Advies van het Europees Economisch en Sociaal Comité over het voorstel voor een verordening van het Europees Parlement en de Raad tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Rapporteur: **Antonio LONGO**

Corapporteur: **Alberto MAZZOLA**

Raadpleging	Europese Raad, 5.10.2018 Europees Parlement, 1.10.2018
Rechtsgrondslag	Artikelen 173(3), 188 en 304 van het Verdrag betreffende de werking van de Europese Unie
Bevoegde afdeling	Afdeling Vervoer, Energie, Infrastructuur en Informatiemaatschappij
Goedkeuring door de afdeling	9.1.2019
Goedkeuring door de voltallige vergadering	23.1.2019
Zitting nr.	540
Stemuitslag (voor/tegen/onthoudingen)	143/5/2

1. Conclusies en aanbevelingen

1.1. Het Europees Economisch en Sociaal Comité (EESC) is ingenomen met het initiatief van de Commissie en acht dit nuttig voor de ontwikkeling van een industriële strategie voor cyberbeveiliging ter verzekering van een solide en verregaande digitale autonomie. Een en ander is onontbeerlijk voor de versterking van de Europese beschermingsmechanismen in de cyberoorlog die momenteel gaande is en die de politieke, economische en sociale stelsels in gevaar dreigt te brengen.

1.2. Een strategie voor cyberbeveiliging zal alleen maar vruchten afwerpen als er sprake is van een brede bewustwording en van veilig gedrag van alle gebruikers.

1.3. Het Comité staat achter de algemene doelstellingen van het voorstel en is er zich van bewust dat specifieke aspecten van de werking ervan verder zullen worden geanalyseerd. Aangezien het een verordening betreft, zouden sommige gevoelige kwesties in verband met governance, financiering en realisering van gestelde doelen niettemin op voorhand moeten worden omschreven. Het is belangrijk dat het toekomstige netwerk en het kenniscentrum zo veel mogelijk voortbouwen op de cybervaardigheden en expertise van de lidstaten en dat de verantwoordelijkheden niet al te zeer worden geconcentreerd in het op te richten kenniscentrum. Ook moet worden voorkomen dat de werkterreinen van het toekomstige netwerk en het kenniscentrum en de bestaande samenwerkingsmechanismen en instellingen elkaar overlappen.

1.4. Het EESC is er voorstander van om op basis van harde toezeggingen op wetenschappelijk en investeringsgebied, de samenwerking uit te breiden tot de industrie, en deze in de toekomst ook in de raad van bestuur op te nemen. In het geval van een tripartiete samenwerking tussen de Europese Commissie, de lidstaten en de industrie moet de aanwezigheid van ondernemingen van buiten de EU beperkt blijven tot de bedrijven die al langere tijd op Europees grondgebied zijn gevestigd en volledig betrokken zijn bij de technologische en industriële basis van Europa. Voorwaarde hierbij is wel dat deze ondernemingen worden onderworpen aan passende screening- en controlemechanismen, en tevens worden gehouden aan de naleving van het wederkerigheidsbeginsel en de verplichtingen inzake vertrouwelijkheid.

1.5. Cyberbeveiliging moet een gezamenlijke inspanning zijn van alle lidstaten, die derhalve op nog vast te stellen voorwaarden deel moeten uitmaken van de raad van bestuur. Met betrekking tot de financiële bijdragen van de lidstaten kan gebruik worden gemaakt van de aan elk van hen toegewezen EU-middelen.

1.6. In het voorstel moet nader worden omschreven op welke wijze het kenniscentrum kan ingrijpen bij het coördineren van de financiering van de programma's Digitaal Europa en Horizon Europa en met name op basis van welke richtsnoeren mogelijke overheidsopdrachten zullen worden uitgeschreven en gegund. Dit is van cruciaal belang om dubbel werk en overlapping te voorkomen. Om meer begrotingsmiddelen vrij te krijgen wordt bovendien aanbevolen de synergieën met andere financiële instrumenten van de EU uit te breiden (bijvoorbeeld regionale fondsen, structuurfondsen, CEF, EDF en InvestEU).

1.7. Het EESC acht het van cruciaal belang dat de voorwaarden van de samenwerking en de relaties tussen het Europees centrum en de nationale centra worden vastgesteld. Daarnaast is het van belang dat de nationale centra door de EU worden gefinancierd, ten minste voor wat de administratieve kosten betreft, om zo harmonisering op administratief en bevoegdheidsgebied te bevorderen en de bestaande kloof tussen de Europese landen te verkleinen.

1.8. Het Comité wijst nogmaals op het belang van menselijk kapitaal en hoopt dat het kenniscentrum, in samenwerking met universiteiten, onderzoekscentra en centra voor hoger onderwijs, excellent onderwijs en opleiding zal bevorderen, onder meer via specifieke universitaire en hogeschoolopleidingen. Ook is het essentieel om te voorzien in specifieke steun voor start-ups en kleine en middelgrote ondernemingen (kmo's).

1.9. Het EESC acht het van essentieel belang de respectieve bevoegdheden en taken van het kenniscentrum en het European Network and Information Security Agency (Enisa) duidelijker af te bakenen door de wijze van samenwerking en wederzijdse ondersteuning duidelijk te omschrijven en overlapping van bevoegdheden en dubbel werk te voorkomen. Andere instanties die zich bezighouden met cyberbeveiliging, zoals EDA, Europol en CERT-EU, kampen met vergelijkbare problemen. Daarom pleit het EESC voor de vaststelling van soortgelijke mechanismen voor een gestructureerde dialoog tussen de verschillende instanties.

2. **Het bestaande kader voor cyberbeveiliging**

2.1. Cyberbeveiliging is een onderwerp dat hoog op de EU-agenda staat, aangezien het een onmisbare factor is voor de bescherming van de instanties, ondernemingen en burgers, en een noodzakelijk instrument vormt voor de instandhouding van democratieën. Een van de meest verontrustende verschijnselen is de gigantische toename van de hoeveelheid malware die via automatische systemen over het internet wordt verspreidt, met een groei van 130000 gevallen in 2007 tot 8 miljoen gevallen in 2017. Daarnaast is de Unie een netto-invoerder van producten en oplossingen op het gebied van cyberbeveiliging, hetgeen problemen veroorzaakt met betrekking tot het concurrentievermogen en de burger- en militaire veiligheid.

2.2. Hoewel de EU over aanzienlijke kennis en ervaring beschikt op het gebied van cyberbeveiliging, lijken de bedrijfstak, de universiteiten en de onderzoekscentra nog altijd versnipperd, onsamenhangend en verstoken van een gezamenlijke ontwikkelingsstrategie. Dit is te wijten aan het feit dat de betreffende sectoren op het gebied van cyberbeveiliging (bijvoorbeeld energie, ruimtelijke ordening, defensie en vervoer) niet voldoende worden ondersteund, net zo min als de synergieën tussen de civiele en defensiecyberbeveiliging op hun juiste waarde worden geschat.

2.3. Om het hoofd te bieden aan de toenemende uitdagingen heeft de Unie in 2013 een strategie voor cyberbeveiliging vastgesteld ter bevordering van een betrouwbaar, veilig en open cyber-ecosysteem ([1]). Vervolgens zijn in 2016 de eerste specifieke maatregelen vastgesteld voor de beveiliging van netwerk- en informatiesystemen ([2]). Dit proces heeft geleid tot de oprichting van het publiek-private partnerschap voor cyberbeveiliging („cPPP").

2.4. In de mededeling van 2017 met als titel „Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU" ([3]) wordt benadrukt dat belangrijke technologische capaciteit op het gebied van cyberbeveiliging gehandhaafd en ontwikkeld moet worden om de digitale eengemaakte markt en met name kritieke informatienetwerken en -systemen te beschermen, alsook om in basisvoorzieningen op het gebied van cyberbeveiliging te voorzien.

([1]) JOIN(2013) 1 final.
([2]) 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 (PB L 194 van 19.7.2016, blz. 1).
([3]) JOIN(2017) 450 final.

2.5. De Unie moet derhalve haar eigen digitale bronnen en processen kunnen beschermen en op de wereldwijde markt voor cyberbeveiliging kunnen concurreren teneinde een sterke en verregaande digitale autonomie tot stand te brengen ([4]).

3. De voorstellen van de Commissie

3.1. Het is de bedoeling dat het kenniscentrum de activiteiten van het netwerk van nationale centra vergemakkelijkt en coördineert, en als referentie dient voor de kennisgemeenschap op het gebied van cyberbeveiliging, waarbij het de technologische agenda opstelt ten aanzien van cyberbeveiliging en de toegang tot verworven kennis vergemakkelijkt.

3.2. In het bijzonder moet het kenniscentrum de relevante delen van de programma's Digitaal Europa en Horizon Europa uitvoeren door middelen vrij te maken en zich bezig te houden met aanbestedingsprocedures. Gezien de grote investeringen in cyberbeveiliging die elders ter wereld zijn gedaan en het feit dat de middelen binnen de sector in Europa gecoördineerd en gebundeld moeten worden, wordt voorgesteld om het kenniscentrum op te zetten als een Europees partnerschap met een dubbele rechtsgrondslag, zodat makkelijker gebruik kan worden gemaakt van gezamenlijke investeringen van de Unie, de lidstaten en/of de sector.

3.3. In het voorstel is bepaald dat de lidstaten een bijdrage leveren met een bedrag dat is afgestemd op de activiteiten van het kenniscentrum en het netwerk. De door de EU toegewezen financiële middelen bedragen circa 2 miljard EUR uit het programma Digitaal Europa, een nader te bepalen bedrag afkomstig uit het programma Horizon Europa en een algemene bijdrage door de lidstaten die ten minste even hoog is als de communautaire bijdrage.

3.4. Het belangrijkste besluitvormingsorgaan is de raad van bestuur, waarin alle lidstaten zijn vertegenwoordigd, maar alleen de landen die een financiële bijdrage hebben geleverd stemrecht hebben. De stemprocedure verloopt volgens het beginsel van de dubbele meerderheid, waarvoor 75 % van de financiële bijdrage en 75 % van de stemmen vereist zijn. De Commissie bezit 50 % van de stemmen. Het kenniscentrum wordt bijgestaan door een industrieel en wetenschappelijk adviescomité dat de dialoog met bedrijven, consumenten en andere belanghebbenden in stand houdt.

3.5. Door zijn nauwe samenwerking met het netwerk van nationale coördinatiecentra en de kennisgemeenschap op het gebied van cyberbeveiliging, is het kenniscentrum het belangrijkste uitvoerende orgaan van de door de EU aan cyberbeveiliging toegewezen fondsen in het kader van de voorgestelde programma's Digitaal Europa en Horizon Europa.

3.6. De nationale coördinatiecentra worden door de lidstaten geselecteerd. Deze centra moeten beschikken over technologische kennis op het gebied van cyberbeveiliging of moeten daar direct toegang toe krijgen, met name wat betreft encryptie, ICT-beveiligingsdiensten, automatische detectie van indringers, beveiliging van systemen, netwerken, software en applicaties, en de menselijke en sociale aspecten van beveiliging en privacy. Bovendien moeten zij zich doeltreffend kunnen aanpassen aan en samenwerken met de industrie, de publieke sector, waaronder de op grond van Richtlijn 2016/1148 aangewezen autoriteiten.

4. Algemene opmerkingen

4.1. Het EESC is ingenomen met het initiatief van de Commissie en acht dit van strategisch belang voor de ontwikkeling van cyberbeveiliging bij de uitvoering van hetgeen op de top van Tallinn in september 2017 overeengekomen is. Bij deze gelegenheid hebben de staatshoofden en regeringsleiders opgeroepen om van Europa uiterlijk in 2025 een leider in cyberbeveiliging te maken, zodat de burgers, consumenten en bedrijven met vertrouwen online kunnen gaan en bescherming genieten, en een vrij en aan het recht onderworpen internet mogelijk wordt.

4.2. Het EESC herhaalt dat er momenteel een echte cyberoorlog woedt die de politieke, economische en sociale stelsels in gevaar kan brengen en zowel computersystemen, kritieke infrastructuur (energie, vervoer, banken en financiële instellingen, ...) als ondernemingen aanvalt, en met nepnieuws tevens het electorale en democratische proces in het algemeen beïnvloedt ([5]). Meer bewustwording en een kordate en tijdige reactie zijn dan ook noodzakelijk. Het opstellen van een duidelijke en goed onderbouwde industriële strategie inzake cyberbeveiliging is dan ook een essentiële voorwaarde voor de verwezenlijking van digitale autonomie. Het EESC is van mening dat in het werkprogramma prioriteit moet worden gegeven aan gebieden die zijn genoemd in Richtlijn (EU) 2016/1148, welke van toepassing is op bedrijven die essentiële diensten leveren, zij het openbaar of particulier, vanwege hun belang voor de samenleving ([6]).

([4]) PB C 227 van 28.6.2018, blz. 86.

([5]) Informatief rapport over "Gebruik van de media om sociaalpolitieke processen in de EU en de Oostelijke nabuurlanden te beïnvloeden", Vareikytė, 2014.

([6]) PB C 227 van 28.6.2018, blz. 86.

4.3. Een strategie voor cyberbeveiliging zal alleen maar vruchten afwerpen als er sprake is van een brede bewustwording en van veilig gedrag van alle gebruikers. Om deze reden moet elk technologie-initiatief vergezeld gaan van passende voorlichtings- en bewustmakingscampagnes om een cultuur van digitale veiligheid te creëren ([7]).

4.4. Het Comité staat achter de algemene doelstellingen van het voorstel en is er zich van bewust dat specifieke aspecten van de werking ervan verder zullen worden geanalyseerd. Aangezien het een verordening betreft, zouden sommige gevoelige kwesties in verband met governance, financiering en realisering van gestelde doelen niettemin op voorhand moeten worden omschreven. Het is belangrijk dat het toekomstige netwerk en het kenniscentrum zo veel mogelijk voortbouwen op de cybervaardigheden en expertise van de lidstaten en dat de verantwoordelijkheden niet al te zeer worden geconcentreerd in het op te richten kenniscentrum. Ook moet worden voorkomen dat de werkterreinen van het toekomstige netwerk en het kenniscentrum en de bestaande samenwerkingsmechanismen en instellingen elkaar overlappen.

4.5. Het Comité wijst erop dat het in zijn advies TEN/646 over de cyberbeveiligingsverordening ([8]) een voorstel heeft gedaan voor een tripartiet publiek-privaat partnerschap tussen de Europese Commissie, de lidstaten en de industrie, met inbegrip van de kleine en middelgrote ondernemingen, terwijl de huidige structuur, waarvan de rechtsvorm moet worden verstevigd, in wezen voorziet in een publiek-publiek partnerschap tussen de Europese Commissie en de lidstaten.

4.6. Het EESC is er voorstander van om op basis van harde toezeggingen op wetenschappelijk en investeringsgebied, de samenwerking uit te breiden tot de industrie, en deze in de toekomst ook in de raad van bestuur op te nemen. De oprichting van een industrieel en wetenschappelijk adviescomité zal mogelijk geen garantie bieden voor een permanente dialoog met de bedrijven, consumenten en andere belanghebbenden. Voorts wordt in de nieuwe door de Commissie geschetste context niet duidelijk welke rol is weggelegd voor de European Cyber Security Organisation, die in juni 2016 op initiatief van de Commissie is opgericht als tegenhanger van de Commissie en waarvan het kostbare netwerk en de schat aan kennis niet verloren mogen gaan.

4.6.1. In het geval van een tripartiete samenwerking is het belangrijk om aandacht te besteden aan de kwestie van bedrijven uit derde landen. Het EESC benadrukt in het bijzonder dat deze samenwerking gebaseerd moet zijn op een rigoureus mechanisme om deelname te voorkomen van bedrijven uit landen van buiten de EU, die de veiligheid en autonomie van de Unie in gevaar kunnen brengen. De betreffende in het EDIDP ([9]) vastgestelde bepalingen moeten ook in dit kader van toepassing zijn.

4.6.2. Tegelijkertijd erkent het EESC dat sommige ondernemingen uit niet-EU-landen die evenwel al langere tijd op Europees grondgebied zijn gevestigd en volledig betrokken zijn bij de technologische en industriële basis van Europa, zeer nuttig kunnen zijn voor communautaire projecten en hier toegang toe moeten hebben, mits deze ondernemingen door de lidstaten worden gehouden aan passende screening- en controlemechanismen, evenals aan de naleving van het beginsel van wederkerigheid en de verplichtingen van vertrouwelijkheid.

4.7. Cyberbeveiliging moet een gezamenlijke inspanning zijn van alle lidstaten, die derhalve op nog vast te stellen voorwaarden deel moeten uitmaken van de raad van bestuur. Voorts is het ook van belang dat alle lidstaten financieel en op passende wijze bijdragen aan het initiatief van de Commissie. Met betrekking tot de financiële bijdragen van de lidstaten kan gebruik worden gemaakt van de aan elk van hen toegewezen EU-middelen.

4.8. Het EESC is het ermee eens dat elke lidstaat vrij is om een eigen vertegenwoordiger aan te wijzen in de raad van bestuur van het Europees kenniscentrum. De loopbaanprofielen van de nationale vertegenwoordigers moeten duidelijk omschreven zijn en zowel strategische en technologische als beheers-, administratieve en budgettaire vaardigheden vermelden.

4.9. In het voorstel moet nader worden omschreven op welke wijze het kenniscentrum een rol kan spelen bij het coördineren van de financiering van de programma's Digitaal Europa en Horizon Europa, waarover tot op heden onderhandelingen worden gevoerd, en met name op basis van welke richtsnoeren mogelijke overheidsopdrachten zullen worden uitgeschreven en gegund. Dit is van cruciaal belang om dubbel werk en overlapping te voorkomen. Om meer begrotingsmiddelen vrij te krijgen wordt bovendien aanbevolen de synergieën met andere financiële instrumenten van de EU uit te breiden (bijvoorbeeld regionale fondsen, structuurfondsen, CEF, EDF en InvestEU). Het Comité hoopt dat het netwerk van nationale centra zal worden betrokken bij het beheer en de coördinatie van de fondsen.

([7]) PB C 227 van 28.6.2018, blz. 86.
([8]) PB C 227 van 28.6.2018, blz. 86.
([9]) COM(2017) 294.

4.10. Het EESC merkt op dat het adviescomité uit 16 leden zou moeten bestaan maar dat de mechanismen op basis waarvan hiervoor een beroep zou worden gedaan op het bedrijfsleven, de academische wereld, de onderzoekswereld en de consument niet worden gespecificeerd. Het zou een goede zaak zijn als de leden van dit comité over een hoog niveau van kennis ter zake zouden beschikken en de verschillende betrokken sectoren op evenwichtige wijze zouden vertegenwoordigen.

4.11. Het EESC acht het van belang dat de voorwaarden van de samenwerking en de relaties tussen het Europees centrum en de nationale centra worden vastgesteld. Daarnaast is het van belang dat de nationale centra door de EU worden gefinancierd, ten minste voor wat de administratieve kosten betreft, om zo harmonisering op administratief en bevoegdheidsgebied te bevorderen en de bestaande kloof tussen de Europese landen te verkleinen.

4.12. In lijn met zijn eerdere adviezen ([10]) onderstreept het EESC het belang van excellent onderwijs en dito opleidingen van personeel op het gebied van cyberbeveiliging, onder meer door specifieke school-, universitaire en postdoctorale opleidingen. Voorts is het belangrijk om te voorzien in voldoende financiële middelen voor kmo's en start-ups in de sector ([11]), die onmisbaar zijn voor de ontwikkeling van baanbrekend onderzoek.

4.13. Het EESC acht het van essentieel belang de respectieve bevoegdheden en taken van het kenniscentrum en het Enisa duidelijker af te bakenen door de wijze van samenwerking en wederzijdse ondersteuning duidelijk te omschrijven en overlapping van bevoegdheden en dubbel werk te voorkomen ([12]). In het voorstel voor een verordening is bepaald dat een vertegenwoordiger van Enisa als permanent waarnemer zetelt in de raad van bestuur, maar dit biedt geen garantie voor een gestructureerde dialoog tussen de twee organen. Andere instanties die zich bezighouden met cyberbeveiliging, zoals EDA, Europol en CERT-EU, kampen met vergelijkbare problemen. In dit verband is de in mei 2018 ondertekende intentieverklaring tussen Enisa, EDA, Europol en CERT-EU van belang.

Brussel, 23 januari 2019.

De voorzitter
van het Europees Economisch en Sociaal Comité
Luca JAHIER

([10]) PB C 451 van 26.11.2014, blz. 64.
([11]) PB C 227 van 28.6.2018, blz. 86.
([12]) PB C 227 van 28.6.2018, blz. 86.