Advies van het Europees Economisch en Sociaal Comité over het voorstel 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, en over het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de veerkracht van kritieke entiteiten

(COM(2020) 823 final — 2020/0359 (COD) — COM(2020) 829 final — 2020/0365 (COD))

(2021/C 286/28)

Rapporteur: **Maurizio MENSI**

Raadpleging	Europees Parlement, 21.1.2021-11.2.2021
	Raad, 26.1.2021-19.2.2021
Rechtsgrondslag	Artikel 114 van het Verdrag betreffende de werking van de Europese Unie
Bevoegde afdeling	Vervoer, Energie, Infrastructuur en Informatiemaatschappij
Goedkeuring door de afdeling	14.4.2021
Goedkeuring door de voltallige vergadering	27.4.2021
Zitting nr.	560
Stemuitslag	
(voor/tegen/onthoudingen)	243/0/5

1. **Conclusies en aanbevelingen**

1.1. Het EESC waardeert de inspanningen van de Commissie om de veerkracht van publieke en particuliere entiteiten tegen bedreigingen als gevolg van cyber- en fysieke aanvallen en incidenten te vergroten, en beaamt dat het bedrijfsleven en de innovatiecapaciteit van de EU op inclusieve wijze moeten worden versterkt, volgens een strategie die op vier pijlers berust: gegevensbescherming, grondrechten, veiligheid en cyberbeveiliging.

1.2. Gezien het belang en de gevoeligheid van de met beide voorstellen nagestreefde doelstellingen zou een verordening echter de voorkeur verdienen boven een richtlijn. Voorts is het onduidelijk waarom de Commissie deze mogelijkheid niet heeft willen overwegen, zelfs niet als een van de opties.

1.3. Het EESC merkt op dat sommige bepalingen van de twee richtlijnvoorstellen elkaar overlappen, in die zin dat ze nauw met elkaar verbonden zijn en elkaar aanvullen, waarbij de ene voornamelijk betrekking heeft op cyberbeveiliging en de andere op fysieke veiligheid. Het vraagt derhalve te onderzoeken of de twee voorstellen niet tot één tekst moeten worden samengevoegd, omwille van de vereenvoudiging en de functionele concentratie.

1.4. Het EESC stemt in met de voorgestelde aanpak om het onderscheid tussen exploitanten van essentiële diensten en digitaledienstverleners in de bestaande NIS-richtlijn op te heffen, maar wijst erop dat, wat het toepassingsgebied betreft, nauwkeuriger en duidelijker moet worden aangegeven welke partijen aan de richtlijn moeten voldoen. Met name de criteria voor het onderscheid tussen "essentiële" en "belangrijke" entiteiten, alsmede de vereisten waaraan moet worden voldaan, moeten nauwkeuriger worden afgebakend om te voorkomen dat uiteenlopende benaderingen op nationaal niveau leiden tot belemmeringen voor de mededinging en het vrije verkeer van goederen en diensten, met het risico dat bedrijven worden benadeeld en de handel in gevaar wordt gebracht.

1.5. Gezien de objectieve complexiteit van het systeem dat in de twee voorstellen wordt uiteengezet, acht het EESC het van belang dat de Commissie het toepassingsgebied van de twee reeksen regels precies afbakent, met name wanneer verschillende bepalingen met elkaar wedijveren om dezelfde zaak of hetzelfde onderwerp regelen.

1.6. Duidelijkheid van de regelgeving is een essentiële doelstelling, net als vermindering van de bureaucratie en de versnippering door vereenvoudiging van de processen, de veiligheidsvoorschriften en de verplichtingen inzake de melding van ongevallen. Met het oog hierop zou het, ten behoeve van de burgers en het bedrijfsleven, bovendien dienstig kunnen zijn de twee richtlijnvoorstellen samen te voegen tot één tekst, waardoor een soms ingewikkelde interpretatie en toepassing worden vermeden.

1.7. Het EESC erkent de sleutelrol, die in de voorgestelde richtlijn wordt benadrukt, van de bestuursorganen van "kritieke" en "belangrijke" entiteiten, waarvan de leden regelmatig specifieke cursussen moeten volgen om voldoende kennis en vaardigheden te verwerven om de verschillende cyberrisico's te kennen en te beheren en de gevolgen ervan te beoordelen. Zo gezien zou het voorstel moeten aangeven wat de minimuminhoud van dergelijke kennis en vaardigheden is, zodat op Europees niveau kan worden bepaald welke opleidingsvaardigheden als adequaat worden beschouwd en kan worden voorkomen dat de inhoud van verschillende opleidingscursussen van land tot land verschilt.

1.8. Het EESC onderschrijft de belangrijke rol van het Enisa in de algemene institutionele en operationele opzet van cyberbeveiliging op Europees niveau. Dit orgaan moet, naast het tweejaarlijkse verslag over de stand van de cyberbeveiliging in de Unie, regelmatig geactualiseerde informatie over incidenten op het gebied van cyberbeveiliging en sectorale waarschuwingen, online publiceren, zodat het een extra, nuttig informatie-instrument wordt waarmee degenen op wie de NIS 2-richtlijn betrekking heeft hun bedrijven beter kunnen beschermen.

1.9. Het EESC stemt in met het voorstel om het Enisa te belasten met het aanleggen van een Europees kwetsbaarheidsregister; de rapportage over kwetsbaarheden en ernstige incidenten zou verplicht moeten zijn in plaats van vrijwillig, zodat het een nuttig instrument wordt voor aanbestedende diensten bij Europese aanbestedingsprocedures, met inbegrip van 5G-producten en -technologieën.

2. **Algemene opmerkingen**

2.1. Op 16 december 2020 werd de nieuwe EU-strategie voor cyberbeveiliging voorgelegd, samen met twee wetgevingsvoorstellen: de herziening van de richtlijn (EU) 2016/1148 inzake netwerk- en informatiesystemen (NIS 2) ([1]) en een nieuwe richtlijn inzake de veerkracht van kritieke entiteiten (Critical Entities Resilience, CER). De strategie, een belangrijk onderdeel van de mededeling "De digitale toekomst van Europa vormgeven" ([2]), het Europees herstelplan en de EU-strategie voor een veilige Unie, beoogt de collectieve veerkracht van Europa tegen cyberdreigingen te versterken en ervoor te zorgen dat alle burgers en bedrijven kunnen profiteren van betrouwbare en veilige digitale diensten en instrumenten.

2.2. De bestaande maatregelen op EU-niveau om kritieke diensten en infrastructuur te beschermen tegen cyber- en fysieke risico's moeten worden geactualiseerd. De risico's op het gebied van cyberbeveiliging blijven evolueren naarmate de digitalisering en interconnectie toenemen. Daarom moet het huidige regelgevingskader worden herzien overeenkomstig de logica van de veiligheidsstrategie van de EU, waarbij de tweedeling tussen online en offline en een aanpak op basis van een rigide compartimentering moeten worden doorbroken.

2.3. De twee richtlijnvoorstellen bestrijken een breed scala van gebieden en hebben betrekking op de huidige en toekomstige risico's, online en offline, van cyber- en criminele aanvallen, natuurrampen en andere ongevallen, waarbij ook lering is getrokken uit de huidige pandemie, die duidelijk heeft gemaakt hoe samenlevingen en economieën die steeds afhankelijker worden van digitale oplossingen, kwetsbaar zijn en blootstaan aan toenemende en snel evoluerende cyberdreigingen, met name voor groepen die dreigen te worden uitgesloten, zoals mensen met een handicap. Dit heeft de EU ertoe gebracht maatregelen voor te stellen om een wereldwijde en open cyberruimte veilig te stellen op basis van solide veiligheidsgaranties, technologische soevereiniteit en leiderschap, door operationele vermogens te ontwikkelen om mogelijke dreigingen te voorkomen, af te schrikken en er eensgezinder op te reageren, met inachtneming van de prerogatieven van de lidstaten op het gebied van nationale veiligheid.

3. **Het voorstel voor herziening van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen**

3.1. De NIS-richtlijn (EU) 2016/1148, het eerste "horizontale" regelgevingsinstrument van de EU inzake cyberbeveiliging, was bedoeld om netwerk- en informatiesystemen in de Unie beter bestand te maken tegen cyberrisico's. Ondanks de goede resultaten heeft de NIS-richtlijn toch een aantal beperkingen aan het licht gebracht: door de digitale transformatie van de samenleving, nog versterkt door de COVID-19-crisis, is de verscheidenheid aan dreigingen toegenomen en zijn onze onderling steeds afhankelijker samenlevingen nog kwetsbaarder geworden voor relevante en onvoorziene risico's. Er zijn

([1]) PB L 194 van 19.7.2016, blz. 1.
([2]) COM(2020) 67 final.

nieuwe uitdagingen ontstaan, die passende en innovatieve oplossingen vergen. Uit de resultaten van de uitgebreide raadpleging van belanghebbenden bleek dat het niveau van cyberbeveiliging in Europese bedrijven ontoereikend is, dat de regels in de verschillende sectoren door de staten niet consequent worden toegepast en dat de belangrijkste dreigingen en uitdagingen niet goed worden begrepen.

3.2. Het voorstel inzake NIS 2 is nauw verbonden met twee andere initiatieven: het voorstel voor een verordening inzake de digitale financiële sector (Digital Operational Resilience Act, DORA) en het voorstel voor een richtlijn inzake kritieke entiteiten (CER), waarmee het toepassingsgebied van Richtlijn 2008/114/EG ([3]) inzake energie en vervoer wordt uitgebreid tot nieuwe sectoren, zoals de gezondheidssector en entiteiten die onderzoek en ontwikkeling verrichten op het gebied van geneesmiddelen. De CER-richtlijn, waarvan het sectorale toepassingsgebied gelijk is aan dat van NIS 2 voor kritieke entiteiten (bijlage 1 van NIS 2), verlegt de aandacht voor de bescherming van materiële activa naar de veerkracht van de entiteiten die deze activa beheren, en verruilt de inventarisatie van Europese kritieke infrastructuren met een grensoverschrijdende dimensie voor de inventarisatie van kritieke infrastructuren op nationaal niveau. NIS 2 hangt voorts samen met andere bestaande regelgevingsinstrumenten en vult deze aan, zoals de Europese code voor elektronische communicatie, de algemene verordening gegevensbescherming en de eIDAS-verordening betreffende elektronische identificatie en vertrouwensdiensten.

3.3. Het voorstel voor de NIS 2-richtlijn strookt met het programma voor gezonde regelgeving (REFIT), beoogt de regelgevingslast voor de bevoegde autoriteiten en de nalevingskosten voor openbare en particuliere entiteiten te verminderen en actualiseert het juridische referentiekader. Voorts scherpt het voorstel de aan ondernemingen gestelde beveiligingseisen aan, pakt het de beveiliging van bevoorradingsketens aan, stroomlijnt het de rapportageverplichtingen, voert het strengere toezichtsmaatregelen in voor nationale autoriteiten en streeft het naar harmonisatie van de sanctieregelingen in de lidstaten.

3.4. Het voorstel voor de NIS 2-richtlijn draagt ook bij tot meer informatie-uitwisseling en samenwerking inzake cybercrisisbeheer op nationaal en Europees niveau. Het onderscheid tussen exploitanten van essentiële diensten en aanbieders van digitale diensten wordt in de NIS-richtlijn opgeheven. Het toepassingsgebied omvat middelgrote tot grote ondernemingen in sectoren die zijn vastgesteld op basis van hun kritieke karakter voor de economie en de samenleving. Deze entiteiten, zowel openbare als particuliere, worden onderverdeeld in "essentiële" en "belangrijke" entiteiten, waarvoor verschillende toezichtsregelingen gelden. Het is echter aan de lidstaten om ook kleinere entiteiten met een hoog risicoprofiel in aanmerking te nemen.

3.5. Er wordt gedacht aan een nieuw netwerk van door artificiële intelligentie (AI) aangestuurde Security Operations Centres in de hele EU, die een volwaardig "cyberbeveiligingsschild" zullen vormen dat tijdig signalen van een cyberaanval kan detecteren om in te grijpen voordat er schade optreedt. De relevantie van AI voor cyberbeveiliging wordt ook benadrukt in het verslag over artificiële intelligentie (AI) van de Amerikaanse National Security Commission (NSCAI) van 1 maart 2021. Bijgevolg zullen de lidstaten en de exploitanten van kritieke infrastructuur rechtstreeks toegang hebben tot inlichtingen over dreigingen, als onderdeel van een Europees veiligheidsnetwerk op het gebied van inlichtingen over dreigingen.

3.6. De Commissie gaat ook in op de veiligheid van toeleveringsketens en de betrekkingen met leveranciers: de lidstaten kunnen in samenwerking met de Commissie en Enisa gecoördineerde risicobeoordelingen van kritieke toeleveringsketens uitvoeren, op basis van de aanpak die is goedgekeurd voor 5G-netwerken in de aanbeveling van 26 maart 2019 ([4]).

3.7. Het voorstel stroomlijnt de veiligheids- en rapportagevoorschriften voor bedrijven en scherpt deze aan door een gemeenschappelijke aanpak van risicobeheer op te leggen, met een minimumlijst van basisveiligheidselementen die moeten worden toegepast. Er zijn preciezere bepalingen over het proces voor de melding van incidenten, de inhoud van de verslagen en de termijnen. In dit verband bevat het voorstel een aanpak in twee fasen: ondernemingen hebben 24 uur de tijd om een eerste, beknopt verslag in te dienen, dat binnen een maand moet worden gevolgd door een gedetailleerd eindverslag.

([3]) PB L 345 van 23.12.2008, blz. 75.
([4]) PB L 88 van 29.3.2019, blz. 42.

3.8. Het is de bedoeling dat de lidstaten nationale autoriteiten aanwijzen die verantwoordelijk zijn voor crisisbeheer, met specifieke plannen en een nieuw netwerk voor operationele samenwerking: het Europees netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe"). De rol van de samenwerkingsgroep in de strategische besluitvorming wordt versterkt en er wordt een door Enisa beheerd register van in de EU vastgestelde kwetsbaarheden opgezet; ook de informatie-uitwisseling en de samenwerking tussen de autoriteiten van de lidstaten, met inbegrip van de operationele samenwerking inzake cybercrisisbeheersing, worden opgevoerd.

3.9. Er worden strengere toezichtsmaatregelen voor nationale autoriteiten en strengere handhavingsvoorschriften ingevoerd, waarbij gestreefd wordt naar harmonisatie van de sanctieregelingen in alle lidstaten.

3.10. In dat verband wordt in de voorgestelde richtlijn een lijst van administratieve sancties vastgesteld voor inbreuken op de verplichtingen inzake risicobeheer op het gebied van cyberbeveiliging en communicatie. Het voorstel bevat bepalingen inzake de aansprakelijkheid van natuurlijke personen die representatieve of leidinggevende functies bekleden in ondernemingen die onder het toepassingsgebied van de richtlijn vallen. In die zin verbetert het voorstel de manier waarop de EU grootschalige incidenten en crises op het gebied van cyberbeveiliging voorkomt, beheert en erop reageert, met duidelijke verantwoordelijkheden, een goede planning en ruimere samenwerking op EU-niveau.

3.11. De lidstaten worden in staat gesteld gezamenlijk toe te zien op de uitvoering van de EU-regels en elkaar bij te staan in geval van grensoverschrijdende problemen, een meer gestructureerde dialoog met de particuliere sector tot stand te brengen, de openbaarmaking te coördineren van kwetsbare punten die in op de interne markt in de handel gebrachte hard- en software zijn vastgesteld, en veiligheidsrisico's en bedreigingen in verband met nieuwe technologieën op gecoördineerde wijze te beoordelen, zoals het geval was voor 5G.

4. **Het voorstel voor een richtlijn betreffende de veerkracht van kritieke entiteiten**

4.1. De EU heeft in 2006 het Europees programma voor de bescherming van kritieke infrastructuur (EPCIP) opgezet en in 2008 de richtlijn betreffende Europese kritieke infrastructuur (ECI) goedgekeurd, die van toepassing is op de energie- en de vervoerssector. Zowel in de door de Europese Commissie aangenomen EU-strategie voor de veiligheidsunie 2020-2025 ([5]) als in de onlangs goedgekeurde agenda voor terrorismebestrijding wordt benadrukt hoe belangrijk het is dat kritieke infrastructuur bestand is tegen fysieke en digitale risico's. Zowel uit de in 2019 uitgevoerde evaluatie van de uitvoering van de ECI-richtlijn als uit de bevindingen van de effectbeoordeling van het onderhavige voorstel is echter gebleken dat de bestaande Europese en nationale maatregelen er onvoldoende voor zorgen dat de exploitanten de huidige risico's het hoofd kunnen bieden. Vandaar de oproepen van de Raad en het Parlement aan de Commissie om haar huidige opvattingen over de bescherming van kritieke infrastructuur te herzien.

4.2. In de door de Commissie op 24 juli 2020 vastgestelde EU-strategie voor de veiligheidsunie wordt erkend dat fysieke en digitale infrastructuren in toenemende mate met elkaar verweven en van elkaar afhankelijk zijn en wordt benadrukt dat de ECI- en de NIS-richtlijn een samenhangender en consistenter aanpak vergen. In die zin breidt het voorstel voor de CER-richtlijn, waarvan het objectieve toepassingsgebied hetzelfde is als dat van NIS 2 inzake essentiële entiteiten, het oorspronkelijke toepassingsgebied van Richtlijn 2008/114/EG, dat beperkt was tot energie en vervoer, uit tot de volgende sectoren: banken, infrastructuur van de financiële markten, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur en openbare ruimte, en voorziet het tevens in duidelijke verantwoordelijkheden, adequate planning en meer samenwerking. Er dient daartoe een referentiekader te komen voor alle risico's en de lidstaten moeten worden gesteund bij hun inspanningen om ervoor te zorgen dat kritieke entiteiten in staat zijn incidenten te voorkomen, te weerstaan en de gevolgen ervan te boven te komen, ongeacht of de risico's het gevolg zijn van natuurrampen, ongevallen, terrorisme, interne dreigingen of noodsituaties op het gebied van de volksgezondheid, zoals momenteel het geval is.

4.3. Elke lidstaat moet een nationale strategie vaststellen om de veerkracht van kritieke entiteiten te waarborgen, regelmatige risicobeoordelingen uit te voeren en op basis daarvan kritieke entiteiten te identificeren. Kritieke entiteiten moeten op hun beurt risicobeoordelingen uitvoeren, passende technische en organisatorische maatregelen nemen om de veerkracht te vergroten en incidenten aan de nationale autoriteiten melden. Entiteiten die diensten verlenen aan of in ten minste een derde van de lidstaten worden onderworpen aan specifiek toezicht, met inbegrip van door de Commissie georganiseerde, op deze entiteiten gerichte specifieke bijstandsmissies.

4.4. De voorgestelde CER-richtlijn voorziet in verschillende vormen van ondersteuning van lidstaten en kritieke entiteiten, een overzicht van risico's op EU-niveau, beste praktijken en methodologieën, alsook opleiding en oefeningen om de veerkracht van kritieke entiteiten te testen. Het systeem voor grensoverschrijdende samenwerking omvat tevens een ad-hocdeskundigengroep, een groep voor de veerkracht van kritieke entiteiten, een forum voor strategische samenwerking en uitwisseling van informatie tussen de lidstaten.

([5]) COM(2020) 605 final.

5. **Voorstellen om het wetgevingsvoorstel in kwestie te wijzigen**

5.1. Het EESC waardeert de inspanningen van de Commissie om de veerkracht van publieke en particuliere entiteiten tegen bedreigingen als gevolg van cyber- en fysieke aanvallen te vergroten. Dit is van bijzondere betekenis en belang, vooral in het licht van de snelle digitale transformatie ten gevolge van de uitbraak van COVID-19. Het EESC onderschrijft voorts dat Europa de vruchten moet plukken van het digitale tijdperk en zijn industrie, met bijzondere aandacht voor de kleine en middelgrote ondernemingen, en het innovatievermogen daarvan op inclusieve wijze moet versterken, zoals uiteengezet is in de mededeling "De digitale toekomst van Europa vormgeven", en volgens een strategie op basis van vier pijlers: gegevensbescherming, grondrechten, veiligheid en cyberveiligheid, als essentiële voorwaarden voor een samenleving die gebaseerd is op de kracht van gegevens.

5.2. In het licht van de resultaten van de effectbeoordeling en de raadpleging die aan het voorstel voor NIS 2 zijn voorafgegaan, en gezien de vaak beklemtoonde doelstelling om versnippering van de op nationaal niveau vastgestelde regels te voorkomen, zoals ook wordt gesteld in de mededeling van 4 oktober 2017 over de tenuitvoerlegging van de NIS-richtlijn ([6]), merkt het EESC echter op dat niet duidelijk is waarom de Commissie niet heeft overwogen om de vaststelling van een verordening in plaats van een richtlijn voor te stellen, zelfs niet als een van de opties.

5.3. Het EESC merkt op dat sommige bepalingen van de twee richtlijnvoorstellen elkaar overlappen, in die zin dat ze nauw met elkaar verbonden zijn en elkaar aanvullen, waarbij de ene voornamelijk betrekking heeft op cyberbeveiliging en de andere op fysieke veiligheid. Verder zij opgemerkt dat de kritieke entiteiten waarnaar in de CER-richtlijn wordt verwezen dezelfde sectoren bestrijken en samenvallen met de in de in NIS 2 vermelde "essentiële" entiteiten ([7]). Daarnaast vallen alle kritieke entiteiten waarnaar in de CER-richtlijn wordt verwezen onder de cyberbeveiligingsvoorschriften van NIS 2. De twee voorstellen bevatten ook een aantal overbruggingsclausules om de onderlinge koppeling te waarborgen: bepalingen inzake ruimere samenwerking tussen autoriteiten, uitwisseling van informatie over toezichtactiviteiten, kennisgeving aan NIS 2-autoriteiten over in kaart gebrachte kritieke entiteiten in het kader van de CER-richtlijn, alsook regelmatige vergaderingen van de respectieve samenwerkingsgroepen, ten minste eenmaal per jaar. De twee voorstellen hebben ook dezelfde rechtsgrondslag, namelijk artikel 114 VWEU, gericht op de werking van de interne markt door onderlinge aanpassing van de nationale regels, zoals door het Hof van Justitie van de EU onder meer uitgelegd in zijn arrest in zaak C-58/08, Vodafone en andere. De vraagt is derhalve of de twee voorstellen niet tot één tekst moeten worden samengevoegd, omwille van de vereenvoudiging en de functionele concentratie.

5.4. Het EESC stemt in met de voorgestelde aanpak om het onderscheid tussen exploitanten van essentiële diensten en digitaledienstverleners in de bestaande NIS-richtlijn op te heffen, maar wijst erop dat, wat het toepassingsgebied betreft, nauwkeuriger en duidelijker moet worden aangegeven welke partijen aan de richtlijn moeten voldoen. Naast de verwijzingen in de bijlagen I en II wordt in NIS 2 namelijk verwezen naar een reeks onderling verschillende criteria, waaronder gevoelige kwalitatieve en kwantitatieve beoordelingen die op nationaal niveau verschillend kunnen worden toegepast, met het risico dat opnieuw de versnipperde situatie ontstaat die men met de onderhavige wetgevingsmaatregel had willen vermijden. Het is belangrijk te voorkomen dat niet op elkaar aansluitende benaderingen op nationaal niveau leiden tot belemmeringen voor de mededinging en het vrije verkeer van goederen en diensten, met het risico dat bedrijven worden benadeeld en de handel ongunstig wordt beïnvloed.

5.5. NIS 2 bepaalt dat kritieke exploitanten in de sectoren die door dit voorstel als "essentieel" worden beschouwd, ook onderworpen zijn aan algemene verplichtingen inzake het opbouwen van veerkracht, met de nadruk op niet-cyberrisico's in het kader van de CER-richtlijn. Laatstgenoemde stelt echter uitdrukkelijk dat zij niet van toepassing is op aangelegenheden die onder NIS 2 vallen. In de CER-richtlijn staat namelijk dat cyberbeveiliging voldoende aan bod komt in de NIS 2-richtlijn en dat de aangelegenheden die onder deze richtlijn vallen, van het toepassingsgebied van de richtlijn moeten worden uitgesloten, behoudens de speciale regeling voor entiteiten in de sector van de digitale infrastructuur. De CER-richtlijn stelt voorts dat entiteiten in de digitale-infrastructuursector hoofdzakelijk gebruikmaken van netwerk- en informatiesystemen en onder het toepassingsgebied van de NIS 2-richtlijn vallen, die ook betrekking heeft op de fysieke beveiliging van dergelijke systemen als onderdeel van hun verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging. Tegelijkertijd vermeldt de CER-richtlijn dat het niet uitgesloten is dat specifieke bepalingen ervan op hen van toepassing zijn.

5.6. In deze complexe context is het volgens het EESC dan ook geboden dat de Commissie het toepassingsgebied van de twee reeksen regels nauwkeurig omschrijft, met name wanneer zij betrekking hebben op dezelfde situatie of dezelfde entiteit.

5.7. De duidelijkheid van elke regelgevende bepaling, vooral in teksten die zo omvangrijk en complex zijn als de onderhavige, moet op elk niveau een onwrikbare doelstelling zijn, samen met het streven om de bureaucratie en de versnippering tegen te gaan door de processen, de veiligheidsvoorschriften en de verplichtingen inzake de kennisgeving van ongevallen te vereenvoudigen. Ook moet ervoor worden gezorgd dat het groeiend aantal instanties die verantwoordelijk

([6]) COM(2017) 476 final.
([7]) Bijlage 1 (PB L 194 van 19.7.2016, blz 1).

zijn voor specifieke taken de duidelijke afbakening van hun bevoegdheden niet in het gedrang brengt, waardoor de nagestreefde doelstellingen zouden worden ondermijnd. Met het oog hierop zou het, ten behoeve van de burgers en het bedrijfsleven, ook dienstig kunnen zijn de twee richtlijnvoorstellen samen te voegen tot één tekst, waardoor een soms ingewikkelde interpretatie en toepassing worden vermeden.

5.8. Op diverse plaatsen wordt in NIS 2 verwezen naar bepalingen van andere rechtsinstrumenten, zoals naar Richtlijn (EU) 2018/1972 ([8]) tot vaststelling van het Europees wetboek voor elektronische communicatie, waarvan de toepassing gebaseerd is op het specialiteitsbeginsel. Sommige bepalingen van die richtlijn worden uitdrukkelijk ingetrokken (artikelen 40 en 41), terwijl andere volgens bovenbedoeld beginsel moeten worden toegepast, zonder dat dienaangaande enige verduidelijking wordt verstrekt. In dit verband hoopt het EESC dat alle twijfels omtrent de interpretatie worden weggenomen om interpretatieproblemen te voorkomen. Wat de sanctieregeling betreft, onderschrijft het EESC het streven van de Commissie naar harmonisatie van de regeling in geval van niet-naleving van het risicobeheer, in het kader van een betere informatie-uitwisseling en samenwerking op EU-niveau.

5.9. Het EESC erkent de sleutelrol van de bestuursorganen van "essentiële" en "belangrijke" entiteiten in de cyberbeveiligingsstrategie en het risicobeheer, zoals benadrukt in de voorgestelde richtlijn, aangezien zij verplicht zijn risicobeheersmaatregelen goed te keuren, toe te zien op de uitvoering ervan en dienen te reageren in geval van niet-naleving. In dit verband wordt van de leden van deze organen verwacht dat zij regelmatig specifieke cursussen volgen om voldoende kennis en vaardigheden te verwerven om de verschillende cyberrisico's te kennen en te beheren en de gevolgen ervan te beoordelen. Toch zou het voorstel moeten aangeven wat de inhoud van dergelijke kennis en vaardigheden is, zodat op Europees niveau kan worden bepaald welke opleidingsvaardigheden als adequaat worden beschouwd om te voldoen aan de vereisten in het voorstel, en kan worden voorkomen dat de vereisten en de inhoud van opleidingscursussen van land tot land verschillen.

5.10. Het EESC onderschrijft de belangrijke rol van het Enisa in de algemene institutionele en operationele opzet van cyberbeveiliging op Europees niveau. Dit orgaan moet, naast het verslag over de stand van de cyberbeveiliging in de Unie, geactualiseerde informatie over incidenten op het gebied van cyberbeveiliging en sectorale waarschuwingen, online publiceren, zodat het een nuttig informatie-instrument wordt waarmee degenen op wie de NIS 2-richtlijn betrekking heeft hun bedrijven beter kunnen beschermen.

5.11. Het EESC beaamt dat toegang tot correcte en tijdige informatie over kwetsbare punten van ICT-producten en -diensten bijdraagt aan een verbeterd risicobeheer inzake cyberbeveiliging. In dat opzicht vormen bronnen van openbaar beschikbare informatie over kwetsbaarheden een belangrijk instrument voor de nationale bevoegde autoriteiten, CSIRT's, ondernemingen en gebruikers. Daarom stemt het EESC in met het voorstel om het Enisa te belasten met het aanleggen van een Europees kwetsbaarheidsregister, waaraan essentiële en belangrijke entiteiten en hun leveranciers informatie kunnen verstrekken, zodat gebruikers passende mitigatiemaatregelen kunnen nemen. Voorts zou de rapportage over kwetsbaarheden en ernstige incidenten verplicht moeten zijn in plaats van vrijwillig, zodat het ook een nuttig instrument wordt voor aanbestedende diensten bij Europese aanbestedingsprocedures, met inbegrip van 5G-producten en -technologieën. Dit register zou dan bruikbare elementen bevatten voor de beoordeling van de inschrijvingen, teneinde de kwaliteit ervan en de betrouwbaarheid van Europese en niet-Europese contractanten na te gaan vanuit het oogpunt van veiligheid van de producten en diensten waarop wordt ingeschreven, overeenkomstig de aanbeveling inzake cyberbeveiliging van 5G-netwerken van 26 maart 2019. Het register moet ook garanderen dat de daarin opgenomen informatie op zodanige wijze beschikbaar wordt gesteld dat elke vorm van discriminatie wordt voorkomen.

Brussel, 27 april 2021.

De voorzitter
van het Europees Economisch en Sociaal Comité
Christa SCHWENG

([8]) PB L 321 van 17.12.2018, blz. 36.