Raad van de
Europese Unie

Brussel, 17 oktober 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	17 oktober 2022
aan:	de delegaties
nr. vorig doc.:	12930/22
Betreft:	Conclusies van de Raad over de beveiliging van ICT-toeleveringsketens - Raadsconclusies die door de Raad zijn goedgekeurd tijdens zijn zitting van 17 oktober 2022

Voor de delegaties gaan hierbij de conclusies van de Raad over de beveiliging van de ICT-toeleveringsketens, die door de Raad zijn goedgekeurd tijdens zijn zitting van 17 oktober 2022.

BIJLAGE

Conclusies van de Raad over de beveiliging van ICT-toeleveringsketens

DE RAAD VAN DE EUROPESE UNIE,

HERINNEREND aan zijn conclusies over

– de Gezamenlijke mededeling aan het Europees Parlement en de Raad van 20 november 2017: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU",

– het opbouwen van capaciteit en vermogens op het gebied van cyberbeveiliging in de EU,

– het belang van 5G voor de Europese economie en de noodzaak om de veiligheidsrisico's in verband met 5G te beperken,

– de digitale toekomst van Europa vormgeven,

– "een herstel dat de overgang naar een meer dynamische, veerkrachtige en concurrerende Europese industrie bevordert"

– de cyberbeveiliging van verbonden apparaten,

– de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk,

– de ontwikkeling van de cyberhouding van de Europese Unie,

– Speciaal verslag 03/2022 van de Europese Rekenkamer: "Uitrol van 5G in de EU: vertragingen bij de invoering van netwerken, waarbij beveiligingskwesties nog niet zijn opgelost",

HERINNEREND aan de volgende conclusies van de Europese Raad

– COVID-19, de eengemaakte markt, het industriebeleid, digitalisering en externe betrekkingen van 1-2 oktober 2020,

– de Russische militaire agressie tegen Oekraïne, veiligheid en defensie, energie, economische vraagstukken, COVID-19 en externe betrekkingen van 24-25 maart 2022,

– Oekraïne, voedselzekerheid, veiligheid en defensie, en energie van 30-31 mei 2022,

1. BENADRUKT dat de Europese Unie en haar lidstaten, gezien het toenemende belang van geopolitiek voor cyberbeveiliging, deze op een alomvattende en strategische manier moeten benaderen. De militaire agressie van Rusland tegen Oekraïne heeft een grote verschuiving veroorzaakt in de strategische en veiligheidsomgeving van de Europese Unie en heeft duidelijk gemaakt dat de Europese Unie sterker en slagvaardiger moet zijn op het gebied van veiligheid en defensie. De agressie liet zien dat het van het grootste belang is om rekening te houden met het geopolitieke klimaat, niet alleen bij het reageren op kwaadwillige cyberactiviteiten, maar ook bij het opbouwen en in stand houden van de weerbaarheid van informatie- en communicatietechnologieën (ICT). Dit geldt met name voor toeleveringsketens van ICT-producten en -diensten (ICT-toeleveringsketens), die zowel in gevaar kunnen komen door geopolitieke rivaliteit, zoals bij de SolarWinds-aanval het geval was, als door geopolitieke spanningen en instabiliteit, zoals de dreiging die de afhankelijkheid van Russische ICT-leveranciers vormde ten tijde van de militaire agressie van Rusland tegen Oekraïne.

2. MERKT OP dat de aard van de risico's in verband met ICT-toeleveringsketens – een onderling verbonden reeks middelen en processen tussen marktdeelnemers (zoals gedefinieerd in Verordening (EU) 2019/1020) die begint met de aankoop van grondstoffen en gaat van de productie, verwerking en omslag tot de levering van ICT-producten en -diensten, inclusief ondersteuning tijdens de levenscyclus van ICT-producten en -diensten – unieke uitdagingen met zich meebrengt en mogelijk verstrekkende gevolgen heeft. Naast de risico's in verband met het ontbreken van ICT-producten, bijvoorbeeld als gevolg van tekorten aan kritieke grondstoffen en halfgeleiders die nodig zijn voor de productie, zijn de toeleveringsketens van ICT-producten en -diensten blootgesteld aan andere dreigingen. Ze kunnen bijvoorbeeld op geraffineerde en vaak verborgen wijze het doelwit zijn van of misbruikt worden door kwaadwilligen, met gevolgen voor de vertrouwelijkheid, integriteit en beschikbaarheid van verzonden en opgeslagen gevoelige gegevens.

3. ONDERKENT, omdat bij het beveiligen van ICT-activa een alle risico's omvattende aanpak nodig is, het belang van het voorstel voor de richtlijn betreffende de veerkracht van kritieke entiteiten om de fysieke beveiliging van deze entiteiten te verbeteren, en BENADRUKT dat niet alleen de weerbaarheid tegen cyberaanvallen in de toeleveringsketen moet worden vergroot, maar ook de algehele weerbaarheid en beveiliging van ICT-toeleveringsketens tegen alle soorten dreigingen, zoals natuurverschijnselen, systeemfalen, dreigingen van binnenuit en menselijke fouten. ERKENT dat de beveiliging van ICT-toeleveringsketens de bescherming van ICT-producten en -diensten betreft die worden geproduceerd, geleverd, aangekocht en gebruikt in ICT-toeleveringsketens, onder meer door individuele componenten en doorgegeven gegevens te beschermen.

4. SPOORT de lidstaten AAN om, op basis van de lessen die zijn getrokken uit de gevolgen van de strategische afhankelijkheid van de Europese Unie van Russische fossiele brandstoffen en uit de gevolgen van de verstoringen van de toeleveringsketens tijdens de COVID-19-pandemie (vooral wat betreft geneesmiddelen en halfgeleiders, waar de strategische afhankelijkheid van de EU aan het licht kwam), zich in te zetten om soortgelijke situaties van ongewenste strategische externe afhankelijkheid met betrekking tot ICT-producten en -diensten te voorkomen. Gezien de toenemende digitalisering van de samenleving en het toenemende gebruik van ICT in kritieke infrastructuur, moet strategische externe afhankelijkheid in verband met ICT-producten en -diensten en hun toeleveringsketens voortdurend worden geëvalueerd en waar nodig aangepakt.

5. HERINNERT ERAAN dat het tot stand brengen van strategische autonomie met behoud van een open economie een belangrijke doelstelling van de Unie is, waaronder ook het in kaart brengen en het verminderen van strategische afhankelijkheid valt, en het vergroten van de weerbaarheid voor de meest gevoelige industriële ecosystemen en specifieke – waaronder digitale – gebieden. Dit omvat het ontwikkelen en uitrollen van strategische digitale capaciteiten en infrastructuur, het versterken van het vermogen om autonome technologische keuzes te maken en, als een van de belangrijkste pijlers, het zorgen voor veerkrachtige en veilige infrastructuur, producten en diensten voor het opbouwen van vertrouwen in de digitale eengemaakte markt en binnen de Europese samenleving, met behoud van openheid, wereldwijde samenwerking met gelijkgestemde partners en concurrentievermogen, en benutting van de potentiële voordelen daarvan. Tot de kernwaarden van de Europese Unie behoort de bescherming van met name privacy, veiligheid, gelijkheid, menselijke waardigheid, de rechtsstaat en een open internet als noodzakelijke voorwaarden voor het tot stand brengen van een digitale samenleving, economie en industrie waarin de mens centraal staat.

6. MERKT OP dat als gevolg van de ontwikkelingen in het cyberdreigingslandschap, wat zeer ingrijpende en geavanceerde aanvallen op toeleveringsketens – zoals SolarWinds, Mimecast en Kaseyain – de afgelopen jaren al lieten zien en die gelijk met de uitbesteding van essentiële ICT-diensten opkwamen en nog sterker zijn geworden door de algemene afhankelijkheid van ICT-producten en -diensten die door derden worden geproduceerd, verstrekt of verzorgd, er zich in de toekomst meer aanvallen op de toeleveringsketen zullen voordoen, met aanzienlijke schade voor de economie en de samenleving. BENADRUKT in het licht hiervan dat het belangrijk is de beveiliging en weerbaarheid van ICT-toeleveringsketens voor de werking van de eengemaakte markt te verbeteren, net als de noodzaak om de beschikbaarheid, veiligheid en diversiteit van ICT-producten en -diensten op de eengemaakte markt te waarborgen. ONDERKENT derhalve dat het gebruik van de bestaande EU-instrumenten en -benaderingen om deze doelstellingen te verwezenlijken moet worden gemaximaliseerd en gestroomlijnd, en dat voortdurend moet worden ingespeeld op het veranderende cyberdreigingslandschap door aanvullende passende maatregelen en mechanismen in te voeren, onder meer met betrekking tot mogelijke veiligheidsrisico's van opkomende en disruptieve technologieën. MOEDIGT de lidstaten AAN om in dit verband de risicogebaseerde aanpak te volgen om nieuwe technologische ontwikkelingen aan te pakken.

7. IS ZICH ERVAN BEWUST dat inzicht in het voortdurend veranderende cyberdreigingslandschap en de complexiteit van aanvallen in de toeleveringsketen van essentieel belang is voor een doeltreffende beperking van de risico's in verband met ICT-toeleveringsketens. BENADRUKT in dit verband dat het nodig is zich aan nieuwe dreigingen aan te passen door het dreigingslandschap van de toeleveringsketen actief en voortdurend te monitoren, te analyseren en te beoordelen, het bewustzijn te vergroten en kennis te vergaren over dreigingen en kwetsbaarheden, en de betrokken entiteiten proactief op maat te waarschuwen. IS INGENOMEN met de werkzaamheden van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) op het gebied van de beveiliging van ICT-toeleveringsketens, met name met het verslag van het Agentschap over het dreigingslandschap voor aanvallen in de toeleveringsketen.

SECTOROVERSCHRIJDENDE INSTRUMENTEN EN BENADERINGEN

8. HERHAALT dat het belangrijk is dat de lidstaten nagaan of het noodzakelijk is aanbieders van kritieke ICT te diversifiëren om het ontstaan van grote afhankelijkheden van één enkele aanbieder─ en vooral indien dit een aanbieder is met een hoog risico ─ te voorkomen of te beperken, aangezien lidstaten hierdoor in toenemende mate worden blootgesteld aan mogelijke verstoringen en de gevolgen daarvan. ERKENT dat het vermijden van aanbiederafhankelijkheid en het diversifiëren van ICT-aanbieders belangrijke factoren zijn voor de stabiliteit en de veiligheid van de interne markt. BENADRUKT dat adequate strategieën moeten worden gestimuleerd en uitgevoerd om het gemakkelijker te maken aanbieders te diversifiëren en het concurrentievermogen op technologieneutrale wijze een steuntje in de rug te geven. MOEDIGT het daarnaast AAN dat elementen die verband houden met het vermijden van aanbiederafhankelijkheid in EU-wetgeving worden opgenomen. SPREEKT in dit verband ZIJN WAARDERING UIT voor het voorstel voor een verordening betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van gegevens (dataverordening); dit voorstel is bedoeld om de interoperabiliteit van diensten voor gegevensverwerking te vergroten en belemmeringen voor het overstappen naar andere aanbieders van dit soort diensten uit de weg te ruimen.

9. ERKENT het verband tussen de beveiliging van ICT-toeleveringsketens en openbare aanbestedingen. BENADRUKT dat in aanbestedingsprocedures naar behoren moet worden gelet op het belang van de beveiliging van ICT-toeleveringsketens, en wel door in voorkomend geval objectieve en op risico's gebaseerde selectiecriteria te hanteren voor het vermogen van inschrijvers om een hoog niveau van veiligheid van hun diensten te waarborgen. ROEPT ertoe OP te streven naar het juiste evenwicht tussen enerzijds een zo efficiënt en billijk mogelijk gebruik van overheidsmiddelen en anderzijds het beveiligen van informatiesystemen en het waarborgen van de soepele werking van de interne markt, elementen waarmee in beide gevallen het openbaar belang is gediend. VERZOEKT de Commissie om ter vergemakkelijking van de uitvoering van de relevante aanbestedingsregels in het licht van de toenemende cyberbeveiliging, uiterlijk in het derde kwartaal van 2023 methodologische richtsnoeren te ontwikkelen om aanbestedende overheidsdiensten aan te sporen passende aandacht te schenken aan de cyberbeveiligingspraktijk van inschrijvers en hun onderaannemers, en om, indien nodig, voorstellen te doen om de wetgeving inzake aanbestedingsprocedures te herzien of aan te vullen.

10. ONDERKENT dat buitenlandse directe investeringen in ICT-producten en -diensten zeker economische en sociale voordelen opleveren voor lidstaten, bedrijven en burgers, maar dat deze investeringen ook risico's voor de veiligheid en de openbare orde kunnen inhouden, en NEEMT er NOTA VAN dat het screeningmechanisme voor buitenlandse directe investeringen van de EU en de nationale screeningsystemen, die beide middelen bieden om iets te doen aan dergelijke risico's, ook kunnen worden ingezet voor de beveiliging en de bestendigheid van ICT-toeleveringsketens, en wel doordat deze systemen bijdragen tot het elimineren van risicovolle investeringen die van invloed kunnen zijn op de beveiliging en de bestendigheid van deze ketens. ERKENT dat informatie die via dit mechanisme wordt uitgewisseld en gedeeld, de lidstaten kan helpen een beter beeld te krijgen van mogelijke bedreigingen voor de veiligheid van ICT-toeleveringsketens en op basis daarvan de nodige maatregelen te nemen. ROEPT de betrokken nationale entiteiten OP om in voorkomend geval ook oog te hebben voor dit aspect van het screeningmechanisme.

11. HERHAALT met betrekking tot defensie zijn verzoek aan de Commissie, in 2023 samen met de lidstaten de risico's voor toeleveringsketens van kritieke infrastructuur op verschillende gebieden ─ waaronder op digitaal terrein ─ in kaart te brengen, zijnde risico's die verband houden met de veiligheids- en defensiebelangen van de EU, alsmede de mogelijkheden te onderzoeken om de cyberbeveiliging in de gehele toeleveringsketen van de technologische en industriële defensiebasis van de EU te vergroten. VERZOEKT de lidstaten en de Commissie voorts, bij de uitvoering van de toezeggingen en acties van het strategisch kompas inzake veiligheid en defensie aandacht te schenken aan de beveiliging van ICT-toeleveringsketens.

12. Erkent het belang van kritieke grondstoffen en alle soorten halfgeleiders als fundamentele bouwstenen voor ICT-producten, en SPOORT AAN tot constructieve onderhandelingen over het voorstel voor een verordening tot vaststelling van een kader voor maatregelen ter versterking van het Europese ecosysteem voor halfgeleiders (Chipwet) en over het voorstel voor een verordening tot wijziging van Verordening (EU) 2021/2085 voor de oprichting van Gemeenschappelijke Ondernemingen in het kader van Horizon Europa, en wel in het bijzonder voor zover dit voorstel de Gemeenschappelijke Onderneming voor chips betreft.

CYBERSPECIFIEKE INSTRUMENTEN

13. ONDERKENT vooral met betrekking tot de telecommunicatie-infrastructuur de prestaties op het niveau van de Unie om de beveiliging van de toeleveringsketen voor 5G-netwerken te verbeteren, in het bijzonder via de EU-toolbox inzake 5G-cyberbeveiliging. ROEPT de lidstaten OP, informatie uit te wisselen over beste praktijken en methodieken voor de uitvoering van maatregelen die in de toolbox worden aanbevolen, en met name ─ indien passend ─ voor essentiële activa die in de gecoördineerde EU-risicobeoordelingen zijn aangemerkt als kritiek en gevoelig, beperkingen op te leggen aan aanbieders met een hoog risico. BENADRUKT dat de toolbox een flexibel, risicogestuurd instrument is om veiligheidsproblemen aan te pakken die aan het licht zijn gekomen, waardoor er tijdig en efficiënt kan worden opgetreden bij moeilijkheden in verband met 5G-cyberbeveiliging, zulks met inachtneming van de bevoegdheden van de lidstaten, en ERKENT dat de toolbox een waardevol instrument is om de beveiliging van ICT-toeleveringsketens van telecommunicatienetwerken op gecoördineerde wijze en volledig transparant te verbeteren; deze werkwijze kan dienen als inspirerend voorbeeld voor instrumenten inzake risicobeoordeling en -mitigatie in andere vitale sectoren. HERINNERT AAN het verzoek van overheidsdiensten die belast zijn met cyberbeveiliging van ICT-toeleveringsketens, om op basis van risicobeoordelingen aanbevelingen te formuleren aan de lidstaten en aan de Commissie om de bestendigheid van communicatienetwerken en -infrastructuur in de Europese Unie te versterken, mede door de verdere implementatie van de toolbox.

14. WIJST OP het belang van interoperabele benaderingen die iets kunnen doen aan het risico van aanbiederafhankelijkheid en het risico van concentratie kunnen verminderen, en die tegelijkertijd de beveiliging van toeleveringsketens in het gehele spectrum van ICT-infrastructuur en -diensten ten goede kunnen komen. ERKENT in dit verband de potentiële voordelen van het Open RAN-concept, met name voor 5G-netwerken, en WIJST tegelijkertijd OP het verslag over de cyberbeveiliging van Open RAN van de NIS-samenwerkingsgroep, waarin wordt verklaard dat dit concept nog in ontwikkeling is en dat de beveiliging, de transparantie en de standaardisering van Open RAN nog in de kinderschoenen staan, en BENADRUKT dat het belangrijk is de risico's in kaart te brengen en te beoordelen voordat wordt overgestapt op nieuwe normen of architecturen.

15. Benadrukt het belang van bestaande en toekomstige horizontale wetgeving voor cyberbeveiliging om daarmee de beveiliging van ICT-toeleveringsketens te versterken. Met name kan worden gewezen op de verordening inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de cyberbeveiligingsverordening), de toekomstige richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (de NIS 2-richtlijn), het voorstel voor een verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie, alsook het voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (kortweg de nieuwe Europese wet inzake cyberweerbaarheid). NEEMT voorts NOTA van de belangrijke ontwikkelingen in sectorspecifieke verordeningen voor cyberbeveiliging, met name de toekomstige verordening betreffende digitale operationele veerkracht voor de financiële sector (DORA), die een toezichtskader omvat voor derde aanbieders van ICT-diensten die van cruciaal belang zijn voor financiële entiteiten. De sectorspecifieke verordeningen bevatten naast algemene verplichtingen voor de beveiliging van ICT-toeleveringsketens gedetailleerde en specifieke vereisten voor de betrokken sector. BEKLEMTOONT tegelijkertijd dat aanbieders hun producten en diensten dikwijls aan verschillende sectoren leveren en niet aan één enkele bedrijfstak. Daarom is het van groot belang dat de beveiligingsvereisten voor ICT-toeleveringsketens in alle relevante sectoren zoveel mogelijk op elkaar worden afgestemd, met name in de sectoren die onder de toekomstige NIS 2-richtlijn vallen. Zo kunnen discrepanties tussen de verplichtingen voor aanbieders worden voorkomen en kan de lastendruk voor exploitanten in kritieke sectoren worden teruggedrongen (zij moeten immers nagaan of de aanbieders deze verplichtingen nakomen); hierbij moet rekening worden gehouden met de specifieke kenmerken van de sector.

16. IS BLIJ met het voorstel voor een wet inzake cyberweerbaarheid; dit is belangrijke wetgeving ten behoeve van de veilige ontwikkeling van producten met digitale elementen; de wet kan ervoor zorgen dat cyberbeveiliging een element wordt in de gehele levenscyclus van producten met digitale elementen. MERKT OP dat deze wet in belangrijke mate de beveiliging van ICT-toeleveringsketens kan versterken. SPOORT AAN tot opbouwende onderhandelingen en een spoedige vaststelling van deze wet.

17. IS in dit verband INGENOMEN met de werkzaamheden van Enisa, dat samen met de lidstaten en andere belanghebbenden ten behoeve van de EU certificeringsregelingen uitwerkt voor ICT-producten, -diensten en -processen overeenkomstig de cyberbeveiligingverordening; deze certificeringen moeten uitmonden in een hoger algemeen niveau van cyberbeveiliging binnen de digitale eengemaakte markt. SPOORT alle belanghebbenden AAN, te participeren in de werkzaamheden ter voorbereiding van afzonderlijke Europese certificeringsregelingen om zo het nodige vertrouwen in veilige ICT-producten, -processen en -diensten te creëren en hun bestendigheid te vergroten, en ROEPT de Commissie OP, onverwijld na voltooiing van de voorbereidende werkzaamheden uitvoeringshandelingen voor deze regelingen op tafel te leggen, met name voor de *Common Criteria-based European cybersecurity certification scheme (EUCC)*. MERKT OP dat deze regelingen indien nodig vereisten inzake de beveiliging van ICT-toeleveringsketens moeten omvatten, waaronder gegevens over relaties met aanbieders.

18. BEKLEMTOONT dat alle toekomstige NIS 2-bepalingen voor de beveiliging van ICT-toeleveringsketens ook terdege moeten worden uitgevoerd. ONDERSTREEPT in dit verband het belang van gecoördineerde EU-risicobeoordelingen van kritieke ICT-toeleveringsketens (gecoördineerde risicobeoordelingen van de ketens), van nationale beleidsmaatregelen voor de beveiliging van toeleveringsketens, en van beveiligingsmaatregelen die in het algemeen verband houden met toeleveringsketens. MERKT OP dat, als het gaat om de veiligheidsrisico's van de primaire aanbieder of van de eindafnemer, de aandacht niet alleen moet uitgaan naar primaire aanbieders maar ook naar hun onderaannemers. MOEDIGT Enisa AAN, met behulp van de NIS-samenwerkingsgroep beste praktijken voor risicobeheer van ICT-toeleveringsketens te inventariseren en deze samen te brengen in methodologische richtsnoeren, teneinde zo de uitvoering van maatregelen voor risicobeheer van toeleveringsketens te vergemakkelijken. SPOORT voorts Enisa AAN, toezicht te houden op investeringen in de beveiliging van ICT-toeleveringsketens van entiteiten die onder de toekomstige NIS 2-richtlijn vallen.

19. WIJST ook OP de voordelen en risico's van het gebruik van aanbieders van beheerde diensten (MSP's) en aanbieders van beheerde beveiligingsdiensten (MSSP's) in de context van de beveiliging van de toeleveringsketen. Hoewel het gebruik van deze aanbieders de veiligheid binnen organisaties aanzienlijk kan verbeteren en tot een hoger niveau van cyberbeveiliging kan leiden, kan het beheer op afstand van ICT-systemen en -diensten in combinatie met bevoorrechte toegang tot de ICT-omgeving van de klanten, iets wat MSP's en MSSP's nodig kunnen hebben, in het geval van gecompromitteerde MSP's of MSSP's leiden tot ingrijpende cascade-effecten voor een groot aantal klanten. Daarom is het van het grootste belang dat de MSP's en MSSP's een hoog niveau van interne veiligheid en van de veiligheid van de diensten die zij verlenen, handhaven en ten aanzien van hun klanten zeer transparant zijn wat betreft de veiligheid van de diensten die zij verlenen. Is in dit verband INGENOMEN MET de toekomstige opneming ervan in het toepassingsgebied van de komende NIS 2-richtlijn.

20. NEEMT met betrekking tot de uitvoering van het mechanisme voor gecoördineerde risicobeoordelingen van de toeleveringsketen uit hoofde van de komende NIS 2-richtlijn NOTA VAN de relevantie van niet-technische risicofactoren in dit verband, zoals ongepaste beïnvloeding van leveranciers en dienstverleners door een derde land, en ERKENT in dit verband de factoren die kunnen worden gebruikt om het risicoprofiel te beoordelen, zoals vermeld in de gecoördineerde EU-risicobeoordeling van de cyberbeveiliging van 5G-netwerken. VERZOEKT de Commissie om uiterlijk in het tweede kwartaal van 2023, na raadpleging van de NIS-samenwerkingsgroep en Enisa, de specifieke ICT-diensten, -systemen of -producten te identificeren die met voorrang aan de gecoördineerde risicobeoordelingen van de toeleveringsketen kunnen worden onderworpen.

21. MERKT OP dat afhankelijkheid van risicovolle leveranciers van ICT-producten en -diensten die worden gebruikt voor de exploitatie van kritieke netwerken en systemen een strategische bedreiging vormt die moet worden beperkt door middel van passend beleid op zowel nationaal als EU-niveau en door samenwerking tussen de lidstaten en met gelijkgestemde internationale partners. VERZOEKT de NIS-samenwerkingsgroep om, in samenwerking met de Commissie en Enisa, een instrumentarium met maatregelen te ontwikkelen om kritieke ICT-risico's in de toeleveringsketen te verminderen, teneinde de beperking van dit strategische risico te vergemakkelijken en de gecoördineerde risicobeoordelingen van de toeleveringsketen van de toeleveringsketen te ondersteunen (ICT-toolbox voor de toeleveringsketen). De ICT-toolbox voor de toeleveringsketen moet voortbouwen op strategische dreigingsscenario's voor ICT-toeleveringsketens en maatregelen bieden om op deze scenario's te reageren door gebruik te maken van de ervaringen die zijn opgedaan met de 5G-toolbox en de ervaringen die op nationaal niveau zijn opgedaan. De ICT-toolbox moet op transparante wijze een aanvulling vormen op de gecoördineerde risicobeoordelingen van de toeleveringsketen voor specifieke ICT-diensten, -systemen of -producten in het kader van de komende NIS 2-richtlijn door generieke maatregelen aan te bieden ter beperking van risico's die op schaalbare wijze kunnen worden aangepast voor specifieke ICT-diensten, -systemen of -producten, op basis van de risico's die in de afzonderlijke gecoördineerde risicobeoordelingen van de toeleveringsketen zijn vastgesteld.

22. BENADRUKT de belangrijke rol van onderzoek, innovatie, investeringen en ondernemersactiviteiten op het gebied van digitalisering en cyberbeveiliging, alsook van de financiering van dergelijke activiteiten, met het oog op het vermijden van mogelijke toekomstige ongewenste strategische afhankelijkheden en het versterken van de algehele veerkracht van de ICT-toeleveringsketens. ONDERSTREEPT in dit verband de rol en de relevantie van zowel de strategische als de uitvoeringstaken van het Europees Kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging (ECCC) en het netwerk van nationale coördinatiecentra (NCC's) om bij te dragen tot het maximaliseren van de effecten van investeringen ter versterking van het leiderschap en de open strategische autonomie van de EU op het gebied van cyberbeveiliging en de ondersteunende technologische capaciteiten en vaardigheden van de EU, en om het mondiale concurrentievermogen van de EU te vergroten. ROEPT in dit verband OP tot een snelle operationalisering van het ECCC. VERZOEKT het ECCC in zijn strategische agenda rekening te houden met de beveiligingsaspecten van de ICT-toeleveringsketen, met inbegrip van bijvoorbeeld de ontwikkeling van veilige software, en daarbij te zorgen voor consistentie en complementariteit en dubbel werk te voorkomen. STEUNT de versterking van het Europese concurrentievermogen op het gebied van cyberbeveiliging door middel van financieringsprogramma's, zoals het programma Horizon Europa voor onderzoek en innovatie en het programma Digitaal Europa voor het versterken, opbouwen en verwerven van essentiële capaciteiten voor de digitale economie, samenleving en democratie van de EU.

ONDERSTEUNENDE MECHANISMEN

23. MOEDIGT het stimuleren van financiële steun voor maatregelen ter versterking van de beveiliging van de ICT-toeleveringsketen AAN. ROEPT het ECCC, de Commissie en relevante belanghebbenden OP om, mede met het oog op de komende uitvoering van de NIS 2-richtlijn, bij voorrang de mogelijkheden te onderzoeken om beveiligingsaspecten van de ICT-toeleveringsketen op te nemen in de komende oproepen voor de werkprogramma's voor cyberbeveiliging in het kader van het programma Digitaal Europa en het programma Horizon Europa, of andere relevante financieringsmogelijkheden te benutten. Deze financieringsmogelijkheden moeten onder meer de organisaties in staat stellen in de hele toeleveringsketen een hoog niveau van cyberbeveiliging te ondersteunen bij de aanschaf van ICT-producten en -diensten, met name wat de vervanging van specifieke kritieke ICT-diensten, -systemen of -producten betreft die overeenkomstig de toekomstige gecoördineerde risicobeoordelingen van de toeleveringsketen als risicovol worden aangemerkt.

24. ERKENT dat de mondialisering en de specialisatie van ICT-diensten en de toenemende afhankelijkheid van producten en diensten van derden de noodzaak meebrengen van nauwe samenwerking binnen de EU en op internationaal niveau bij het delen van kennis en deskundigheid tussen relevante belanghebbenden, en MOEDIGT hen AAN een sterke en gecoördineerde positie te vinden die de veiligheid van de ICT-toeleveringsketen op alomvattende wijze waarborgt. ERKENT ook dat de relevante geavanceerde benaderingen en technieken verder moeten worden onderzocht, zowel voor passende elementaire cyberhygiëne en langetermijnoplossingen voor veilige en veerkrachtige ICT-toeleveringsketens, evenals voor de meest geschikte manieren om deze te bevorderen en eventueel te integreren in beleids- of andere initiatieven. ONDERKENT in dit verband dat bijzondere aandacht moet worden besteed aan onderzoek naar de voor- en nadelen van systematische oplossingen, zoals de zero trust principles, de materiaalstaat van software en soortgelijke langetermijnoplossingen. BEVEELT AAN hiervoor gebruik te maken van de NIS-samenwerkingsgroep.

25. WIJST OP de voordelen van monitoring en doeltreffende uitwisseling van informatie over cyberincidenten en -dreigingen voor de preventie, opsporing en beperking van de gevolgen van aanvallen op de toeleveringsketen. BENADRUKT de noodzaak om vertrouwen tussen de lidstaten te blijven opbouwen met het oog op een doeltreffende uitwisseling van dergelijke informatie. HERINNERT in dat verband aan het voorstel van de Commissie om de lidstaten te ondersteunen bij het opzetten en versterken van operationele beveiligingscentra, teneinde een netwerk van dergelijke centra in de hele EU uit te bouwen, om signalen van mogelijke aanvallen op netwerken verder te monitoren en erop te anticiperen. HERINNERT AAN de noodzaak van complementariteit en coördinatie binnen bestaande netwerken en mechanismen, en BENADRUKT in dit verband met name de rol van het "Computer Security Incident Response Teams"-netwerk (CSIRT-netwerk) en de noodzaak om het potentieel van deze netwerken verder te onderzoeken om een doeltreffende, veilige en betrouwbare cultuur van informatie-uitwisseling te bevorderen. HERINNERT aan de door de EU gesteunde inspanningen van de lidstaten om sectorale, nationale en regionale CSIRT's en nationale of Europese centra voor informatie-uitwisseling en -analyse (ISAC's) op te zetten als onderdeel van een doeltreffend netwerk van cyberbeveiligingspartnerschappen in de Unie.

26. BENADRUKT, gezien de verwevenheid en de mondiale aard van bedreigingen van de ICT-toeleveringsketen, dat het belangrijk is de veiligheid van de ICT-toeleveringsketen op mondiaal niveau te benaderen en te verbeteren. BEVEELT met het oog hierop AAN gebruik te maken van digitale partnerschappen, cyberdialogen en andere relevante EU-initiatieven, waaronder, in voorkomend geval, vrijhandelsovereenkomsten, voor de bevordering van risicogebaseerde evaluaties van leveranciers van ICT-producten en aanbieders van ICT-diensten, het gebruik van betrouwbare leveranciers en de invoering van een veilig en innovatief digitaal ecosysteem op basis van open, interoperabele en transparante normen. WIJST daarnaast NOGMAALS OP de visie van de Global Gateway-partnerschappen en de Handels- en Technologieraad EU-VS, en de activiteiten in het kader van zijn werkgroepen, om het gebruik van betrouwbare/niet-risicovolle leveranciers te bevorderen en een financieringsmechanisme te ontwikkelen om projecten die ICT-infrastructuur en -diensten in derde landen veiliger, veerkrachtiger en betrouwbaarder maken tot stand te brengen, onder meer door op technologieneutrale wijze af te zien van het financieren van aankopen bij niet-betrouwbare/risicovolle leveranciers.

27. BEVESTIGT zijn toezegging om bij te dragen tot en te ijveren voor een open, vrije, mondiale, stabiele en veilige cyberruimte en zich te houden aan de normen, regels en beginselen van verantwoordelijk gedrag van staten in de cyberspace die in het raamverdrag van de VN zijn vastgelegd. HERINNERT, met name met betrekking tot de beveiliging van de ICT-toeleveringsketen, AAN de door de VN-groep van regeringsdeskundigen en de open werkgroep OEWG goedgekeurde norm die staten aanmoedigt redelijke stappen te ondernemen om de integriteit van de toeleveringsketen te waarborgen, onder meer door de ontwikkeling van objectieve samenwerkingsmaatregelen, zodat eindgebruikers vertrouwen kunnen hebben in de beveiliging van ICT-producten, en ernaar te streven de verspreiding van kwaadwillige ICT-instrumenten en -technieken en het gebruik van schadelijke verborgen functies te voorkomen, en PLEIT voor de brede toepassing ervan.