



---

*Plenarhandling*

---

**B8-0153/2019**

6.3.2019

# FÖRSLAG TILL RESOLUTION

till följd av uttalanden av rådet och kommissionen

i enlighet med artikel 123.2 i arbetsordningen

om säkerhetshot kopplade till Kinas ökande teknologiska närvaro i EU och  
möjliga åtgärder på EU-nivå för att minska dem  
(2019/2575(RSP))

**Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas**  
för EFDD-gruppen

**Europaparlamentets resolution om säkerhetshot kopplade till Kinas ökande teknologiska närvaro i EU och möjliga åtgärder på EU-nivå för att minska dem (2019/2575(RSP))**

*Europaparlamentet utfärdar denna resolution*

- med beaktande av kommissionens meddelanden av den 14 september 2016 *Konnektivitet för en konkurrenskraftig digital inre marknad – mot ett europeiskt gigabitsamhälle* (COM(2016)0587) och *5G för Europa: en handlingsplan* (COM(2016)0588),
- med beaktande av kommissionens ändrade förslag till Europaparlamentets och rådets förordning av den 29 januari 2016 om tillträdet för varor och tjänster från tredjeländer till unionens inre marknad för offentlig upphandling och förfaranden till stöd för förhandlingar om tillträde för varor och tjänster från unionen till tredjeländers marknader för offentlig upphandling (COM(2016)0034),
- med beaktande av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen<sup>1</sup> (NIS-direktivet),
- med beaktande av förslaget av den 13 september 2017 till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013 och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) (COM(2017)0477),
- med beaktande av Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation<sup>2</sup>,
- med beaktande av kommissionens förslag av den 12 september 2018 till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (COM(2018)0630),
- med beaktande av WTO:s tvistlösningsärende (WT/DS549/6) av den 1 juni 2018 om vissa åtgärder som Kina infört avseende överföring av utländsk teknik till Kina,
- med beaktande av sin ståndpunkt fastställd vid första behandlingen den 14 februari 2019 om förslaget till Europaparlamentets och rådets förordning om upprättande av en ram för granskning av utländska direktinvesteringar i Europeiska unionen<sup>3</sup>,

---

<sup>1</sup> EUT L 194, 19.7.2016, s. 1.

<sup>2</sup> EUT L 321, 17.12.2018, s. 36.

<sup>3</sup> Antagna texter, P8\_TA(2019)0121.

- med beaktande av de pågående förhandlingarna mellan EU och Kina om ett övergripande investeringsavtal,
- med beaktande av artikel 123.2 i arbetsordningen, och av följande skäl:
  - A. Den senaste utvecklingen inom informations- och kommunikationstekniken (IKT), däribland den femte generationens telekommunikation (5G), har banat väg för nya former för produktion, distribution och åtnjutande av varor och tjänster, och för interaktion mellan enheter och mellan medborgare, offentliga förvaltningar och andra socioekonomiska aktörer, och har därmed potential att stimulera den europeiska ekonomin.
  - B. Cybersäkerhet inom IKT, skydd av känslig information, respekt för individuella rättigheter och skydd mot externa cyberhot är förutsättningar för att säkra EU-medborgarnas tekniska suveränitet och i slutändan skapa välstånd och stödja demokratin i EU.
  - C. Forskningen inom och provningen av 5G lyckas knappt hålla jämna steg med det internationella trycket för utbyggnad och kommersialisering av 5G, samtidigt som ett antal vetenskapliga studier har väckt farhågor och osäkerhet när det gäller både säkerheten och tryggheten med tekniken, särskilt i fråga om riskerna med elektromagnetiska föroreningar för människors hälsa och miljön.
  - D. Att säkerställa cybersäkerhet för 5G-nät är en ny och komplex utmaning på grund av 5G-teknikens virtualiserade och decentraliserade natur och dess fragmenterade och väldigt specialiserade värdekedja, från produktion till leverans, installation, konfiguration, drift, underhåll och programvaruuppdateringar. EU behöver fylla igen den brist på cybersäkerhet som finns i dess grundläggande infrastruktur inom sektorerna telekommunikation, energi, transport, hälso- och sjukvård, försvar och säkerhet, bland andra.
  - E. Att säkerställa trygga och säkra 5G-nät är en uppgift som inte kan utföras av enskilda tillverkare eller systemoperatörer, utan som kräver effektiva samordnade åtgärder av alla relevanta nationella och internationella myndigheter.
  - F. EU har potential att leda utvecklingen av teknik för cybersäkerhet genom att stödja europeiska företag inom denna sektor och främja alla förändringar i värdekedjan som skulle kunna minska EU:s beroende av utländsk teknik.
  - G. EU har utvecklat en uppsättning åtgärder för att säkerställa cybersäkerhet, däribland direktivet om nät- och informationssäkerhet och cybersäkerhetsakten, som snabbt bör genomföras och kontinuerligt övervakas för att säkerställa att de förblir ändamålsenliga igenom alla nödvändiga uppdateringar och översyner.
  - H. Den ökade närvaron av teknikleverantörer från Kina och andra tredjeländer har blivit uppenbar på EU:s 5G-marknad, särskilt när det gäller statligt ägda företag eller företag som saknar transparens.
  - I. Ömsesidighet är ett av de mest effektiva sätten att göra framsteg på vägen mot lika villkor på global nivå.

- J. De utländska företagen måste hantera den nuvarande luckan i EU:s dataskyddsnormer mellan å ena sidan den allmänna dataskyddsförordningen och å andra sidan olika krav enligt nationella lagar.
- K. EU och Kina har förhandlat om ett övergripande investeringsavtal sedan 2013. Den föreslagna uppgörelsen skulle bidra till att lösa frågor som rör marknadstillträde, inrätta en ram för investeringsskydd och fastställa grundläggande arbetsrättsliga och miljömässiga normer.
- L. Det har uppstått bevis, även om det inte går att dra några säkra slutsatser utifrån dem, i fråga om säkerhetsluckor i den utrustning som tillhandahålls av leverantörer från tredjeländer, däribland Kina, vilket skulle kunna äventyra den enskildes rätt till personlig integritet och skyddet av känslig information i EU.
1. Europaparlamentet betonar att utbyggnaden och kommersialiseringen av 5G bör genomföras i enlighet med försiktighetsprincipen, där alla socioekonomiska aktörers förutser möjliga konsekvenser för tryggheten och säkerheten och vidtar proportionella försiktighetsåtgärder, däribland ett snabbt offentliggörande av faktorer som kan äventyra folkhälsan eller miljön.
  2. Europaparlamentet betonar att de sociala och ekonomiska konsekvenserna av 5G och av den teknik som möjliggörs av 5G, allt från sakernas internet till artificiell intelligens, bör utvärderas noggrant och att åtgärder bör vidtas för att övergången till ett europeiskt gigabitsamhälle ska ske på ett rättvist och likvärdigt sätt för alla och på grundval av etiskt ansvar.
  3. Europaparlamentet uppmanar kommissionen och medlemsstaterna att skapa en innovationsvänlig miljö för EU:s leverantörer att utveckla nya produkter och tjänster och ny teknik, och att stödja entreprenörskap från EU i samband med utbyggnad och kommersialisering av trygg och säker 5G-teknik, samtidigt som det säkerställs att den teknikens potential är tillgänglig för alla företag i EU:s digitala ekonomi, även små och medelstora företag.
  4. Europaparlamentet påminner om att cybersäkerhet är en av de största utmaningar som EU för närvarande står inför och att ett misslyckande på detta område skulle kunna kränka EU:s konsumenters och producenters integritet och grundläggande rättigheter, allvarligt undergräva medborgarnas förtroende för produkter och tjänster inom IKT, och i slutändan orsaka allvarlig ekonomisk skada. Parlamentet efterlyser ett nätverk med automatisk och inbyggd säkerhet.
  5. Europaparlamentet uppmanar kommissionen och medlemsstaterna att ha ett nära samarbete vid genomförandet av EU:s strategi för cybersäkerhet och att kombinera EU-åtgärder och nationella åtgärder för att minimera risken för säkerhetsbrister och personuppgiftsbrott längs hela värdekedjan. Parlamentet anser att sådana åtgärder skulle kunna omfatta EU:s cybersäkerhetscertifiering, konfigurationskrav och operativa förfaranden och rutiner samt främjandet av it-hygien och digital utbildning.
  6. Europaparlamentet anser att EU:s byrå för cybersäkerhet (Europeiska unionens byrå för nät- och informationssäkerhet – Enisa) har en avgörande roll att spela när det gäller att analysera möjliga hot från utländska leverantörer, däribland Kina, och samordna

en gemensam strategi mellan medlemsstaterna för att ta itu med cyberhot och it-angrepp.

7. Europaparlamentet uppmanar kommissionen och medlemsstaterna att snabbt genomföra paketet om cirkulär ekonomi och förbättra hanteringen av råvaror under deras hela livscykel samt återvinningen av avfall, för att förbättra EU:s tillgång till viktiga råvaror som är grundläggande för högteknologiska produkter och nya innovationer.
8. Europaparlamentet anser att det är brådskande att hantera de eventuella tekniska säkerhetshot som följer av det nuvarande genomslaget på EU-marknaden av utländska leverantörer, däribland Kina, genom att anta en gemensam strategi för säkerhet och uppgiftsskydd mellan medlemsstaterna.
9. Europaparlamentet uppmanar kommissionen och medlemsstaterna att analysera och övervaka säkerheten i de IKT-system i vilka teknik från tredjeländer är starkt förekommande, också genom att utföra stresstester.
10. Europaparlamentet betonar att leverantörer från tredjeländer inte bör diskrimineras på grund av sitt ursprungsland, men att insyn i dessa företag, deras cybersäkerhetsstandarder och förekomsten av ömsesidiga villkor för europeiska företag i ursprungslandet bör beaktas för att säkerställa lika villkor.
11. Europaparlamentet betonar att leverantörer och operatörer från Kina eller andra tredjeländer under inga omständigheter får äventyra de individuella rättigheter som garanteras enligt EU-lagstiftningen, inte ens om det finns annorlunda krav i nationell rätt i deras ursprungsland.
12. Europaparlamentet uppmanar rådet att positivt överväga att återuppta diskussionerna om det nya omarbetade kommissionsförslaget om det förfarande som inskränker tillträdet för utländska produkter till EU:s marknad för upphandling där det råder brist på ömsesidigt tillträde.
13. Europaparlamentet påminner om vikten av att ytterligare förbättra förhandlingarna om regleringssamarbete med tredjeländer i fråga om digital teknik, och av att säkerställa ett större engagemang från deras sida i internationella standardiseringsorgan.
14. Europaparlamentet uppdrar åt talmannen att översända denna resolution till rådet och kommissionen.