Evropski parlament
2014-2019

SPREJETA BESEDILA

P8_TA(2019)0156

Varnostne grožnje zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možni ukrepi na ravni EU za njihovo zmanjšanje

Resolucija Evropskega parlamenta z dne 12. marca 2019 o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možnih ukrepih na ravni EU za njihovo zmanjšanje (2019/2575(RSP))

Evropski parlament,

– ob upoštevanju Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah[1],

– ob upoštevanju Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[2],

– ob upoštevanju Direktive 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ[3],

– ob upoštevanju predloga Komisije z dne 13. septembra 2017 za uredbo Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti) (COM(2017)0477),

– ob upoštevanju predloga Komisije z dne 12. septembra 2018 za uredbo o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov (COM(2018)0630),

– ob upoštevanju, da je kitajski nacionalni ljudski kongres 28. junija 2017 sprejel nov zakon o državnih obveščevalnih dejavnostih,

– ob upoštevanju izjav Sveta in Komisije z dne 13. februarja 2019 o varnostnih grožnjah zaradi vedno večje prisotnosti Kitajske na tehnološkem področju v EU in možnih ukrepih na ravni EU za njihovo zmanjšanje,

---

1 UL L 321, 17.12.2018, str. 36.
2 UL L 194, 19.7.2016, str. 1.
3 UL L 218, 14.8.2013, str. 8.

– ob upoštevanju, da je avstralska vlada sprejela varnostne reforme vladnega telekomunikacijskega sektorja, ki so začele veljati 18. septembra 2018,

– ob upoštevanju svojega stališča, sprejetega v prvi obravnavi dne 14. februarja 2019, o predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvira za pregled neposrednih tujih naložb v Evropski uniji[1],

– ob upoštevanju svojih prejšnjih resolucij o stanju odnosov med EU in Kitajsko, zlasti resolucije z dne 12. septembra 2018[2],

– ob upoštevanju sporočila Komisije z dne 14. septembra 2016 z naslovom Akcijski načrt za 5G v Evropi (COM(2016)0588),

– ob upoštevanju svoje resolucije z dne 1. junija 2017 o internetni povezljivosti za rast, konkurenčnost in kohezijo: evropska gigabitna družba in 5G[3],

– ob upoštevanju Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)[4],

– ob upoštevanju Uredbe (EU) št. 1316/2013 Evropskega parlamenta in Sveta z dne 11. decembra 2013 o vzpostavitvi Instrumenta za povezovanje Evrope, spremembi Uredbe (EU) št. 913/2010 in razveljavitvi uredb (ES) št. 680/2007 in (ES) št. 67/2010[5],

– ob upoštevanju predloga Komisije z dne 6. junija 2018 za uredbo Evropskega parlamenta in Sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027 (COM(2018)0434),

– ob upoštevanju člena 123(2) in 123(4) Poslovnika,

A. ker mora EU še naprej izvajati svojo agendo za kibernetsko varnost, da bi izpolnila svoj potencial in postala vodilni akter na področju kibernetske varnosti, to pa mora uporabiti v korist svoje industrije;

B. ker bi bilo mogoče šibke točke v omrežjih 5G izkoristiti za ogrožanje informacijskih sistemov, kar bi lahko povzročilo zelo resno škodo za gospodarstva na evropski in nacionalni ravni; ker je za zmanjšanje tveganj na najmanjšo možno raven potreben pristop na podlagi analize tveganj v celotni vrednostni verigi;

C. ker bo omrežje 5G temelj naše digitalne infrastrukture, ki bo razširil možnost povezave različnih naprav v omrežje (internet stvari itd.), in bo prineslo nove koristi in priložnosti družbi in podjetjem na številnih področjih, vključno s kritičnimi sektorji gospodarstva, kot so prometni, energetski, zdravstveni, finančni, telekomunikacijski, obrambni, vesoljski in varnostni sektor;

D. ker bi vzpostavitev ustreznih mehanizmov za odzivanje na varnostne grožnje EU dala

---

1 Sprejeta besedila, P8_TA(2019)0121.
2 Sprejeta besedila, P8_TA(2018)0343.
3 UL C 307, 30.8.2018, str. 144.
4 UL L 119, 4.5.2016, str. 1.
5 UL L 348, 20.12.2013, str. 129.

možnost, da aktivno ukrepa pri določanju standardov za omrežje 5G;

E. ker so bili izraženi pomisleki glede prodajalcev opreme iz tretjih držav, ki bi lahko pomenili varnostno grožnjo za EU zaradi zakonov njihove države izvora, zlasti po uveljavitvi kitajskih zakonov o državni varnosti, ki vsem državljanom, podjetjem in drugim subjektom nalagajo obveznosti sodelovanja z državo pri zaščiti, da se zaščitita državna in zelo široko opredeljena nacionalna varnost; ker ni jamstva, da se te obveznosti ne uporabljajo ekstrateritorialno, in ker so odzivi na kitajske zakone v različnih državah različni in segajo od varnostnih ocen do neposrednih prepovedi;

F. ker je češki nacionalni organ za kibernetsko varnost decembra 2018 izdal opozorilo pred varnostnimi grožnjami, ki jih predstavljajo tehnologije, ki jih nudita kitajski podjetji Huawei in ZTE; ker so nato češki davčni organi januarja 2019 izločili podjetje Huawei iz razpisa za vzpostavitev davčnega portala;

G. ker je potrebna temeljita preiskava, da bi pojasnili, ali vpletene naprave ali katere koli druge naprave ali dobavitelji predstavljajo varnostne grožnje zaradi funkcij, kot so stranska vrata v sisteme;

H. ker bi bilo treba rešitve uskladiti in obravnavati na ravni EU, da bi se izognili oblikovanju različnih ravni varnosti in morebitnim vrzelim v kibernetski varnosti, pri tem pa je potrebno usklajevanje na svetovni ravni, da bi dosegli odločen odziv;

I. ker koristi enotnega trga spremlja obveznost, da se upoštevajo standardi in pravni okvir Unije, in ker dobaviteljev ne bi smeli obravnavati drugače glede na njihovo državo porekla;

J. ker uredba o pregledu neposrednih tujih naložb, ki bi morala začeti veljati do konca leta 2020, krepi zmožnost držav članic za pregled tujih naložb na podlagi meril varnosti in javnega reda ter določa mehanizem sodelovanja, ki Komisiji in državam članicam omogoča sodelovanje pri oceni varnostnih tveganj, vključno s tveganji kibernetske varnosti, ki jih predstavljajo občutljive tuje naložbe, zajema pa tudi projekte in programe v interesu EU, kot so vseevropska telekomunikacijska omrežja in Obzorje 2020;

1. meni, da mora Unija prevzeti vodilno vlogo na področju kibernetske varnosti s skupnim pristopom, ki bi temeljil na uspešni in učinkoviti uporabi strokovnega znanja EU, držav članic in industrije, saj bi mozaik različnih nacionalnih odločitev škodil enotnemu digitalnemu trgu;

2. izraža globoko zaskrbljenost zaradi nedavnih trditev, da bi oprema 5G, ki jo razvijajo kitajska podjetja, lahko vsebovala vgrajena stranska vrata, ki bi proizvajalcem in oblastem omogočala nepooblaščen dostop do zasebnih in osebnih podatkov in telekomunikacij iz EU;

3. je prav tako zaskrbljen zaradi morebitne prisotnosti večjih šibkih točk v opremi 5G, ki jo razvijajo ti proizvajalci, če bi se vgradila pri vzpostavitvi omrežij 5G v prihodnjih letih;

4. poudarja, da so posledice za varnost omrežij in opreme podobne po vsem svetu in poziva, naj EU upošteva vse razpoložljive izkušnje, da bi lahko zagotovila najvišje standarde kibernetske varnosti; poziva Komisijo, naj pripravi strategijo, ki bo Evropo

postavila v ospredje na področju tehnologije kibernetske varnosti in bo namenjena zmanjšanju odvisnosti Evrope od tuje tehnologije na tem področju; meni, da je treba uporabiti ustrezne ukrepe, kadar ni mogoče zagotoviti skladnosti z varnostnimi zahtevami;

5. poziva države članice, naj Komisijo obvestijo o vseh nacionalnih ukrepih, ki jih nameravajo sprejeti, da bi uskladila odziv Unije in tako zagotovila najvišje standarde kibernetske varnosti po vsej Uniji, ter ponavlja, kako pomembno se je izogniti uvedbi nesorazmernih enostranskih ukrepov, ki bi razdrobili enotni trg;

6. ponavlja, da morajo vsi subjekti, ki v EU nudijo opremo ali storitve, ne glede na njihovo državo porekla, upoštevati obveznosti glede temeljnih pravic ter zakonodajo EU in držav članic, vključno s pravnim okvirom v zvezi z zasebnostjo, varstvom podatkov in kibernetsko varnostjo;

7. poziva Komisijo, naj oceni trdnost pravnega okvira Unije, da bi obravnavala pomisleke glede prisotnosti ranljive opreme v strateških sektorjih in osrednji infrastrukturi; poziva Komisijo, naj po potrebi predstavi pobude, vključno z zakonodajnimi predlogi, da bi pravočasno obravnavala ugotovljene pomanjkljivosti, saj je Unija v stalnem procesu opredeljevanja in obravnavanja izzivov ter krepitve odpornosti na področju kibernetske varnosti v EU;

8. poziva tiste države članice, ki še niso v celoti prenesle direktive o varnosti omrežij in informacijskih sistemov, naj to nemudoma storijo, in poziva Komisijo, naj pozorno spremlja prenos, da bi zagotovila, da se bodo določbe te direktive ustrezno uporabljale in izvrševale in da bodo evropski državljani bolje zaščiteni pred zunanjimi in notranjimi varnostnimi grožnjami;

9. poziva Komisijo in države članice, naj zagotovijo, da se bodo mehanizmi poročanja iz direktive o varnosti omrežij in informacijskih sistemov pravilno uporabljali; ugotavlja, da bi morale Komisija in države članice sprejeti temeljite nadaljnje ukrepe v zvezi z vsemi varnostnimi incidenti ali neprimernimi odzivi dobaviteljev, da bi obravnavale ugotovljene vrzeli;

10. poziva Komisijo, naj oceni, ali je treba področje uporabe direktive o varnosti omrežij in informacijskih sistemov dodatno razširiti na druge kritične sektorje in storitve, ki niso zajeti v posebni zakonodaji za sektor;

11. pozdravlja in podpira doseženi dogovor o uredbi o kibernetski varnosti in okrepitev mandata Agencije EU za varnost omrežij in informacij (ENISA), da bi bolje podprli države članice v boju proti grožnjam kibernetski varnosti in kibernetskim napadom;

12. poziva Komisijo, naj agenciji ENISA naroči, naj prednostno obravnava shemo certificiranja za opremo 5G, zato da bo uvedba omrežja 5G v Uniji v skladu z najvišjimi varnostnimi standardi in da bo omrežje odporno na stranska vrata ali pomembne šibke točke, ki bi ogrozile varnost telekomunikacijskih omrežij in odvisnih storitev Unije; priporoča, da se posebna pozornost nameni splošno uporabljenim postopkom, proizvodom in programski opremi, ki imajo zaradi svojega velikega obsega pomemben vpliv na vsakdanje življenje državljanov in gospodarstvo;

13. toplo pozdravlja predloga o strokovnih centrih za kibernetsko varnost in mreži

nacionalnih koordinacijskih centrov, ki naj bi EU pomagali pri ohranjanju in razvoju tehnoloških in industrijskih zmogljivosti na področju kibernetske varnosti, ki so potrebne za zagotovitev enotnega digitalnega trga; opozarja, da vključitev certificiranja vseeno ne pomeni, da pristojnim organom in operaterjem ni treba nadzirati dobavne verige, da bi zagotovili celovitost in varnost svoje opreme, ki deluje v kritičnih okoljih in telekomunikacijskih omrežjih;

14. opozarja, da so za kibernetsko varnost potrebne visoke varnostne zahteve; poziva k omrežju, skladnem z načelom privzete in vgrajene varnosti; poziva države članice, naj skupaj s Komisijo preučijo vsa razpoložljiva sredstva za zagotovitev visoke ravni varnosti;

15. poziva Komisijo in države članice, naj v sodelovanju z agencijo ENISA pripravijo smernice za obravnavanje kibernetskih groženj in šibkih točk pri nabavi opreme 5G, na primer z diverzifikacijo opreme različnih prodajalcev ali z uvedbo večfaznih postopkov javnih naročil;

16. ponovno potrjuje svoje stališče o programu za digitalno Evropo, ki določa varnostne zahteve in nadzor Komisije nad subjekti s sedežem v EU, ki so pod nadzorom tretjih držav, zlasti ko gre za ukrepe na področju kibernetske varnosti;

17. poziva države članice, naj zagotovijo, da javne institucije in zasebna podjetja, ki sodelujejo pri zagotavljanju pravilnega delovanja kritičnih infrastrukturnih omrežij, kot so telekomunikacijski, energetski, zdravstveni in socialni sistemi, izvedejo ustrezne ocene tveganja, pri čemer upoštevajo varnostne grožnje, ki so posebej povezane s tehničnimi značilnostmi zadevnega sistema ali odvisnostjo od zunanjih dobaviteljev strojne in programske opreme;

18. opozarja, da morajo države članice po veljavnem pravnem okviru za telekomunikacijske storitve zagotoviti, da telekomunikacijski operaterji spoštujejo celovitost in razpoložljivost javnih elektronskih komunikacijskih omrežij, vključno s šifriranjem od konca do konca, kjer je to ustrezno; poudarja, da imajo v primeru neskladnosti proizvodov na trgu EU države članice v skladu z evropskim zakonikom o elektronskih komunikacijah obsežna pooblastila za preiskovanje teh proizvodov in uporabo številnih pravnih sredstev;

19. poziva Komisijo in države članice, naj v vseh postopkih javnih naročil za ustrezno infrastrukturo zagotovijo, da bo varnost obvezen vidik tako na ravni EU kot na nacionalni ravni;

20. države članice opozarja na njihovo obveznost iz pravnega okvira EU, zlasti Direktive 2013/40/EU o napadih na informacijske sisteme, da naložijo sankcije pravnim osebam, ki so storile kazniva dejanja, kot so napadi na take sisteme; poudarja, da bi morale države članice uporabiti tudi možnost nalaganja drugih sankcij tem pravnim osebam, kot so začasna ali stalna izključitev iz opravljanja komercialnih dejavnosti;

21. poziva države članice, agencije za kibernetsko varnost, telekomunikacijske operaterje, proizvajalce in ponudnike storitev kritične infrastrukture, naj Komisiji in agenciji ENISA sporočijo morebitne dokaze o stranskih vratih ali drugih večjih šibkih točkah, ki bi lahko ogrozili celovitost in varnost telekomunikacijskih omrežij ali kršili pravo in temeljne pravice Unije; pričakuje, da bodo nacionalni organi za varstvo podatkov in

evropski nadzornik za varstvo podatkov temeljito preučili navedbe o kršitvah varstva osebnih podatkov zunanjih prodajalcev ter naložili ustrezne kazni in sankcije v skladu z evropsko zakonodajo o varstvu podatkov;

22. pozdravlja skorajšnji začetek veljavnosti uredbe o vzpostavitvi okvira za pregled neposrednih tujih naložb zaradi varnosti in javnega reda ter poudarja, da ta uredba prvič uvaja seznam področij in dejavnikov, vključno s komunikacijami in kibernetsko varnostjo, ki so pomembni za varnost in javni red na ravni EU;

23. poziva Svet, naj pospeši delo v zvezi s predlagano uredbo o e-zasebnosti;

24. ponavlja, da mora EU podpirati kibernetsko varnost v celotni vrednostni verigi, od raziskav do uvedbe in uporabe ključnih tehnologij, razširjati ustrezne informacije ter spodbujati kibernetsko higieno in učne načrte, ki vključujejo kibernetsko varnost, ter meni, da bo program za digitalno Evropo skupaj z drugimi ukrepi učinkovito orodje za to;

25. poziva Komisijo in države članice, naj sprejmejo potrebne ukrepe, vključno s trdnimi naložbenimi shemami, za vzpostavitev inovacijam prijaznega okolja v EU, ki bi moralo biti dostopno vsem podjetjem v digitalnem gospodarstvu EU, vključno z malimi in srednjimi podjetji; poziva tudi, da bi moralo tako okolje evropskim prodajalcem omogočiti, da razvijejo nove proizvode, storitve in tehnologije, kar bi jim omogočilo konkurenčnost;

26. poziva Komisijo in države članice, naj upoštevajo zgornje zahteve v okviru bližajočih se razprav o prihodnji strategiji za odnose med EU in Kitajsko, saj gre za pogoje, ki so nujni za ohranitev konkurenčnosti EU in zagotavljanje varnosti njene digitalne infrastrukture;

27. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu in Komisiji.