Europees Parlement
2014-2019

Zittingsdocument

B8-0154/2019 }
B8-0155/2019 }
B8-0159/2019 }
B8-0160/2019 } RC1

8.3.2019

GEZAMENLIJKE ONTWERPRESOLUTIE

ingediend overeenkomstig artikel 123, leden 2 en 4, van het Reglement

ter vervanging van de volgende ontwerpresoluties:
B8-0154/2019 (ALDE)
B8-0155/2019 (PPE)
B8-0159/2019 (S&D)
B8-0160/2019 (Verts/ALE)

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))

Luděk Niedermayer
namens de PPE-Fractie
Dan Nica
namens de S&D-Fractie
Caroline Nagtegaal
namens de ALDE-Fractie
Reinhard Bütikofer
namens de Verts/ALE-Fractie

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 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 Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad[3],

– 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 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening") (COM(2017)0477),

– gezien het voorstel van de Commissie van 12 september 2018 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 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,

– gezien de goedkeuring door de Australische regering van de hervormingen op het gebied van de beveiliging van de telecommunicatiesector, die op 18 september 2018 in werking zijn getreden,

– gezien 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

---

[1] PB L 321 van 17.12.2018, blz. 36.
[2] PB L 194 van 19.7.2016, blz. 1.
[3] PB L 218 van 14.8.2013, blz. 8.

kader voor de screening van buitenlandse directe investeringen in de Europese Unie[4],

– gezien zijn eerdere resoluties over de stand van zaken van de betrekkingen tussen de EU en China, in het bijzonder die van 12 september 2018[5],

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

– gezien zijn resolutie van 1 juni 2017 over internetconnectiviteit voor groei, concurrentievermogen en cohesie: Europese gigabitmaatschappij en 5G[6],

– 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)[7],

– gezien Verordening (EU) nr. 1316/2013 van het Europees Parlement en de Raad van 11 december 2013 tot vaststelling van de financieringsfaciliteit voor Europese verbindingen, tot wijziging van Verordening (EU) nr. 913/2010 en tot intrekking van Verordeningen (EG) nr. 680/2007 en (EG) nr. 67/2010[8],

– gezien het voorstel van de Commissie van 6 juni 2018 voor een verordening van het Europees Parlement en de Raad tot vaststelling van het programma Digitaal Europa voor de periode 2021-2027 (COM(2018)0434),

– gezien artikel 123, leden 2 en 4, van zijn Reglement,

A. overwegende dat de EU vaart moet zetten achter haar agenda voor cyberbeveiliging om het potentieel ervan te benutten om uit te groeien tot een leidende speler op het gebied van cyberbeveiliging en hiervan gebruik te maken ten voordele van het Europese bedrijfsleven;

B. overwegende dat kwetsbaarheden in 5G-netwerken uitgebuit zouden kunnen worden om IT-systemen aan te vallen, mogelijkerwijs resulterend in zeer ernstige schade aan economieën op Europees en nationaal niveau; overwegende dat een op risicoanalyse gebaseerde benadering in de gehele waardeketen noodzakelijk is om de risico's tot een minimum te beperken;

C. overwegende dat het 5G-netwerk de ruggengraat van onze digitale infrastructuur zal vormen, waarmee de mogelijkheid wordt uitgebreid om diverse apparaten aan te sluiten op netwerken (het internet der dingen enz.), en nieuwe voordelen en kansen zal opleveren voor de samenleving en het bedrijfsleven op diverse terreinen, met inbegrip van kritieke sectoren van de economie, zoals vervoer, energie, gezondheid, financiën,

---

[4] Aangenomen teksten, P8_TA(2019)0121.
[5] Aangenomen teksten, P8_TA(2018)0343.
[6] PB C 307 van 30.8.2018, blz. 144.
[7] PB L 119 van 4.5.2016, blz. 1.
[8] PB L 348 van 20.12.2013, blz. 129.

telecommunicatie, defensie, ruimtevaart en veiligheid;

D. overwegende dat de totstandbrenging van een adequaat mechanisme om op veiligheidsuitdagingen te reageren de EU de kans zou bieden actief stappen te ondernemen om normen voor 5G vast te stellen;

E. overwegende dat er bezorgdheid is geuit over verkopers van apparatuur uit derde landen die een veiligheidsrisico voor de EU kunnen vormen als gevolg van de wetgeving van hun land van herkomst, met name na de inwerkingtreding van de Chinese wetten op de staatsveiligheid, die alle burgers, ondernemingen en andere entiteiten de verplichting opleggen met de staat samen te werken om de staatsveiligheid te waarborgen, in het kader van een zeer ruime definitie van nationale veiligheid; overwegende dat er geen garanties zijn dat deze verplichting niet extraterritoriaal wordt toegepast, en dat in diverse landen uiteenlopend op de Chinese wetten is gereageerd, gaande van veiligheidsbeoordelingen tot absolute verboden;

F. overwegende dat de Tsjechische nationale cyberbeveiligingsinstantie in december 2018 heeft gewaarschuwd voor veiligheidsrisico's die verbonden zijn aan de door de Chinese bedrijven Huawei en ZTE geleverde technologie; overwegende dat de Tsjechische belastingautoriteiten Huawei in januari 2019 vervolgens hebben uitgesloten van een aanbesteding om een belastingportaalsite te bouwen;

G. overwegende dat een grondig onderzoek nodig is om na te gaan of de betrokken apparaten, of andere apparatuur of leveranciers, veiligheidsrisico's inhouden vanwege functies als achterdeurtjes naar systemen;

H. overwegende dat oplossingen op EU-niveau moeten worden gecoördineerd en behandeld om te voorkomen dat er verschillende niveaus van beveiliging en potentiële lacunes op het gebied van cyberbeveiliging ontstaan, en dat er op mondiaal niveau coördinatie nodig is om een krachtig antwoord te bieden;

I. overwegende dat de voordelen van de eengemaakte markt gepaard gaan met de verplichting om te voldoen aan de EU-normen en het rechtskader van de Unie, en dat leveranciers niet verschillend mogen worden behandeld op basis van hun land van herkomst;

J. overwegende dat de verordening tot vaststelling van een kader voor de screening van buitenlandse directe investeringen, die tegen eind 2020 in werking moet treden, de lidstaten meer mogelijkheden geeft om buitenlandse investeringen te screenen op basis van overwegingen in verband met de veiligheid en de openbare orde, en een samenwerkingsmechanisme behelst dat de Commissie en de lidstaten in staat stelt samen te werken bij het beoordelen van veiligheidsrisico's, onder meer op het gebied van cyberbeveiliging, als gevolg van gevoelige buitenlandse investeringen, en ook betrekking heeft op projecten en programma's die van belang zijn voor de EU, zoals de trans-Europese telecommunicatienetwerken en Horizon 2020;

1. is van mening dat de Unie het voortouw moet nemen op het gebied van cyberbeveiliging, door middel van een gezamenlijke benadering op basis van het doeltreffende en efficiënte gebruik van de expertise van de EU, de lidstaten en het bedrijfsleven, aangezien een lappendeken van uiteenlopende nationale beslissingen

nadelig zou zijn voor de digitale eengemaakte markt;

2. spreekt zijn diepe bezorgdheid uit over de recente beschuldigingen dat door Chinese bedrijven ontwikkelde 5G-apparatuur mogelijk geïntegreerde achterdeurtjes bevat die fabrikanten en autoriteiten in staat zouden stellen onrechtmatige toegang te verkrijgen tot particuliere en persoonlijke gegevens en telecommunicatie van EU-burgers en -bedrijven;

3. is tevens bezorgd over de mogelijke aanwezigheid van grote kwetsbaarheden in de 5G-apparatuur die door deze fabrikanten wordt ontwikkeld indien deze wordt geïnstalleerd bij de uitrol van 5G-netwerken in de komende jaren;

4. onderstreept dat de gevolgen voor de veiligheid van netwerken en apparatuur over de hele wereld dezelfde zijn, en verzoekt de EU lessen te trekken uit de opgedane ervaring om de strengste normen op het gebied van cyberbeveiliging te kunnen waarborgen; verzoekt de Commissie een strategie te ontwikkelen waarmee Europa een koploper wordt op het gebied van cyberbeveiligingstechnologie en die tot doel heeft Europa minder afhankelijk te maken van buitenlandse technologie op het gebied van cyberbeveiliging; is van mening dat er, wanneer de naleving van de beveiligingsvoorschriften niet kan worden gewaarborgd, passende maatregelen moeten worden genomen;

5. verzoekt de lidstaten de Commissie in kennis te stellen van nationale maatregelen die zij voornemens zijn te nemen met het oog op een gecoördineerde respons van de Unie, teneinde in de hele Unie de strengste normen op het gebied van cyberbeveiliging te waarborgen, en onderstreept nogmaals hoe belangrijk het is geen onevenredige eenzijdige maatregelen te treffen die de eengemaakte markt zouden versnipperen;

6. herhaalt dat alle entiteiten die in de EU apparatuur leveren of diensten verlenen, ongeacht hun land van herkomst, moeten voldoen aan de verplichtingen op het gebied van de grondrechten en aan het recht van de EU en de lidstaten, met inbegrip van het rechtskader met betrekking tot de persoonlijke levenssfeer, gegevensbescherming en cyberbeveiliging;

7. 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 met initiatieven en zo nodig wetgevingsvoorstellen te komen om tijdig eventueel vastgestelde tekortkomingen te ondervangen, aangezien de Unie voortdurend bezig is uitdagingen op het gebied van cyberbeveiliging in kaart te brengen en aan te pakken en de weerbaarheid op het gebied van cyberbeveiliging in de EU te verbeteren;

8. verzoekt de lidstaten die de NIS-richtlijn nog niet volledig hebben omgezet, dat onverwijld te doen en verzoekt de Commissie deze omzetting nauwlettend te volgen om te waarborgen dat de bepalingen van de richtlijn naar behoren worden toegepast en gehandhaafd en dat de Europese burgers beter beschermd zijn tegen externe en interne veiligheidsdreigingen;

9. dringt er bij de Commissie en de lidstaten op aan ervoor te zorgen dat de bij de NIS-

richtlijn ingevoerde verslagleggingsmechanismen naar behoren worden toegepast; merkt op dat de Commissie en de lidstaten grondig moeten toezien op beveiligingsincidenten of inadequate reacties van leveranciers, teneinde vastgestelde lacunes te verhelpen;

10. verzoekt de Commissie na te gaan of het nodig is het toepassingsgebied van de NIS-richtlijn verder uit te breiden naar andere kritieke sectoren en diensten die niet onder sectorspecifieke wetgeving vallen;

11. verwelkomt en steunt het akkoord over de cyberbeveiligingsverordening en de versterking van het mandaat van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), voor het beter ondersteunen van de lidstaten bij het aanpakken van cyberdreigingen en -aanvallen;

12. 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 beveiligingsnormen voldoet en vrij is van achterdeurtjes of grote kwetsbaarheden die de veiligheid van de telecommunicatienetwerken en de hiervan afhankelijke diensten van de Unie in gevaar zouden brengen; beveelt aan om bijzondere aandacht te besteden aan veelgebruikte processen, producten en software die door hun omvang een aanzienlijke invloed hebben op het dagelijks leven van burgers en de economie;

13. is zeer verheugd over de voorstellen voor kenniscentra voor cyberbeveiliging en een netwerk van nationale coördinatiecentra, die bedoeld zijn om de EU te helpen bij het behouden en ontwikkelen van de technologische en industriële capaciteiten op het gebied van cyberbeveiliging die nodig zijn om haar digitale eengemaakte markt te beschermen; 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;

14. herinnert eraan dat cyberbeveiliging strenge beveiligingsnormen vergt; dringt aan op een netwerk dat zowel door standaardinstellingen als door ontwerp veilig is; verzoekt de lidstaten met klem om samen met de Commissie te bekijken hoe een hoog niveau van beveiliging tot stand kan worden gebracht;

15. dringt er bij de Commissie en de lidstaten op aan om, in samenwerking met het Enisa, richtsnoeren te verstrekken voor de aanpak van cyberdreigingen en -kwetsbaarheden bij de aanschaf van 5G-apparatuur, bijvoorbeeld door de diversificatie van apparatuur wat verkopers betreft of de invoering van meerfasige aanbestedingsprocedures;

16. herhaalt zijn standpunt in verband met het programma Digitaal Europa, dat in de EU gevestigde maar vanuit derde landen gecontroleerde entiteiten aan beveiligingsvereisten en toezicht door de Commissie onderwerpt, in het bijzonder ten aanzien van aan cyberbeveiliging gerelateerde acties;

17. verzoekt de lidstaten ervoor te zorgen dat overheidsinstellingen en particuliere bedrijven die ertoe bijdragen dat kritieke infrastructuurnetwerken zoals telecommunicatie-, energie-, gezondheids- en sociale systemen goed werken, daaromtrent

risicobeoordelingen uitvoeren waarbij rekening wordt gehouden met de veiligheidsdreigingen die specifiek verbonden zijn aan de technische kenmerken van het betrokken systeem of de afhankelijkheid van externe leveranciers van hardware- en softwaretechnologieën;

18. herinnert eraan dat het huidige rechtskader voor telecommunicatie de lidstaten opdraagt te garanderen dat telecomexploitanten de verplichting naleven om te zorgen voor de integriteit en beschikbaarheid van de openbare elektronische-communicatienetwerken, met inbegrip van, in voorkomend geval, eind-tot-eindversleuteling; benadrukt dat de lidstaten krachtens het Europees wetboek voor elektronische communicatie over uitgebreide bevoegdheden beschikken om producten op de EU-markt te onderzoeken en een breed scala aan rechtsmiddelen toe te passen in geval van niet-conformiteit ervan;

19. roept de Commissie en de lidstaten op beveiliging tot een verplicht aspect te maken van alle openbare aanbestedingsprocedures voor relevante infrastructuur op zowel EU- als nationaal niveau;

20. herinnert de lidstaten eraan dat zij krachtens het rechtskader van de EU, met name Richtlijn 2013/40/EU over aanvallen op informatiesystemen, verplicht zijn sancties op te leggen aan rechtspersonen die strafbare feiten hebben gepleegd, zoals aanvallen op dergelijke systemen; benadrukt dat de lidstaten ook gebruik moeten maken van hun vermogen om deze rechtspersonen andere sancties op te leggen, zoals een tijdelijk of permanent verbod op het uitoefenen van commerciële activiteiten;

21. 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; verwacht van de nationale gegevensbeschermingsautoriteiten en de Europese Toezichthouder voor gegevensbescherming dat zij grondig onderzoek doen naar aanwijzingen van inbreuken in verband met persoonsgegevens door externe verkopers en dat zij passende boetes en sancties opleggen in overeenstemming met het Europese gegevensbeschermingsrecht;

22. is ingenomen met de aanstaande inwerkingtreding van een verordening tot vaststelling van een kader voor de screening van buitenlandse directe investeringen om redenen van veiligheid en openbare orde, en onderstreept dat in deze verordening voor het eerst een lijst wordt vastgesteld van gebieden en factoren, met inbegrip van communicatie en cyberbeveiliging, die van belang zijn voor de veiligheid en de openbare orde op EU-niveau;

23. verzoekt de Raad zijn werkzaamheden met betrekking tot de voorgestelde e-privacyverordening te bespoedigen;

24. herhaalt dat de EU cyberbeveiliging moet ondersteunen in de gehele waardeketen, van onderzoek tot de uitrol en invoering van belangrijke technologieën, dat zij relevante informatie moet verspreiden en dat zij cyberhygiëne en onderwijsprogramma's met inbegrip van cyberbeveiliging moet bevorderen, en is van mening dat onder meer het programma Digitaal Europa daarvoor een doeltreffend instrument zal zijn;

25. dringt er bij de Commissie en de lidstaten op aan de nodige stappen te ondernemen, met inbegrip van robuuste investeringsprojecten, om binnen de EU een innovatievriendelijk klimaat te scheppen dat toegankelijk is voor alle ondernemingen in de digitale economie van de EU, met inbegrip van kleine en middelgrote ondernemingen (kmo's); dringt er voorts op aan dat een dergelijk klimaat Europese verkopers in staat stelt nieuwe producten, diensten en technologieën te ontwikkelen waarmee zij de concurrentie aankunnen;

26. dringt er bij de Commissie en de lidstaten op aan rekening te houden met bovenstaande verzoeken in het kader van de komende besprekingen over de toekomstige EU-China-strategie, wat noodzakelijk is om de EU concurrerend te houden en de veiligheid van haar digitale infrastructuur te waarborgen;

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