bei paslaugas, nepatenkančius į konkretiems sektoriams skirtų teisės aktų taikymo sritį;

11. teigiamai vertina ir remia pasiektą susitarimą dėl Kibernetinio saugumo akto ir Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimų sustiprinimą siekiant geriau paremti valstybes nares šioms kovojant su grėsmėmis kibernetiniam saugumui ir kibernetiniais išpuoliais;

12. primygtinai ragina Komisiją įgalioti ENISA prioritetą teikti darbui rengiant 5G ryšio įrangos sertifikavimo sistemą, siekiant užtikrinti, kad Sąjungoje diegiamas 5G ryšys

atitiktų aukščiausius saugumo standartus ir būtų atsparus užpakalinėms durims arba dideliam pažeidžiamumui, kurie keltų pavojų Sąjungos telekomunikacijų tinklų ir nuo jų priklausomų paslaugų saugumui; rekomenduoja ypatingą dėmesį skirti dažnai naudojamiems procesams, produktams ir programinei įrangai, kurie vien dėl jų naudojimo masto turi didelį poveikį kasdieniam piliečių gyvenimui ir ekonomikai;

13. labai teigiamai vertina pasiūlymus dėl kibernetinio saugumo kompetencijos centrų ir nacionalinių koordinavimo centrų tinklo, skirto padėti ES išlaikyti ir plėtoti technologinius ir pramoninius pajėgumus kibernetinio saugumo srityje, kurių jai reikia siekiant apsaugoti savo bendrąją skaitmeninę rinką; vis dėlto primena, kad taikant sertifikavimą neturėtų būti panaikinamos kompetentingų institucijų ir operatorių galimybės tikrinti tiekimo grandinę siekiant užtikrinti savo įrangos, veikiančios ypatingos svarbos aplinkoje ir telekomunikacijų tinkluose, vientisumą ir saugumą;

14. primena, kad kibernetiniam saugumui užtikrinti reikia taikyti aukštus kibernetinio saugumo standartus; ragina kurti tinklą, kuris būtų patikimas pagal standartizuotosios ir integruotosios privatumo apsaugos principus; primygtinai ragina valstybes nares kartu su Komisija išnagrinėti visas turimas galimybes užtikrinti aukštą saugumo lygį;

15. ragina Komisiją ir valstybes nares bendradarbiaujant su ENISA parengti gaires, kaip kovoti su kibernetinėmis grėsmėmis ir pažeidžiamumu perkant 5G ryšio įrangą, pavyzdžiui, diversifikuojant įrangos pirkimą iš įvairių pardavėjų arba diegiant daugiaetapes viešųjų pirkimų procedūras;

16. dar kartą patvirtina savo poziciją dėl programos „Skaitmeninė Europa“, kurią įgyvendinant bus taikomi saugumo reikalavimai ir Komisija prižiūrės ES įsisteigusių, bet trečiųjų šalių kontroliuojamų įmonių veiklą, visų pirma susijusią su kibernetiniu saugumu;

17. ragina valstybes nares užtikrinti, kad viešojo sektoriaus institucijos ir privačios įmonės, dalyvaujančios užtikrinant tinkamą ypatingos svarbos infrastruktūros tinklų, tokių kaip telekomunikacijų, energetikos, sveikatos apsaugos ir socialinė sistemos, veikimą, atliktų atitinkamus rizikos vertinimus, atsižvelgdamos į konkrečias grėsmes saugumui, susijusias su atitinkamos sistemos techninėmis savybėmis ar priklausomybe nuo techninės ir programinės įrangos technologijas teikiančių išorės tiekėjų;

18. primena, jog pagal dabartinę telekomunikacijų teisinę sistemą valstybės narės įpareigojamos užtikrinti, kad telekomunikacijų operatoriai laikytųsi viešųjų elektroninių ryšių tinklų vientisumo ir prieinamumo principų, įskaitant ištisinį šifravimą, kai tinkama; pabrėžia, kad pagal Europos elektroninių ryšių kodeksą valstybėms narėms suteikti išsamūs įgaliojimai atlikti ES rinkoje esančių produktų tyrimus ir taikyti įvairias teisių gynimo priemones tuo atveju, jei nustatyta, jog jie neatitinka reikalavimų;

19. ragina Komisiją ir valstybes nares užtikrinti, kad saugumas taptų privalomu visų tiek ES, tiek nacionaliniu lygmeniu vykdomų svarbioms infrastruktūroms skirtų viešųjų pirkimų procedūrų aspektu;

20. primena valstybėms narėms jų įsipareigojimą pagal ES teisinę sistemą, ypač pagal Direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, skirti sankcijas juridiniams asmenims, kurie padarė nusikalstamas veikas, pvz., išpuolius prieš tokias sistemas; pabrėžia, kad valstybės narės taip pat turėtų pasinaudoti turimomis

galimybėmis tokiems juridiniams asmenims taikyti kitas sankcijas, pvz., laikinai ar visam laikui atimti teisę verstis komercine veikla;

21. ragina valstybes nares, kibernetinio saugumo agentūras, telekomunikacijų operatorius, ypatingos svarbos infrastruktūros objektų gamintojus ir paslaugų teikėjus pateikti Komisijai ir ENISA bet kokius įrodymus apie užpakalines duris arba kitus didelio pažeidžiamumo atvejus, per kuriuos galėtų būti pakenkta telekomunikacijų tinklų vientisumui ir saugumui arba pažeidžiama Sąjungos teisė ir pagrindinės teisės; tikisi, kad nacionalinės duomenų apsaugos institucijos ir Europos duomenų apsaugos priežiūros pareigūnas nuodugniai ištirs įtarimus dėl išorės pardavėjų vykdomų asmens duomenų saugumo pažeidimų ir skirs atitinkamas nuobaudas ir sankcijas, numatytas Europos duomenų apsaugos teisės aktuose;

22. teigiamai vertina tai, kad ateityje įsigalios reglamentas, kuriuo dėl saugumo ir viešosios tvarkos priežasčių nustatoma tiesioginių užsienio investicijų tikrinimo sistema, ir pabrėžia, kad šiuo reglamentu pirmą kartą ES lygmeniu nustatomas saugumui ir viešajai tvarkai svarbių sričių ir veiksnių, įskaitant ryšius ir kibernetinį saugumą, sąrašas;

23. ragina Tarybą paspartinti savo darbą, susijusį su pasiūlymu dėl E. privatumo reglamento;

24. pakartoja, kad ES turi remti kibernetinį saugumą visoje vertės grandinėje – nuo mokslinių tyrimų iki pagrindinių technologijų diegimo ir naudojimo, skleisti atitinkamą informaciją ir propaguoti kibernetinę higieną ir švietimo programas, be kita ko, kibernetinio saugumo klausimais, ir mano, kad, be kitų priemonių, programa „Skaitmeninė Europa“ bus veiksminga priemonė siekiant tokio tikslo;

25. primygtinai ragina Komisiją ir valstybes nares imtis būtinų veiksmų, įskaitant tvirtų investicijų schemų parengimą, siekiant sukurti ES inovacijoms palankią aplinką, kuri turėtų būti prieinama visoms ES skaitmeninėje ekonomikoje veikiančioms įmonėms, įskaitant mažąsias ir vidutines įmones (MVĮ); be to, primygtinai ragina užtikrinti, kad tokia aplinka sudarytų sąlygas Europos gamintojams kurti naujus produktus, paslaugas ir technologijas, kurios leistų jiems būti konkurencingiems;

26. ragina Komisiją ir valstybes nares per artėjančias diskusijas dėl būsimos ES ir Kinijos strategijos atsižvelgti į minėtus reikalavimus, nes tai būtina ES konkurencingumo išlaikymo ir jos skaitmeninės infrastruktūros saugumo užtikrinimo sąlyga;

27. paveda Pirmininkui perduoti šią rezoliuciją Tarybai ir Komisijai.