Europees Parlement
2014-2019

Zittingsdocument

B8-0159/2019

6.3.2019

ONTWERPRESOLUTIE

naar aanleiding van verklaringen van de Raad en de Commissie

ingediend overeenkomstig artikel 123, lid 2, van het Reglement

over het gevaar voor de veiligheid in verband met de toenemende technologische aanwezigheid van China in de EU en mogelijke maatregelen op EU-niveau om dit tegen te gaan
(2019/2575(RSP))

Dan Nica, Peter Kouroumbashev
namens de S&D-Fractie

B8-0159/2019

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

Het Europees Parlement,

– 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[1],

– 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[2],

– 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 ("de cyberbeveiligingsverordening") (COM(2017)0477),

– gezien het voorstel voor een verordening 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 goedkeuring van de nieuwe nationale inlichtingenwet door het Chinese Nationale Volkscongres op 28 juni 2017,

– gezien de verklaringen van de Raad en de Commissie van 13 februari 2019 over het gevaar voor de veiligheid in verband met de toenemende technologische aanwezigheid van China in de EU en mogelijke maatregelen op EU-niveau om dit tegen te gaan

– 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 de Europese Unie[3],

– gezien zijn resolutie van 12 september 2018 over de stand van zaken van de betrekkingen tussen de EU en China[4],

– gezien de mededeling van de Commissie van 14 september 2016 met als titel "5G voor Europa: een actieplan" (COM(2016)0588),

[1] PB L 321 van 17.12.2018, blz. 36.
[2] PB L 194 van 19.7.2016, blz. 1.
[3] Aangenomen teksten, P8_TA-PROV(2019)0121.
[4] Aangenomen teksten, P8_TA-PROV(2018)0343.

– gezien zijn resolutie met als titel "Internettoegang voor groei, concurrentievermogen en cohesie: Europese gigabitmaatschappij en 5G" die is goedgekeurd op 1 juni 2017[5],

– gezien Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming),

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

A. overwegende dat het 5G-netwerk de ruggengraat zal worden van onze digitale infrastructuur, door connectiviteit en gegevens te verschaffen in het dagelijks leven naast kritieke sectoren van de economie, zoals vervoer, energie, gezondheid, financiën, telecommunicatie, defensie, ruimtevaart en de veiligheidssector;

B. overwegende dat de kosten voor de uitrol van 5G in Europa naar schatting tussen 300 miljard en 500 miljard EUR zullen liggen, waardoor deze netwerken na de uitrol op korte termijn moeilijk te vervangen zullen zijn;

C. overwegende dat 5G-apparatuur wordt aangeboden door slechts een beperkt aantal bedrijven, vooral uit China en de Europese Unie;

D. overwegende dat een aantal derde landen een verbod heeft ingesteld op in China vervaardigde 5G-apparatuur of voornemens is voor deze apparatuur beperkingen in te voeren;

E. overwegende dat momenteel geen enkele EU-lidstaat publiekelijk heeft verklaard dat zijn telecommunicatienetwerken geïntegreerde achterdeurtjes bevatten;

F. overwegende dat in de lidstaten het veilingproces aan de gang is voor de verkoop van spectrum bij opbod met het oog op de uitrol van 5G vóór 31 december 2020, zoals vereist in het Europees wetboek voor elektronische communicatie;

G. overwegende dat Chinese burgers en entiteiten op grond van de Chinese inlichtingenwet van 2017 verplicht zijn de Chinese regering toegang te verlenen tot particuliere gegevens om redenen in verband met de nationale veiligheid of nationale belangen;

H. overwegende dat de Chinese wet inzake cyberveiligheid, die in werking is getreden op 1 juni 2017, bepaalt dat netwerkexploitanten de veiligheidsorganen van de overheid bij hun werkzaamheden technische bijstand moeten verlenen;

I. overwegende dat soortgelijke wetgeving is aangenomen in andere derde landen, met name in de VS, met de recente goedkeuring van de Clarifying Lawful Overseas Use of Data Act (CLOUD-wet), die Amerikaanse data- en communicatiebedrijven verplicht tot het verstrekken van de gegevens van Amerikaanse burgers die opgeslagen zijn op elke server die zij bezitten en gebruiken, wanneer hier door middel van een bevelschrift om wordt gevraagd;

[5] Aangenomen teksten, P8_TA(2017)0234.

J. overwegende dat de EU in juni 2018 een procedure voor geschillenbeslechting heeft ingesteld bij de Wereldhandelsorganisatie, die in december 2018 werd aangevuld, tegen Chinese praktijken waarbij Europese ondernemingen gedwongen worden gevoelige technologie en knowhow prijs te geven als voorwaarde voor investeringen in China;

1. spreekt zijn diepe bezorgdheid uit over de recente beschuldigingen dat door Chinese bedrijven ontwikkelde 5G-apparatuur geïntegreerde achterdeurtjes bevat die de fabrikanten en de Chinese autoriteiten in staat stellen onrechtmatige toegang te verkrijgen tot particuliere gegevens en particuliere telecommunicatie van EU-burgers en -bedrijven; is van mening dat deze beschuldigingen grondig moeten worden gecontroleerd en onderzocht;

2. is van mening dat de mogelijke aanwezigheid van grote kwetsbaarheden in de 5G-apparatuur die door deze fabrikanten wordt gecreëerd, ook moet worden gecontroleerd en onderzocht bij de uitrol van 5G-netwerken in de komende jaren;

3. herhaalt dat elke entiteit die in de EU gevestigd is of die producten op de interne markt brengt, ongeacht haar nationaliteit, moet voldoen aan het rechten van de EU en de lidstaten en aan de verplichtingen op het gebied van de grondrechten, met inbegrip van de verplichtingen op het gebied van persoonlijke levenssfeer, gegevensbescherming en cyberveiligheid;

4. herhaalt dat elke entiteit die producten, diensten en processen in de EU aanbiedt, ongeacht haar nationaliteit, moet voldoen aan de criteria inzake beveiliging door ontwerp, die niet alleen geïntegreerde ingebedde achterdeurtjes zullen ontmoedigen, maar ook zullen helpen om andere mogelijkheden voor cyberinterferentie met het netwerk, bijvoorbeeld DDoS-aanvallen (Distributed Denial-of-Service), tegen te gaan;

5. verzoekt de Commissie dringend te zorgen voor één respons op deze nieuwe cyberdreigingen en -kwetsbaarheden als gevolg van de telecommunicatienetwerken van de volgende generatie; verzoekt de lidstaten de Commissie in kennis te stellen van de nationale maatregelen die zij voornemens zijn te nemen met het oog op een gecoördineerde respons van de Unie, teneinde de strengste normen inzake cyberbeveiliging te waarborgen in de hele Unie; herhaalt dat het belangrijk is geen onevenredige eenzijdige maatregelen in te voeren die de interne markt onnodig zouden versnipperen;

6. is van mening dat de EU een onafhankelijke respons moet bieden op basis van een risicobeoordeling en degelijk bewijs;

7. verzoekt de lidstaten, cyberbeveiligingsinstanties, telecomexploitanten, fabrikanten en aanbieders van kritieke infrastructuurdiensten bij de Commissie en het Enisa melding te maken van alle bewijs van achterdeurtjes of andere grote kwetsbaarheden die de integriteit en veiligheid van telecomnetwerken in gevaar kunnen brengen of inbreuk kunnen maken op het recht van de Unie en de grondrechten;

8. herinnert eraan dat telecommunicatienetwerken met elkaar verbonden zijn en dat elke kwetsbaarheid in het systeem andere delen van het netwerk kan aantasten en in gevaar kan brengen; verzoekt de Commissie de deugdelijkheid van het rechtskader van de Unie te beoordelen om tegemoet te komen aan de bezorgdheid over de aanwezigheid van

kwetsbare apparatuur in strategische sectoren en in de basisinfrastructuur; dringt er bij de Commissie op aan te zijner tijd initiatieven te presenteren, met inbegrip van wetgevingsvoorstellen, om mogelijke tekortkomingen aan te pakken;

9. herinnert eraan dat het huidige rechtskader voor telecommunicatie de lidstaten opdraagt om te garanderen dat telecomexploitanten de verplichting naleven om te zorgen voor de integriteit en beschikbaarheid van de openbare elektronische-communicatienetwerken; wijst erop dat de lidstaten volgens het Europees wetboek voor elektronische communicatie alle nodige bevoegdheden hebben om een breed scala aan rechtsmiddelen te onderzoeken en toe te passen in geval van niet-naleving, teneinde te garanderen dat de producten op de EU-markt gekenmerkt worden door privacy door ontwerp;

10. verzoekt de lidstaten en de Commissie erop toe te zien dat de 5G-apparatuur die in gebruik zal worden genomen, beveiligd is door ontwerp en gedurende de hele levensduur ervan veilig blijft werken; verzoekt de Commissie o, in samenwerking met het Enisa richtsnoeren te verstrekken over de manier om cyberdreigingen en -kwetsbaarheden aan te pakken bij de aanschaf van 5G-apparatuur en andere diensten met grote hoeveelheden privégegevens (d.w.z. diversificatie van de uitrusting wat verkopers betreft, voorwaarden voor het veilen van spectrum enz.); is van mening dat deze benadering niet beperkt mag blijven tot fabrikanten en verkopers van 5G-netwerkapparatuur, maar zich ook moet uitstrekken tot de bestaande netwerken en de volledige toeleveringsketen; verzoekt het Europees kenniscentrum voor cyberbeveiliging bij zijn werkzaamheden en bij de vaststelling van zijn strategische oriëntatie rekening te houden met bovengenoemde richtsnoeren;

11. verzoekt de lidstaten die Richtlijn (EU) 2016/1148 betreffende de beveiliging van netwerk- en informatiesystemen niet hebben omgezet, dringend nationale wetgeving goed te keuren om de richtlijn na te leven; verzoekt de Commissie na te gaan of het nodig is het toepassingsgebied van de richtlijn verder uit te breiden naar nieuwe sectoren en diensten waar grote hoeveelheden privégegevens worden blootgesteld en niet onder specifieke wetgeving (bv. telecommunicatie en elektronische identificatie) vallen;

12. is ingenomen met de vaststelling van de cyberbeveiligingsverordening, die de rol van het Enisa met betrekking tot het doeltreffend reageren op cyberaanvallen zal versterken, de samenwerking en coördinatie op het niveau van de Unie zal versterken en nieuwe certificeringsregelingen voor geconnecteerde producten en processen zal invoeren;

13. dringt er bij de Commissie op aan het Enisa op te dragen prioriteit te verlenen aan de opstelling van een certificeringsregeling voor 5G-apparatuur, om ervoor te zorgen dat de uitrol van 5G in de Unie aan de strengste veiligheidsnormen voldoet en bestand is tegen achterdeurtjes of andere grote kwetsbaarheden die de veiligheid van de telecommunicatienetwerken en de hiervan afhankelijke diensten van de Unie in gevaar zouden brengen; verzoekt de Commissie certificeringsprogramma's voor systemen van kunstmatige intelligentie op te nemen waarmee malware en beveiligingslekken in 5G-apparatuur kunnen worden opgespoord, beperkt en onmiddellijk kunnen worden gemeld;

14. herinnert er evenwel aan dat certificering de bevoegde autoriteiten en de exploitanten niet mag beletten de toeleveringsketen te controleren om de integriteit en veiligheid van

hun apparatuur die in kritieke omgevingen en telecommunicatienetwerken functioneert, te waarborgen;

15. merkt op dat Chinese ondernemingen, met inbegrip van overheidsbedrijven, ondanks het gebrek aan wederkerigheid, toegang hebben tot wijd opengestelde markten in de EU, en dat China sinds 2016 een nettoinvesteerder in de EU is; spreekt zijn bezorgdheid uit over de talrijke beperkingen waarmee Europese ondernemingen in China te kampen hebben, zoals de steeds strengere voorwaarden voor het verkrijgen van markttoegang, waaronder gedwongen technologieoverdracht, verplichte joint-ventures, discriminerende technische vereisten, waaronder gedwongen gegevenslokalisering, en openbaarmaking van de broncode;

16. spreekt zijn bezorgdheid uit over het feit dat de door de staat georganiseerde aankopen en investeringen uit China de Europese strategische belangen en de doelstellingen op het gebied van openbare veiligheid, het concurrentievermogen van de Europese ondernemingen en de hoogwaardige werkgelegenheid in de Unie in het gedrang kunnen brengen;

17. wijst nogmaals op de dringende noodzaak voor de EU om over de industriële capaciteit te beschikken in belangrijke strategische sectoren (bijvoorbeeld 5G-netwerkapparatuur en soortgelijke essentiële technologieën), om de afhankelijkheid van fabrikanten uit derde landen te verminderen die opereren op grond van nationale wetten die fundamenteel strijdig zijn met het recht van de Unie op het gebied van persoonlijke levenssfeer en industriële eigendom; is ingenomen met de goedkeuring van de nieuwe verordening tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Europese Unie[6], om de mogelijke veiligheidsrisico's te beoordelen, met inbegrip van cyberdreigingen, die gevolgen kunnen hebben voor de veiligheid of de openbare orde, en die kunnen worden veroorzaakt door buitenlandse investeringen op het niveau van de lidstaten of de Unie;

18. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Raad, de Europese Dienst voor Extern Optreden, de Commissie, de regeringen en parlementen van de lidstaten en de toetredende landen en kandidaat-lidstaten, de regering van de Volksrepubliek China en het Chinese Nationale Volkscongres.

[6] Aangenomen teksten, P8_TC1-COD(2017)0224.