Europa-Parlamentet
2014-2019

Mødedokument

B8-0153/2019

6.3.2019

FORSLAG TIL BESLUTNING

på baggrund af Rådets og Kommissionens redegørelser

jf. forretningsordenens artikel 123, stk. 2

om sikkerhedstrusler forbundet med den stigende kinesiske teknologiske tilstedeværelse i EU og mulige foranstaltninger på EU-plan til at mindske dem (2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
for EFDD-Gruppen

B8-0153/2019

Europa-Parlamentets beslutning om sikkerhedstrusler forbundet med den stigende kinesiske teknologiske tilstedeværelse i EU og mulige foranstaltninger på EU-plan til at mindske dem
(2019/2575(RSP))

Europa-Parlamentet,

– der henviser til Kommissionens meddelelser af 14. september 2016, henholdsvist "Konnektivitet med henblik på et konkurrencedygtigt digitalt indre marked – På vej mod et europæisk gigabitsamfund" (COM(2016)0587) og "5G til Europa: En handlingsplan" (COM(2016)0588),

– der henviser til Kommissionens ændrede forslag til Europa-Parlamentets og Rådets forordning af 29. januar 2016 om adgangen for tredjelandes varer og tjenesteydelser til Unionens indre marked for offentlige indkøb og procedurer for støtte til forhandlingerne om adgang for Unionens varer og tjenesteydelser til tredjelandes markeder for offentlige indkøb (COM(2016)0034),

– der henviser til Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele Unionen (NIS-direktivet)[1],

– der henviser til forslaget af 13. september 2017 til Europa-Parlamentets og Rådets forordning om ENISA, "EU's Agentur for Cybersikkerhed", og om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed") (COM(2017)0477),

– der henviser til Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation[2],

– der henviser til Kommissionens forslag af 12. september 2018 til Europa-Parlamentets og Rådets forordning om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre (COM(2018)0630),

– der henviser til WTO's tvistbilæggelsessag (WT/DS549/6) af 1. juni 2018 om visse af Kinas foranstaltninger vedrørende overførsel af udenlandsk teknologi til Kina,

– der henviser til sin holdning, der blev vedtaget ved førstebehandlingen den 14. februar 2019, om forslag til Europa-Parlamentets og Rådets forordning om et regelsæt for screening af udenlandske direkte investeringer i Den Europæiske Union[3],

[1] EUT L 194 af 19.7.2016, s. 1.
[2] EUT L 321 af 17.12.2018, s. 36.
[3] Vedtagne tekster, P8_TA(2019)0121.

– der henviser til de igangværende forhandlinger mellem EU og Kina om en omfattende investeringsaftale,

– der henviser til forretningsordenens artikel 123, stk. 2,

A. der henviser til, at nylige fremskridt inden for ikt, herunder femte generation af telekommunikation (5G), har banet vej for produktion, distribution og realisering af varer og tjenesteydelser og for interaktion mellem apparater og borgere, offentlige forvaltninger og andre samfundsøkonomiske aktører og dermed har potentiale til at sætte skub i den europæiske økonomi;

B. der henviser til, at cybersikkerhed inden for ikt, beskyttelse af følsomme oplysninger, respekt for individuelle rettigheder og beskyttelse mod eksterne cybertrusler er en forudsætning for at sikre EU-borgernes teknologiske suverænitet og i sidste ende tilsikre velstand i EU og støtte demokratiet i Unionen;

C. der henviser til, at 5G-forskningen og -testning knap nok holder trit med det internationale pres for at opstille og markedsføringen 5G-teknologien, mens en række videnskabelige undersøgelser har givet anledning til bekymring og usikkerhed med hensyn til såvel datasikkerhed og personsikkerhed, navnlig med hensyn til risikoen for elektromagnetisk forurening for menneskers sundhed og miljøet;

D. der henviser til, at sikring af cybersikkerhed for 5G-netværk er en ny og kompleks udfordring på grund af 5G's digitalbaserede og decentraliserede karakter og dens fragmenterede og meget specialiserede værdikæde, både hvad angår produktion, afsendelse, installation, konfiguration, drift, vedligeholdelse og softwareopdateringer; der henviser til, at EU er nødt til at udbedre manglerne ved cybersikkerhed i sin kritiske infrastruktur inden for bl.a. telekommunikation, energi, transport, sundhed, forsvar og sikkerhed;

E. der henviser til, at sikring af sikre 5G-net er en opgave, der ikke kan udføres af individuelle fabrikanter eller systemoperatører, men kræver en effektiv koordineret indsats fra alle relevante nationale og internationale myndigheders side;

F. der henviser til, at EU har potentiale til at lede udviklingen af cybersikkerhedsteknologier ved at støtte europæiske virksomheder i denne sektor og fremme alle ændringer i værdikæden, som kan mindske EU's afhængighed af udenlandsk teknologi;

G. der henviser til, at EU har udviklet en række foranstaltninger til at sikre cybersikkerhed, herunder NIS-direktivet og forordningen om cybersikkerhed, som bør gennemføres hurtigt og overvåges løbende for at sikre, at de forbliver virkningsfulde i alle de nødvendige opdateringer og revisioner;

H. der henviser til, at en øget tilstedeværelse af kinesiske og andre tredjelandsleverandører af teknologi er blevet tydelig på EU's 5G-marked, navnlig af statsejede virksomheder eller virksomheder, der mangler gennemsigtighed;

I. der henviser til, at gensidighed er en af de mest effektive måder at gøre fremskridt på i retning af lige vilkår på globalt plan;

J. der henviser til, at udenlandske virksomheder skal håndtere det nuværende hul i EU's databeskyttelsesstandarder mellem den generelle forordning om databeskyttelse og de forskellige krav i den nationale lovgivning;

K. der henviser til, at EU og Kina har forhandlet om en omfattende investeringsaftale siden 2013; der henviser til, at den foreslåede aftale vil bidrage til at løse problemer vedrørende markedsadgang, etablere en ramme for investeringsbeskyttelse og fastsætte grundlæggende arbejds- og miljøstandarder;

L. der henviser til, at der foreligger beviser, der, endskønt de ikke er entydige, peger i retning af, at det udstyr, som leveres af leverandører fra tredjelande, herunder Kina, kan bringe den enkeltes ret til privatlivets fred og beskyttelse af følsomme oplysninger i EU i fare;

1. understreger, at indførelsen og markedsføringen af 5G bør gennemføres i overensstemmelse med forsigtighedsprincippet, hvor alle socioøkonomiske aktører foregriber potentielle sikkerhedsmæssige konsekvenser og træffer forholdsmæssige foranstaltninger, herunder hurtig offentliggørelse af faktorer, der kan være til fare for folkesundheden eller miljøet;

2. understreger, at de sociale og økonomiske konsekvenser af 5G og af de teknologier, som det muliggør, fra tingenes internet til kunstig intelligens, bør vurderes grundigt, og at der bør træffes foranstaltninger med henblik på at sikre, at overgangen til det europæiske gigabitsamfund finder sted på en måde, der er fair og ens for alle og baseret på et etisk ansvar;

3. opfordrer Kommissionen og medlemsstaterne til at skabe et innovationsvenligt miljø for EU's leverandører med henblik på at udvikle nye produkter, tjenester og teknologier og støtte EU's iværksætterånd i udbredelsen og markedsføringen af sikre og sikre 5G, samtidig med at det sikres, at dets potentiale er tilgængeligt for alle virksomheder i EU's digitale økonomi, herunder små og mellemstore virksomheder;

4. minder om, at cybersikkerhed er en af de vigtigste problematikker, som EU i øjeblikket står over for, og at manglende formåen desangående kan resultere i krænkelse af privatlivets fred og af EU's forbrugeres og producenters grundlæggende rettigheder samt i alvorlig grad undergrave borgernes tillid til ikt-produkter og -tjenester og i sidste ende forårsage alvorlige økonomiske skader; efterlyser et netværk, hvor sikkerheden er indbygget via standardindstillinger og teknisk udformning;

5. opfordrer Kommissionen og medlemsstaterne til at arbejde tæt sammen om at gennemføre EU's strategi for cybersikkerhed og til at kombinere EU- og medlemsstatsforanstaltninger for at minimere risikoen for brud på sikkerheden og brud på datasikkerheden i hele værdikæden; mener, at sådanne foranstaltninger kan omfatte EU's cybersikkerhedscertificering, konfigurationskrav og operationelle procedurer og praksisser samt fremme af cyberhygiejne og digital uddannelse;

6. mener, at EU's Agentur for Cybersikkerhed (Den Europæiske Unions Agentur for Net- og Informationssikkerhed – ENISA) har en afgørende rolle at spille med hensyn til at analysere mulige trusler fra udenlandske salgsudbydere, herunder Kina, og koordinere en fælles tilgang mellem medlemsstaterne med henblik på at tackle

cybersikkerhedstrusler og -angreb;

7. opfordrer Kommissionen og medlemsstaterne til hurtigt at gennemføre pakken om cirkulær økonomi og fremme forvaltningen af råstoffer gennem hele deres livscyklus såvel som genanvendelse af affald med henblik på at forbedre EU's adgang til kritiske råstoffer, som er afgørende for højteknologiske produkter og innovationer;

8. mener, at det haster med at håndtere de mulige teknologiske sikkerhedstrusler, som skyldes udenlandske virksomheders, herunder Kinas, nuværende markedsindtrængning i EU ved at anvende en fælles tilgang til sikkerhed og databeskyttelse mellem medlemsstaterne;

9. opfordrer Kommissionen og medlemsstaterne til at analysere og overvåge sikkerheden i de ikt-systemer, hvor teknologier fra tredjelande er stærkt til stede, også ved at gennemføre stresstest;

10. understreger, at tredjelandsleverandører ikke bør udsættes for forskelsbehandling på grund af deres oprindelsesland, men at gennemsigtigheden af disse virksomheder, deres cybersikkerhedsstandarder og eksistensen af gensidige vilkår for europæiske virksomheder i oprindelseslandet bør tages i betragtning med henblik på at sikre lige konkurrencevilkår;

11. understreger, at hverken kinesiske eller andre leverandører og operatører fra tredjelande under nogen omstændigheder må bringe de individuelle rettigheder, der er garanteret i henhold til EU-retten, i fare, heller ikke selv om der måtte gælde andre krav i henhold til deres oprindelseslands nationale ret;

12. anmoder Rådet om på imødekommende vis as genoverveje at genoptage drøftelserne om det nye reviderede forslag fra Kommissionen om den procedure, der begrænser adgangen for udenlandske produkter til EU's marked for offentlige indkøb, hvor der mangler gensidig adgang;

13. minder om betydningen af yderligere at forbedre forhandlingerne med tredjelande om reguleringssamarbejde om digital teknologi og af at sikre større engagement fra disses side i internationale standardiseringsorganer;

14. pålægger sin formand at sende denne beslutning til Rådet og Kommissionen.