Europees Parlement
2014-2019

Zittingsdocument

B8-0153/2019

6.3.2019

ONTWERPRESOLUTIE

naar aanleiding van verklaringen van de Raad en de Commissie

ingediend overeenkomstig artikel 123, lid 2, van het Reglement

over de veiligheidsdreigingen in verband met de toenemende technologische aanwezigheid van China in de EU en mogelijke maatregelen op EU-niveau om deze tegen te gaan
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
namens de EFDD-Fractie

B8-0153/2019

Resolutie van het Europees Parlement over de veiligheidsdreigingen in verband met de toenemende technologische aanwezigheid van China in de EU en mogelijke maatregelen op EU-niveau om deze tegen te gaan
(2019/2575(RSP))

Het Europees Parlement,

– gezien de mededelingen van de Commissie van 14 september 2016 getiteld "Connectiviteit voor een competitieve digitale eengemaakte markt – Naar een Europese gigabitmaatschappij" (COM(2016)0587) en "5G voor Europa: een actieplan" (COM(2016)0588),

– gezien het gewijzigde voorstel van de Commissie van 29 januari 2016 voor een verordening van het Europees Parlement en de Raad over toegang van goederen en diensten uit derde landen tot de interne aanbestedingsmarkt van de Unie en procedures tot ondersteuning van onderhandelingen over toegang van goederen en diensten uit de Unie tot de aanbestedingsmarkten van derde landen (COM(2016)0034),

– gezien Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn)[1],

– gezien het voorstel van de Commissie van 13 september 2017 voor een verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (cyberbeveiligingsverordening) (COM(2017)0477),

– gezien Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie[2],

– gezien het voorstel voor een verordening van het Europees Parlement en de Raad van 12 september 2018 tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (COM(2018)0630),

– gezien de WTO-geschillenbeslechtingsprocedure (WT/DS549/6) van 1 juni 2018 betreffende bepaalde maatregelen die China heeft opgelegd in verband met de overdracht van buitenlandse technologie naar China,

– onder verwijzing naar zijn standpunt vastgesteld in eerste lezing op 14 februari 2019 over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in

[1] PB L 194 van 19.7.2016, blz. 1.
[2] PB L 321 van 17.12.2018, blz. 36.

de Europese Unie[3],

– gezien de lopende onderhandelingen tussen de EU en China over een brede investeringsovereenkomst,

– gezien artikel 123, lid 2, van zijn Reglement,

A. overwegende dat de recente ontwikkelingen op ICT-gebied, waaronder telecommunicatie van de vijfde generatie (5G), nieuwe wegen hebben gebaand voor de productie, de distributie en het gebruik van goederen en diensten en voor de interactie tussen apparaten en tussen burgers, overheidsdiensten en andere sociaal-economische actoren, en aldus het potentieel hebben om de Europese economie te stimuleren;

B. overwegende dat cyberbeveiliging bij ICT, bescherming van gevoelige informatie, eerbiediging van individuele rechten en bescherming tegen externe cyberdreigingen noodzakelijke voorwaarden zijn om de technologische soevereiniteit van de EU-burgers te waarborgen en uiteindelijk welvaart te brengen en de democratie te ondersteunen in de EU;

C. overwegende dat het onderzoek en de tests op het gebied van 5G nauwelijks gelijke tred kunnen houden met de internationale druk om 5G uit te rollen en op de markt te brengen, terwijl in aantal wetenschappelijke studies sprake is van bezorgdheid en onzekerheid over zowel de beveiliging als de veiligheid van 5G, met name wat betreft de risico's van elektromagnetische vervuiling voor de menselijke gezondheid en het milieu;

D. overwegende dat het waarborgen van de cyberbeveiliging van 5G-netwerken een nieuwe en complexe uitdaging is als gevolg van de gevirtualiseerde en gedecentraliseerde aard van 5G en de gefragmenteerde en zeer gespecialiseerde waardeketen, van productie tot verzending, installatie, configuratie, exploitatie, onderhoud en software-updates; overwegende dat de EU de leemte in haar kritieke infrastructuur in onder meer de sectoren telecommunicatie, energie, vervoer, gezondheid, defensie en beveiliging moet opvullen;

E. overwegende dat het waarborgen van veilige en beveiligde 5G-netwerken een taak is die niet door afzonderlijke fabrikanten of systeemexploitanten kan worden uitgevoerd, maar een doeltreffend gecoördineerd optreden van alle betrokken nationale en internationale autoriteiten vereist;

F. overwegende dat de EU het potentieel heeft om het voortouw te nemen bij de ontwikkeling van cyberbeveiligingstechnologie door Europese ondernemingen in deze sector te ondersteunen en alle veranderingen in de waardeketen te bevorderen waardoor de EU minder afhankelijk kan worden van buitenlandse technologie;

G. overwegende dat de EU een reeks maatregelen heeft ontwikkeld om cyberbeveiliging te waarborgen, waaronder de NIS-richtlijn en de cyberbeveiligingsverordening, die snel ten uitvoer moeten worden gelegd en voortdurend moeten worden gemonitord opdat ze

[3] Aangenomen teksten, P8_TA(2019)0121.

door de nodige updates en evaluaties doeltreffend blijven;

H. overwegende dat er op de 5G-markt in de EU steeds meer technologieleveranciers uit China en andere derde landen aanwezig zijn, met name staatsbedrijven of ondernemingen die onvoldoende transparant zijn;

I. overwegende dat wederkerigheid een van de meest effectieve manieren is om vooruitgang te boeken in de richting van een wereldwijd gelijk speelveld;

J. overwegende dat buitenlandse bedrijven te maken krijgen met de huidige discrepantie in de EU-normen voor gegevensbescherming tussen de algemene verordening gegevensbescherming en de verschillende nationale wettelijke voorschriften;

K. overwegende dat de EU en China sinds 2013 onderhandelen over een brede investeringsovereenkomst; overwegende dat de voorgestelde overeenkomst zou helpen om problemen met de toegang tot de markt op te lossen, een kader voor de bescherming van investeringen tot stand te brengen en fundamentele arbeids- en milieunormen vast te stellen;

L. overwegende dat er weliswaar geen harde bewijzen, maar wel aanwijzingen zijn dat de beveiliging van de door leveranciers uit derde landen, waaronder China, geleverde apparatuur tekortkomingen vertoont, waardoor de individuele rechten op privacy en de bescherming van gevoelige informatie in de EU in gevaar zouden kunnen komen;

1. benadrukt dat de uitrol en het op de markt brengen van 5G moeten plaatsvinden in overeenstemming met het voorzorgsbeginsel, zodat alle sociaal-economische actoren kunnen anticiperen op mogelijke gevolgen voor de veiligheid en beveiliging en evenredige voorzorgsmaatregelen kunnen nemen, zoals het onverwijld openbaar maken van factoren die een gevaar kunnen vormen voor de volksgezondheid of het milieu;

2. benadrukt dat de sociale en economische effecten van 5G en van de technologie die 5G mogelijk maakt, van het internet van de dingen tot kunstmatige intelligentie, grondig moeten worden beoordeeld en dat er maatregelen moeten worden genomen om ervoor te zorgen dat de overgang naar de Europese gigabitmaatschappij plaatsvindt op een billijke en voor iedereen gelijke wijze en op basis van ethische verantwoordelijkheid;

3. vraagt de Commissie en de lidstaten een innovatievriendelijk klimaat te creëren waarin verkopers in de EU nieuwe producten, diensten en technologieën kunnen ontwikkelen, en ondernemerschap in de EU te ondersteunen bij de uitrol en het op de markt brengen van veilige en beveiligde 5G, en er tegelijk voor te zorgen dat het potentieel van 5G toegankelijk is voor alle bedrijven in de digitale economie van de EU, ook kleine en middelgrote ondernemingen;

4. herinnert eraan dat cyberbeveiliging een van de belangrijkste uitdagingen is waarmee de EU momenteel wordt geconfronteerd en dat een mislukking op dit gebied de privacy en de fundamentele rechten van consumenten en producenten in de EU zou kunnen schenden, het vertrouwen van de burgers in ICT-producten en -diensten ernstig zou kunnen ondermijnen en uiteindelijk ernstige economische schade zou kunnen veroorzaken; dringt aan op een netwerk dat zowel door standaardinstellingen als door ontwerp veilig is;

5. vraagt de Commissie en de lidstaten nauw samen te werken bij de tenuitvoerlegging van de EU-strategie inzake cyberbeveiliging en EU-maatregelen met nationale maatregelen te combineren om het risico van tekortkomingen in de beveiliging en inbreuken in verband met gegevens in de hele waardeketen tot een minimum te beperken; meent dat dergelijke maatregelen onder meer kunnen bestaan uit EU-certificering van cyberbeveiliging, configuratievoorschriften en operationele procedures en praktijken, alsook de bevordering van cyberhygiëne en digitale educatie;

6. is van mening dat het EU-agentschap voor cyberbeveiliging (het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging – ENISA) een cruciale rol te spelen heeft bij het analyseren van mogelijke dreigingen in verband met buitenlandse verkopers, waaronder China, en het coördineren van een gemeenschappelijke aanpak tussen de lidstaten om cyberdreigingen en -aanvallen tegen te gaan;

7. vraagt de Commissie en de lidstaten het pakket circulaire economie snel ten uitvoer te leggen en grondstoffenbeheer gedurende de hele levenscyclus van grondstoffen alsook afvalrecycling te stimuleren, teneinde de EU een betere toegang te bieden tot kritieke grondstoffen, die van fundamenteel belang zijn voor hightechproducten en opkomende innovaties;

8. vindt dat de mogelijke technologische beveiligingsrisico's in verband met de huidige penetratie van buitenlandse verkopers, waaronder China, op de EU-markt dringend moeten worden aangepakt door een gemeenschappelijke aanpak van de lidstaten inzake beveiliging en gegevensbescherming;

9. verzoekt de Commissie en de lidstaten de veiligheid van ICT-systemen waarin veel technologie uit derde landen aanwezig is, te analyseren en te monitoren, onder meer door middel van stresstests;

10. benadrukt dat leveranciers uit derde landen niet mogen worden gediscrimineerd op grond van hun land van herkomst, maar dat rekening moet worden gehouden met de transparantie van deze bedrijven, hun normen op het gebied van cyberbeveiliging en het bestaan van wederzijdse voorwaarden voor Europese bedrijven in het land van herkomst, teneinde een gelijk speelveld te waarborgen;

11. benadrukt dat leveranciers en exploitanten uit China of andere derde landen in geen geval de door de EU-wetgeving gewaarborgde individuele rechten in gevaar mogen brengen, ook al gelden in hun land van oorsprong andere voorschriften krachtens de nationale wetgeving;

12. verzoekt de Raad de heropening van de besprekingen over het nieuwe herziene voorstel van de Commissie over de procedure om de toegang van buitenlandse producten tot de EU-markt voor overheidsopdrachten te beperken als de toegang niet wederkerig is, welwillend te overwegen;

13. wijst nogmaals op het belang van een verdere verbetering van de onderhandelingen met derde landen over samenwerking op het gebied van de regelgeving inzake digitale technologie en van een grotere betrokkenheid van deze landen bij internationale normalisatie-instellingen;

14. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad en de Commissie.