Donderdag, 10 juni 2021

P9_TA(2021)0286

De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

Resolutie van het Europees Parlement van 10 juni 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk (2021/2568(RSP))

(2022/C 67/08)

Het Europees Parlement,

— gezien de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid van 16 december 2020 getiteld "De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk" (JOIN(2020)0018),

— gezien het voorstel van de Commissie van 16 december 2020 voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 (COM(2020)0823),

— gezien het voorstel van de Commissie van 24 september 2020 voor een richtlijn van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (COM(2020)0595),

— gezien het voorstel van de Commissie 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 mededeling van de Commissie van 19 februari 2020, getiteld "De digitale toekomst van Europa vormgeven" (COM(2020)0067),

— gezien Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) ([1]),

— gezien Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG ([2]),

— 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 ([3]),

— gezien Verordening (EU) nr. 1290/2013 van het Europees Parlement en de Raad van 11 december 2013 tot vaststelling van de regels voor de deelname aan acties en de verspreiding van resultaten in het kader van "Horizon 2020 — het kaderprogramma voor onderzoek en innovatie (2014-2020)" en tot intrekking van Verordening (EG) nr. 1906/2006 ([4]),

— gezien Verordening (EU) nr. 1291/2013 van het Europees Parlement en de Raad van 11 december 2013 tot vaststelling van Horizon 2020 — het kaderprogramma voor onderzoek en innovatie (2014-2020) en tot intrekking van Besluit nr. 1982/2006/EG ([5]),

— gezien Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot vaststelling van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 ([6]),

([1]) PB L 151 van 7.6.2019, blz. 15.
([2]) PB L 153 van 22.5.2014, blz. 62.
([3]) PB L 321 van 17.12.2018, blz. 36.
([4]) PB L 347 van 20.12.2013, blz. 81.
([5]) PB L 347 van 20.12.2013, blz. 104.
([6]) PB L 166 van 11.5.2021, blz. 1.

Donderdag, 10 juni 2021

— gezien Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen ([7]),

— gezien het Verdrag van Boedapest inzake cybercriminaliteit van 23 november 2001 (ETS nr. 185),

— gezien zijn resolutie van 16 december 2020 over een nieuwe strategie voor Europese kmo's ([8]),

— gezien zijn resolutie van 25 maart 2021 over een Europese datastrategie ([9]),

— gezien zijn resolutie van 20 mei 2021 over de digitale toekomst van Europa vormgeven: belemmeringen voor de werking van de digitale eengemaakte markt wegnemen en het gebruik van AI voor Europese consumenten verbeteren ([10]),

— gezien zijn resolutie van 21 januari 2021 over de digitale kloof tussen vrouwen en mannen dichten: de deelname van vrouwen aan de digitale economie ([11]),

— gezien zijn resolutie van 12 maart 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 ([12]),

— gezien de vraag aan de Commissie over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk (O-000037/2021 — B9-0024/2021),

— gezien artikel 136, lid 5, en artikel 132, lid 2, van zijn Reglement,

A. overwegende dat de digitale transformatie een belangrijke strategische prioriteit van de Unie is, die onvermijdelijk gepaard gaat met een grotere blootstelling aan cyberdreigingen;

B. overwegende dat aangesloten apparaten, waaronder machines, sensoren, industriële componenten en netwerken die deel uitmaken van het internet der dingen (Internet of Things, IoT), in aantal blijven toenemen, met naar verwachting wereldwijd 22,3 miljard met het IoT verbonden apparaten in 2024, waardoor de blootstelling aan cyberaanvallen toeneemt;

C. overwegende dat technologische vooruitgang — zoals kwantumcomputers — en asymmetrieën bij de toegang daartoe een uitdaging kunnen vormen voor het cyberbeveiligingslandschap;

D. overwegende dat het aantal cyberaanvallen aanzienlijk toeneemt, zoals onder meer blijkt uit de recente reeks kwaadwillige en georganiseerde cyberaanvallen op gezondheidszorgstelsel in Ierland, Finland en Frankrijk; overwegende dat deze cyberaanvallen aanzienlijke schade toebrengen aan gezondheidszorgstelsels en patiëntenzorg, alsook aan andere gevoelige openbare en particuliere instellingen;

E. overwegende dat de COVID-19-crisis cyberkwetsbaarheden in sommige cruciale sectoren, met name in de gezondheidszorg, verder aan het licht heeft gebracht, en dat de bijbehorende maatregelen van telewerken en sociale afstand onze afhankelijkheid van digitale technologieën en connectiviteit hebben vergroot, terwijl cyberaanvallen en cybercriminaliteit, waaronder spionage en sabotage, alsmede het binnendringen in en manipuleren van ICT-systemen, -structuren en -netwerken via kwaadwillige en onwettige installaties, in heel Europa in aantal en geraffineerdheid toenemen;

F. overwegende dat hybride dreigingen, waaronder het gebruik van desinformatiecampagnes en cyberaanvallen op infrastructuur, economische processen en democratische instellingen, toenemen en een serieus probleem aan het worden zijn in zowel de cyber- als de fysieke wereld, en een risico vormen voor democratische processen zoals verkiezingen, wetgevingsprocedures, rechtshandhaving en justitie;

G. overwegende dat er in toenemende mate een beroep wordt gedaan op de kernfunctie van internet en op essentiële internetdiensten voor communicatie en hosting, toepassingen en gegevens, waarvan het marktaandeel geleidelijk wordt geconcentreerd bij steeds minder bedrijven;

([7]) PB L 207 van 6.8.2010, blz. 1.
([8]) Aangenomen teksten, P9_TA(2020)0359.
([9]) Aangenomen teksten, P9_TA(2021)0098.
([10]) Aangenomen teksten, P9_TA(2021)0261.
([11]) Aangenomen teksten, P9_TA(2021)0026.
([12]) PB C 23 van 21.1.2021, blz. 2.

H. overwegende dat de mogelijkheden voor Distributed Denial-of-Service-aanvallen toenemen en dat daarom de veerkracht van de kern van het internet overeenkomstig moet worden vergroot;

I. overwegende dat de paraatheid en het bewustzijn op het gebied van cyberbeveiliging bij bedrijven laag blijven, met name bij kmo's en eenmanszaken, en dat er een tekort aan geschoolde werknemers is (de personeelskloof is sinds 2015 met 20 % toegenomen), waarbij traditionele wervingskanalen niet aan de vraag kunnen voldoen, ook niet voor leidinggevende en interdisciplinaire functies; overwegende dat bijna 90 % van het personeel dat zich wereldwijd bezighoudt met cyberbeveiliging van het mannelijk geslacht is en dat "dit hardnekkige gebrek aan genderdiversiteit het aanwezige talent verder beperkt" ([13]);

J. overwegende dat de slagkracht op het gebied van cyberbeveiliging in de lidstaten heterogeen is en dat het melden van incidenten en het delen van informatie tussen hen systematisch noch alomvattend is, terwijl de mogelijkheden voor het inzetten van centra voor informatie-uitwisseling en -analyse (Information Sharing and Analysis Centres, ISAC's) voor de uitwisseling van informatie tussen de publieke en de particuliere sector onvoldoende worden benut;

K. overwegende dat er op EU-niveau geen overeenstemming bestaat over samenwerking op het gebied van cyberinlichtingen en over de collectieve reactie op cyber- en hybride aanvallen; overwegende dat tegenmaatregelen tegen cyberdreigingen en cyberaanvallen, met name die van hybride aard, voor de lidstaten technisch en geopolitiek zeer moeilijk zijn om individueel aan te pakken;

L. overwegende dat grensoverschrijdende en wereldwijde gegevensuitwisseling belangrijk zijn voor waardecreatie, op voorwaarde dat privacy en intellectuele en eigendomsrechten worden gewaarborgd; overwegende dat de handhaving van buitenlandse gegevenswetgeving een cyberbeveiligingsrisico kan vormen voor Europese gegevens, aangezien bedrijven die in verschillende regio's actief zijn, onderworpen zijn aan overlappende verplichtingen, ongeacht de locatie van de gegevens of hun herkomst;

M. overwegende dat cyberbeveiliging een wereldmarkt van 600 miljard EUR vertegenwoordigt en dat dit bedrag naar verwachting snel zal toenemen, en dat de Unie een netto-importeur van producten en oplossingen is;

N. overwegende dat er een risico bestaat op versnippering van de eengemaakte markt als gevolg van nationale regelgeving inzake cyberbeveiliging en het ontbreken van horizontale wetgeving met betrekking tot essentiële cyberbeveiligingsvereisten voor hardware en software, met inbegrip van verbonden producten en applicaties;

1. is ingenomen met de initiatieven die door de Commissie zijn uiteengezet in de gezamenlijke mededeling getiteld "De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk";

2. dringt erop aan de ontwikkeling van veilige en betrouwbare netwerk- en informatiesystemen, infrastructuur en connectiviteit in de hele Unie te bevorderen;

3. dringt erop aan als doel te stellen dat alle met internet verbonden producten in de Unie, met inbegrip van die voor consumenten- en industrieel gebruik, samen met alle toeleveringsketens die deze producten beschikbaar stellen, een veilig ontwerp moeten hebben en bestand moeten zijn tegen cyberincidenten en snel moeten kunnen worden bijgewerkt wanneer er kwetsbaarheden worden ontdekt; is ingenomen met de plannen van de Commissie om horizontale wetgeving inzake cyberbeveiligingsvereisten voor verbonden producten en bijbehorende diensten voor te stellen, en verzoekt dat die wetgeving voorstellen bevat voor de harmonisatie van nationale wetgeving om versnippering van de eengemaakte markt te voorkomen; verzoekt om rekening te houden met bestaande wetgeving (de cyberbeveiligingswet, het nieuwe wetgevingskader, de verordening betreffende normalisatie) om dubbelzinnigheid en versnippering te voorkomen;

4. verzoekt de Commissie te beoordelen of er behoefte is aan een voorstel voor een horizontale verordening tot invoering van cyberbeveiligingseisen voor applicaties, software, ingebedde software en besturingssystemen in 2023, voortbouwend op het EU-acquis voor vereisten op het gebied van risicobeheer; benadrukt dat verouderde applicaties, software, ingebedde software en besturingssystemen (d.w.z. die niet langer regelmatig patches en beveiligingsupdates ontvangen) een niet te verwaarlozen aandeel van alle aangesloten apparaten uitmaken en een cyberbeveiligingsrisico vormen; dringt er bij de Commissie op aan dat zij dit aspect opneemt in haar voorstel; stelt voor dat het voorstel de verplichting voor producenten bevat om van tevoren de minimumperiode mee te delen waarin zij beveiligingspatches en updates ondersteunen, zodat kopers weloverwogen keuzes kunnen maken; is van mening dat producenten deel moeten uitmaken van het gecoördineerde programma voor de bekendmaking van kwetsbaarheden zoals beschreven in het voorstel voor de NIS 2-richtlijn;

([13]) Europese Rekenkamer *Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging*, briefingdocument, maart 2019.

Donderdag, 10 juni 2021

5. benadrukt dat cyberbeveiliging moet worden ingebed in digitalisering; dringt er daarom op aan dat door de Unie gefinancierde digitaliseringsprojecten cyberbeveiligingseisen omvatten; is ingenomen met de steun voor onderzoek en innovatie op het gebied van cyberbeveiliging, met name wat betreft disruptieve technologieën (zoals kwantumcomputing en kwantumcryptografie), waarvan de opkomst het internationale evenwicht zou kunnen verstoren; dringt bovendien aan op verder onderzoek naar post-kwantumalgoritmen als cyberbeveiligingsnorm;

6. is van mening dat de digitalisering van onze samenleving betekent dat alle sectoren met elkaar verbonden zijn en dat de tekortkomingen in de ene sector een belemmering kunnen vormen voor andere; dringt er daarom op aan dat cyberbeveiligingsbeleid wordt opgenomen in de digitale strategie van de EU en in EU-financiering, en dat dit coherent moet zijn en interoperabel in alle sectoren;

7. roept op tot een coherent gebruik van EU-middelen voor de uitrol van cyberbeveiliging en aanverwante infrastructuur; verzoekt de Commissie en de lidstaten ervoor te zorgen dat synergieën op het gebied van cyberbeveiliging tussen verschillende programma's worden benut, met name het programma Horizon Europa, het programma Digitaal Europa, het EU-ruimtevaartprogramma, de herstel- en veerkrachtfaciliteit van de EU, InvestEU en de Connecting Europe Facility (CEF), en om ten volle gebruik te maken van het kenniscentrum en netwerk voor cyberbeveiliging;

8. herinnert eraan dat communicatie-infrastructuur de hoeksteen is van alle digitale activiteiten en dat het waarborgen van de veiligheid ervan een strategische prioriteit is voor de Unie; steunt de huidige ontwikkeling van de EU-regeling voor cyberbeveiligingscertificering voor 5G-netwerken; is ingenomen met de EU-toolbox voor 5G-cyberbeveiliging en verzoekt de Commissie, de lidstaten en het bedrijfsleven hun inspanningen voor veilige communicatienetwerken voort te zetten, met inbegrip van maatregelen met betrekking tot de gehele toeleveringsketen; verzoekt de Commissie de afhankelijkheid van één aanbieder te voorkomen en de netwerkbeveiliging te verbeteren door initiatieven te bevorderen die de virtualisering en cloudificering van de verschillende componenten van de netwerken verbeteren; dringt aan op de snelle ontwikkeling van de volgende generaties communicatietechnologieën met een cyberveilig ontwerp als grondbeginsel, die de bescherming van privacy en persoonsgegevens waarborgen;

9. wijst nogmaals op het belang van de totstandbrenging van een nieuw, robuust veiligheidskader voor cruciale EU-infrastructuren om de veiligheidsbelangen van de EU te beschermen en van het voortbouwen op bestaande slagkracht om adequaat te reageren op risico's, bedreigingen en technologische veranderingen;

10. verzoekt de Commissie bepalingen op te stellen om de toegankelijkheid, beschikbaarheid en integriteit van de openbare kern van het internet, en zodoende de stabiliteit van de cyberruimte, met name wat betreft de toegang van de EU tot het wereldwijde DNS-rootsysteem, te waarborgen; is van mening dat deze bepalingen maatregelen moeten omvatten voor de diversificatie van leveranciers om het huidige risico van afhankelijkheid van de paar bedrijven die de markt beheersen te verminderen; is ingenomen met het voorstel voor een Europees domeinnaamsysteem (DNS4EU) als instrument voor een veerkrachtiger internetkern; verzoekt de Commissie te evalueren hoe dit DNS4EU gebruik zou kunnen maken van de nieuwste technologieën, beveiligingsprotocollen en deskundigheid op het gebied van cyberbedreigingen om alle Europeanen een snel, veilig en veerkrachtig domeinnaamsysteem te bieden; herinnert aan de noodzaak van een betere bescherming van het Border Gateway Protocol (BGP) om BGP-kapingen te voorkomen; herinnert aan zijn steun voor een multi-stakeholdermodel voor internetgovernance, waarvan cyberbeveiliging een van de kernthema's moet zijn; benadrukt dat de EU de uitvoering van IPv6 moet versnellen; erkent het open source-model dat, als basis voor het functioneren van internet, efficiënt en effectief is gebleken; moedigt daarom het gebruik ervan aan;

11. erkent de noodzaak van meer forensisch onderzoek op het gebied van cyberbeveiliging om misdaad, cybercriminaliteit en cyberaanvallen te bestrijden, met inbegrip van door de staat gesteunde aanvallen, maar waarschuwt voor onevenredige maatregelen die de privacy en de vrijheid van meningsuiting van EU-burgers tijdens het gebruik van internet in gevaar brengen; herinnert eraan dat de herziening van het tweede aanvullende protocol bij het Verdrag van Boedapest inzake cybercriminaliteit moet worden afgerond, waardoor de paraatheid tegen cybercriminaliteit kan worden vergroot;

12. verzoekt de Commissie en de lidstaten hun middelen te bundelen om de strategische veerkracht van de EU te vergroten, haar afhankelijkheid van buitenlandse technologieën te verminderen en haar leiderschap en concurrentievermogen op het gebied van cyberbeveiliging in de hele digitale toeleveringsketen (waaronder gegevensopslag en -verwerking in de cloud, processortechnologieën, geïntegreerde schakelingen (chips), ultraveilige connectiviteit, kwantumcomputers en de volgende generatie netwerken) te versterken;

13. beschouwt het plan voor een ultraveilige connectiviteitsinfrastructuur als een belangrijk instrument voor de beveiliging van gevoelige digitale communicatie; is ingenomen met de aankondiging van de ontwikkeling van een wereldwijd veilig communicatiesysteem in de ruimte van de EU, waar kwantumversleutelingstechnologieën deel van uitmaken; herinnert eraan dat er, in samenwerking met het Agentschap van de Europese Unie voor het ruimtevaartprogramma (Euspa) en het Europees Ruimteagentschap (ETA), voortdurend inspanningen moeten worden geleverd om Europese ruimtevaartactiviteiten veilig te stellen;

14. betreurt dat de praktijken voor het delen van informatie rond cyberdreigingen en -incidenten niet goed zijn omarmd door de particuliere en de publieke sector; verzoekt de Commissie en de lidstaten het vertrouwen te vergroten en de belemmeringen voor het delen van informatie over cyberdreigingen en cyberaanvallen op alle niveaus te verminderen; is ingenomen met de inspanningen van sommige sectoren en dringt aan op sectoroverschrijdende samenwerking, aangezien kwetsbaarheden zelden sectorspecifiek zijn; benadrukt dat de lidstaten hun krachten op Europees niveau moeten bundelen teneinde hun meest recente kennis over cyberbeveiligingsrisico's efficiënt te delen; moedigt de oprichting aan van een werkgroep van de lidstaten inzake cyberinlichtingen teneinde de uitwisseling van informatie in de EU en de Europese economische ruimte te bevorderen, en met name om grootschalige cyberaanvallen te voorkomen;

15. is ingenomen met de geplande oprichting van een gezamenlijke cybereenheid om de samenwerking te versterken tussen de EU-organen en de autoriteiten van de lidstaten die verantwoordelijk zijn voor het voorkomen, afschrikken van en reageren op cyberaanvallen; verzoekt de lidstaten en de Commissie de samenwerking op het gebied van cyberdefensie verder te versterken en onderzoek naar geavanceerde cyberdefensieslagkracht te ontwikkelen;

16. herinnert aan het belang van de menselijke factor in de cyberbeveiligingsstrategie; dringt aan op voortdurende inspanningen om het bewustzijn op het gebied van cyberbeveiliging te verspreiden, met inbegrip van cyberhygiëne en cybergeletterdheid;

17. benadrukt het belang van een robuust en consistent veiligheidskader om alle EU-personeel, gegevens, communicatienetwerken en informatiesystemen en besluitvormingsprocessen te beschermen tegen cyberdreigingen op basis van alomvattende, consistente en homogene regels en adequate governance; dringt erop aan voldoende middelen en slagkracht beschikbaar te stellen, onder meer in het kader van de versterking van het mandaat van CERT-EU en met betrekking tot de lopende discussies over de vaststelling van gemeenschappelijke bindende regels inzake cyberbeveiliging voor alle EU-instellingen, -organen en agentschappen;

18. dringt aan op een ruimer gebruik van vrijwillige certificering en cyberbeveiligingsnormen, aangezien dit belangrijke instrumenten zijn om het algemene niveau van cyberbeveiliging te verbeteren; is ingenomen met het tot stand komen van het Europees certificeringskader en met het werk van de Europese groep voor cyberbeveiligingscertificering; verzoekt Enisa en de Commissie om bij de voorbereiding van de EU-regeling voor cyberbeveiligingscertificering voor clouddiensten te overwegen de toepassing van de EU-wetgeving verplicht te stellen met betrekking tot het "hoge" zekerheidsniveau;

19. benadrukt de noodzaak om aan de vraag naar arbeidskrachten op het gebied van cyberbeveiliging te voldoen door de vaardigheidskloof te dichten met behulp van voortgezette de inspanningen op het gebied van onderwijs en opleiding; dringt aan op bijzondere aandacht voor het wegwerken van de genderkloof, die ook in deze sector aanwezig is;

20. erkent de noodzaak van betere ondersteuning voor micro-, kleine en middelgrote ondernemingen om hun inzicht in alle informatiebeveiligingsrisico's en hun mogelijkheden om hun cyberbeveiliging te verbeteren, te vergroten; verzoekt Enisa en de nationale autoriteiten zelftestportalen en handleidingen voor beste praktijken te ontwikkelen voor micro-, kleine en middelgrote ondernemingen; herinnert aan het belang van opleiding en van toegang tot specifieke financiering voor de veiligheid van deze entiteiten;

21. verzoekt zijn Voorzitter deze resolutie te doen toekomen aan de Commissie en aan de Raad, alsmede aan de regeringen en de parlementen van de lidstaten.