Internetconsultatie ProRail B.V. op wetsvoorstel en memorie van toelichting Wet weerbaarheid kritieke entiteiten

Algemeen	ProRail constateert dat de wettekst nauwelijks echt concreet is voor kritieke entiteiten en dat het vooral de rol van de overheid beschrijft. Hoe kritieke entiteiten concreet invulling aan de wet moeten gaan geven, moet uit de lagere regelgeving, de te ontwikkelen richtsnoeren en methodologieën volgen. Maar die zijn er (nog) niet, niet duidelijk is wat er moet komen en wanneer die er zullen komen. Zonder die nadere regelgeving, richtsnoeren e.d. is niet duidelijk wanneer invulling aan de wet wordt gegegeven.

Wetsvoorstel

Artikel	Bladzijde	Commentaar
-		ProRail vraagt zich af waarom artikel 14 (Antecedentenonderzoek) uit de CER richtlijn niet in de wettekst is overgenomen.
-		ProRail vraagt zich af waarom artikel 16 (normen) uit de CER richtlijn niet in de wettekst is overgenomen.
1	1	Het is ProRail niet duidelijk waarom voor de definitie van een aantal begrippen die in de wettekst gebruikt worden enkel wordt verwezen naar artikel 2 van de CER richtlijn, waarom worden die begrippen (zoals essentiële dienst, kritieke infrastructuur, incident, overheidsinstantie, risico, risicobeoordeling, weerbaarheid) in het wetsvoortsel niet nader gedefinieerd?
4	2	Titel van het artikel is aangevuld met '(netwerk- en informatiesystemen en de fysieke componenten en omgevingen daarvan). Gesteld wordt:“Deze wet is niet van toepassing op aangelegenheden waarop de Cyberbeveiligingswet van toepassing is, onverminderd artikel 8 van de CER-richtlijn”. Zonder de Cyberbeveiligingswet te kennen (en te kunnen doorgronden) is het niet duidelijk wat er nu wel en niet onder deze wet valt. Welke delen van de “netwerk- en informatiesystemen en de fysieke componenten en omgevingen daarvan” vallen wel onder Wet weerbaarheid kritieke entiteiten en welke vallen er niet onder maar juist onder de Cyberbeveiligingswet? De Wwke en Cbw komen op een aantal punten niet exact met elkaar overeen.
7 lid 3 sub d	2	Tekstueel: "op (i.p.v. "van") haar verlening van andere essentiële diensten in de sectoren"

7	2 en 3	Wat wordt bedoeld met “2°. van haar verlening van andere essentiële diensten in de sectoren, genoemd in de bijlage van deze wet, of indien van toepassing, de sectoren, bedoeld in artikel 7a, eerste lid, die afhankelijk zijn van die diensten.”? Artikel 7 lid 4 en lid 7 zijn volgens ProRail niet SMART geformuleerd en niet verder duidelijk uitgewerkt. Wat zijn bijvoorbeeld de drempelwaarden? Welke criteria zijn er vastgesteld? Conform CER richtlijn: “Er moeten criteria worden vastgesteld aan de hand waarvan kan worden bepaald hoe ernstig het verstorend effect van een incident is. Die criteria moeten voortbouwen op de criteria van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad (6) teneinde zowel de inspanningen van de lidstaten om exploitanten van essentiële diensten als gedefinieerd in die richtlijn en de daarmee opgedane ervaring te benutten.”
7a	3	Het is ProRail niet duidelijk waarom hier wordt afgeweken van de volgorde van de criteia in artikel 7 lid 4? Bovendien zijn de criteria niet verder uitgewerkt.
8 lid 3 sub a	4	Is de rol van de bevoegde autoriteit als 'bestuursrechtelijke handhaver' verenigbaar met de ondersteunende, hulp biedende, adviserende rol die zij ook heeft? In hoeverre is er dan sprake van onafhankelijkheid?
8 lid 3 sub b	4	In lid 3 sub b wordt gesproken over: “b. de in de artikelen 7, 9 tot en met 11, 20, 25,28 tot en met 30, en 30b genoemde taken.” Dergelijke verwijzingen worden vaker in de wettekst gebruikt maar dat komt de leesbaarheid, het begrip en de duidelijkheid over het algemeen niet ten goede.
9 lid 1	4	De bevoegde autoriteit voert een risicobeoordeling uit. De Kritieke Entiteit (KE) baseert hierop diens risicobeoordeling. De kwaliteit van de tweede is afhankelijk van die van de bovenliggende. De toezichthouder houdt toezicht op de kwaliteit van de risicobeoordeling van de KE. Houdt de toezichthouder dan ook toezicht op de kwaliteit van de bovenliggende beoordeling van de bevoegde autoriteit ?
9 lid 1	4	Er gaan, naar ProRail begrijpt, binnen Nederland voor de verschillende sectoren verschillende bevoegde autoriteiten en ca 7 toezichthouders komen. De vitale sectoren kennen hun eigen dynamiek, maar in de supplychain leveren vele grote bedrijven missie-kritieke producten. De eisen die deze via hun "vitale klant" doorkrijgen dienen zoveel mogelijk uniform te zijn zodat dit voor hun werkbaar blijft. Hoe wordt dit over de verschillende bevoegde autoriteiten en toezichthouders heen geborgd ?
9 lid 1	4	Een belangrijk aspect van de risicobeoordeling is het geheel aan cascade-effecten dat zou kunnen ontstaan. Vaak zijn deze intersectoraal. Bijvoorbeeld: power black-out => uitval treindienst => uitval bevoorading etc. Deze cascade-effecten kunnen niet per sector in beeld gebracht worden, dat dient in de bovenliggende analyse te gebeuren.
9 lid 1	4	De bevoegde autoriteit gaat voor ProRail een risicobeoordeling uitvoeren? Hoe pakken ze dat aan? Hoe wordt geborgd dat de juiste expertise wordt aangehaakt voor de spoorsector?

9	4 en 5	Uit de genoemde risico's blijkt nauwelijks dat het ook om fysieke beveiligingsrisico's gaat. Hieruit blijkt ook niet direct/duidelijk de scope (in relatie tot de Cyberbeveiligingswet en artikel 4 van de wet). De demarcatie tussen Wet weerbaarheid kritieke entiteiten en Cyberbeveiligingswet is in de wettekst voor Wet weerbaarheid kritieke entiteiten niet duidelijk (zie opmerking bij artikel 4). Richt de Cyberbeveiligingswet zich alleen op cyber (dus internet) gerelateerde risico's of de informatiebeveiligingsrisico's in bredere zin of vallen die laatste dan juist weer onder de Wet weerbaarheid kritieke entiteiten? Zonder de wettekst Cyberbeveiligingswet volledig te kennen is dit niet duidelijk. De scope van de wet is, net als bij de originele Europese CER-tekst, niet expliciet duidelijk. Wat valt er nu wel precies onder (de fysieke assets? Of de kritieke processen? Of de kritieke entiteit als geheel?) ? En er wordt aangegeven dat naar "alle relevante door de natuur en door de mens veroorzaakte" risico's gekeken moet worden zonder goed wordt afgebakend wat dan de scope is en welke risico's dat dan betreft. Het is niet eenvoudig voor een kritieke entiteit om te bepalen of ze het nu goed hebben gedaan of niet. Fysieke beveiligingsrisico's staan er niet expliciet in en zouden dan moeten worden afgeleid uit 'de hybride dreigingen en/of de antagonistische dreigingen'(?) Maar die begrippen worden niet gedefinieerd en er zijn geen algemeen erkende definities voor en dat maakt ze multi-interpretabel.
9 en 14	4, 5 en 6	Is het niet veel efficiënter en effectiever dat de bevoegde autoriteit en de kritieke entiteit gezamenlijk een risicobeoordeling uitvoeren etc.?
10 lid 2	5	Valt onder de ondersteuning van de Kritieke Entiteiten mogelijk ook het bijdragen in de kosten ? Volgens ProRail laat de CER-richtlijn die mogelijkheid wel toe. Dit volgt uit artikel 10 lid 1, laatste zin van de CER-richtlijn.
10 lid 2 sub e	5	"e. het geven van opleidingen aan het personeel van kritieke entiteiten." Wie gaat de bevoegde autoriteit daarvoor inschakelen? Gaat zij ook gebruik maken van de bestaande opleidingen en opleidingencentra voor de spoorsector?
10 lid 3	5	Bestaat er al een beeld van de regels die in dit geval bij AMvB zullen worden gesteld?
12 sub b	5	De Groep voor weerbaarheid van kritieke entiteiten wordt hier 1x genoemd. In de CER-richtlijn is hier een uitgebreid artikel aan gewijd (artikel 19). Deze Groep ondersteunt de Commissie en faciliteert de samenwerking tussen de lidstaten en de uitwisseling van informatie over aangelegenheden in verband met de CER-richtlijn. Moet hier in de Wwke niet ook een artikel aan gewijd worden?
12 sub c	5	Betekent dit ook dat het centrale contactpunt er zorg voor draagt dat kritieke entiteiten die in verschillende landen opereren moeten voldoen aan één set eisen, en niet een per land ? Bijvoorbeeld spoorvervoerders die internationaal opereren.

13	5	Lid 1: waarom wordt hier verwezen naar de CER richtlijn en worden niet de genoemde elementen opgenomen? lid 2: “2. Onze Minister stelt in overeenstemming met Onze Ministers die het aangaat de eerste strategie uiterlijk op 17 januari 2026 vast en actualiseert de strategie vervolgens ten minste om de vier jaar.” Ontbreekt hier niet de toevoeging: “of eerder indien hiertoe aanleiding bestaat”? Dit wordt bij andere artikelen wel expliciet vermeld. Lid 3: “3. Onze Minister consulteert in overeenstemming met Onze Ministers die het aangaat eerst de relevante betrokken partijen voordat hij de strategie vaststelt of actualiseert.” Het is ProRail niet duidelijk wat hier bedoeld wordt met 'relevante betrokken partijen' en welke partijen dit dan zijn.
14	6	“De kritieke entiteit beoordeelt in dat kader alle relevante door de natuur en door de mens veroorzaakte risico’s”. Het zou duidelijker zijn als er (bijvoorbeeld) staat dat het ook om risico’s t.a.v. fysieke objecten (assets) gaat. De scope van de wet is echter niet duidelijk afgebakend (zie ook eerdere opmerkingen bij de artiekelen 9 en 14).
14	6	De wettekst zegt ten behoeve van de kritieke entiteiten (bijvoorbeeld) iets over de risicobeoordeling door de kritieke entiteit (artikel 14) in lijn met de CER-artikelen maar geeft daarin het minimum aan (geen “volledig” overzicht, voor zover dat te maken is) en de scope is ook niet heel concreet gedefinieerd: “alle relevante door de natuur en door de mens veroorzaakte risico’s die de verlening van haar essentiële dienst of diensten kunnen verstoren”. Wat zijn “alle” risico’s? Volstaat één beoordeling voor de kritieke entiteit als geheel? Moet het per dienst, per bedrijfsonderdeel, per proces, per locatie, etc. (in relatie tot wat onduidelijk in artikel 4 staat)? Wat is de scope en wanneer is de risicobeorodeling voldoende?
14 lid 1	6	Voor het uitvoeren van risicobeoordelingen en kwetsbaarheidsanalyses zijn bestaande methodieken en standaarden voorhanden. Zo is bijvoorbeeld het opstellen van een Business Impact Analyse (BIA) uitgewerkt in ISO 22301, ISO 22313 en onderligende normen voor Business Continuity Management. Voorstel ProRail: maak in deze wettekst en zeker de uitwerking in de amvb zoveel mogelijk gebruik van deze bestaande standaarden. Dit geeft vele voordelen, zoals dat een deel van de KE's hier al mee werkt zodat er werk met werk gemaakt kan worden; audits worden ook eenvoudiger en minder kostbaar omdat ook gecertificeerde auditeurs gewend zijn met deze normen te werken. Zie verder ook het aanbod van de NEN om dit verder te ondersteunen.
14 lid 1 sub e	6	In artikel 14 eerste lid sub e van het wetsvoortsel zijn de begrippen “hybride dreigingen en andere antagonistische dreigingen” multi-interpretabel (geen duidelijke definitie van) en maken niet direct duidelijk wat er precies onder verstaan wordt. Uit de opsomming in dit artikel volgt niet expliciet of direct dat ook de fysieke beveiligingsrisico’s ertoe gerekend worden.

15 lid 1 en 17 lid 1	6 en 7	"Artikel 14 is niet van toepassing op kritieke entiteiten in de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur" "Artikel 16 is niet van toepassing op kritieke entiteiten in de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur, genoemd in de bijlage van deze wet." Waarom niet terwijl zij toch juist ook kritieke digitale infrastructuren beheren?
16	6	Op basis van artikel 16 van het wetsvoorstel dient de kritieke entiteit passende en evenredige technische, beveiligings-, en organisatorische maatregelen te nemen om voor haar weerbaarheid te zorgen maar een verdieping daarvan ontbreekt. In CER-artikel 13 is dit verder uitgewerkt maar in het wetsvoorstel komt die nadere invulling niet terug.
16 lid 1	6	Wat verstaan wordt onder "passend en evenredig" dient verder uitgewerkt te worden. Waarschijnlijk is de amvb daarvoor de beste plaats. Wat "passend" is hangt ook af van de drempelwaarden die worden gehanteerd voor wanneer een risico qua impact onacceptabel is. Of een maatregel "evenredig" is hangt ook af van de wijze waarop de financiering daarvan kan plaats vinden. Een deel van de KE's is voor haar financiering geheel of deels afhankelijk van een van de ministeries. Indien een maatregel evenredig lijkt maar het financierende ministerie stelt daarvoor niet de benodigde financien beschikbaar, is dat dan ook onderwerp van beoordeling door de toezichtjhouder? En kan deze hierin in de richting van de financier (ministerie) handhavend optreden?
16 lid 1	6	Lid 1 :“1. De kritieke entiteit neemt passende en evenredige technische, beveiligings-, en organisatorische maatregelen om voor haar weerbaarheid te zorgen. Dit doet zij op basis van de door de bevoegde autoriteit verstrekte relevante informatie over de risicobeoordeling, bedoeld in artikel 9, en op basis van de resultaten van de risicobeoordeling van de kritieke entiteit, bedoeld in artikel 14.” Maar de maatregelen als genoemd in artikel 13 CER richtlijn: Weerbaarheidsmaatregelen van kritieke entiteiten' ontbreken in de wettekst. Naar de mening van ProRail zouden die maatregelen in de wettekst moeten worden overgenomen.
16 lid 3	6	Lid 3: “3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren en subsectoren en type entiteiten.” Het is ProRail niet duidelijk welke regels met betrekking tot de maatregelen zullen worden gesteld, waaraan moet ProRail dan denken?

17	7	Dit artikel gaat weliswaar over bepaalde met name financiële sectoren maar in lid 3 wordt gesproken over een vrijstelling voor sectorspecifieke rechtshandelingen van de EU. Wordt hier ingeval van ProRail ook gedoeld op bijvoorbeeld de Spoorwegveiligheidsrichtlijn en de maatregelen die onder meer in geval van een veiligheidsincident dienen te worden getroffen? In dat geval zou artikel 16 (zorgplicht) namelijk niet van toepassing zijn. Met andere woorden: gaat bijvoorbeeld de Spoorwegveiligheidsrichtlijn voor op (boven) de CER richtlijn en dit wetsvoorstel?
17	7	Op basis van artikel 1 lid 3 van de CER richtlijn kan het toepassingsgebied worden beperkt in geval van sectorspecifieke rechtshandelingen van de EU wanneer de voorschriften daarin tenminste gelijkwaardig worden geacht aan de in de CER richtlijn genoemde verplichtingen. Wie bepaalt die gelijkwaardigheid en wat betekent betekent dat met betrekking tot bijvoorbeeld de Spoorwegveiligheidsrichtijn, de TSI's en andere spoorse richtlijnen en verordeningen en wat betekent dat dan specifiek voor ProRail in relatie tot het wetsvoorstel?
18	7	Lid 5: Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over de wijze waarop een melding als bedoeld in het eerste lid wordt gedaan, aanvullende aspecten en drempelwaarden die in aanmerking worden genomen om te bepalen of een verstoring aanzienlijk is, en de gegevens die ter uitvoering van het derde lid worden verstrekt.” Wat zijn aanvullende aspecten, drempelwaarden die in aanmerking moeten worden genomen? Waar moet ProRail dan aan denken?
18 lid 1	7	De drempelwaarden voor de meldplicht dienen geconcretiseerd te worden. Daarbij dient het doel van deze meldplicht uitgelegd te worden. Is dat: de KE helpen met het oplossen van de calamiteit ? Of is dat, bijvoorbeeld bij een bewuste sabotage, het waarschuwen van andere KE's zodat zij extra alert kunnen zijn voor het geval ook zij doelwit worden?
18-21 en 32	7, 8 en 11	Begrijpt ProRail het goed dat ook haar meldingen, verslagen, rapporten etc. met bedrijfsvertrouwelijke informatie, buiten de reikwijdte van de Wet Open Overheid (WOO) vallen?
20 lid 2	8	De bevoegde autoriteit waarschuwt zo nodig het publiek. Het kan zeker zo belangrijk zijn dat niet het algemene publiek, maar gericht bepaalde sectoren of organisaties gewaarschuwd worden op basis van vooraf uitgewerkte criteria. Is dat ook een taak van de bevoegde autoriteit?
20 lid 2	8	ProRail gaat ervanuit dat het hier een verplichte en geen facultatieve raadpleging betreft.
hoofdstuk 13 (art. 27a e.v.)	9 en verder	ProRail stelt voor om (zie artikel 18) 'benodigde' persoonsgegevens te vervangen in 'noodzakelijke' persoonsgegevens. De AVG ken namelijk proportionaliteit en subsidiariteit. Onder informatie vallen eveneens persoonsgegevens. Wellicht kan dit begrip worden gedefinieerd.
hoofdstuk 13 (art. 27a e.v.)	9 en verder	ProRail neemt aan dat wanneer op grond van de AVG aanvullende eisen worden gesteld, deze worden meegenomen. Hierbij kun je denken aan de dpia of artikel 26 AVG e.d..
35 lid 1	11	Welke eisen worden aan de onafhankelijke en gekwalificeerde deskundige gesteld?

Memorie van toelichting		
Paragraaf	**Bladzijde**	**Commentaar**
2.2 onder j	5	Niet wordt aangeven dat ook financiële steun mogelijk is. De CER laat dat open.
5.4	13-14	Zoals aangegeven in het commentaar op het wetsvoorstel zelf is het advies om zoveel mogelijk gebruik te maken van bestaande standaarden zoals de normen ISO 22301 en 22313 voor Business Continuity Management en ISO 22361 voor crisismanagement. Het Normalisatie instituut Nederland (NEN) heeft aangeboden om hierin te adviseren.
5.5.2	15	De alinea over evenredigheid is vaag en niet concreet. Hier worden alleen enkele relevante principes weergegeven. Uiteindelijk moeten de spelregels en criteria voldoende concreet worden, onder meer met betrekking tot de financiële capaciteit, zodat de Kritieke Entiteiten weten waar ze aan toe zijn en de toezichthouder waartegen ze dienen te beoordelen. ProRail neemt aan dat ook de evenredigheid in de lagere regelgeving wordt uitgewerkt.
5.5.2	15	De tekst in de 2e aline komt in feite neer op het internationaal gebruikelijke criterium "ALARP" (As Low As Reanosable Practicable). ProRail adviseert om bij de internationaal gebruikelijke terminologie aan te sluiten.
5.5.3	16	De Europese Commissie zal, na raadpleging van de CERG, als bedoeld in artikel 19 van de CER-richtlijn, niet-bindende richtsnoeren vaststellen die kunnen helpen bij het nader bepalen van geschikte technische en organisatorische veiligheids- en beveiligingsmaatregelen.'. Er is sprake van niet bindende richtsnoeren voor te treffen maatregelen maar op toepassing/uitvoering van de maatregelen kan wel handhavend worden opgetreden, is dat niet tegenstrijdig? Zeker nu niet concreet gemaakt wordt waaraan voldaan moet worden.
5.5.3 onder v.	16	Welke maatregelen kan een kritieke entiteit ten aanzien van het personeel van externe dienstverleners die kritieke functies vervullen, treffen? Kunnen hier voorbeelden van gegeven worden?
5.6	17-18	Zoals is opgemerkt bij de wettekst verdient het volgens ProRail aanbeveling om rondom de meldplicht aan te geven welke doelen bereikt dienen te worden met de meldplicht. Is het doel alleen om de geraakte kritieke entiteit te helpen? Of ook om andere kritieke entiteiten te waarschuwen dat er sprake is van een actuele bijzondere dreiging zodat zij zo nodig qua defensieve maatregelen kunnen opschalen?

5.10	20	Blijkbaar behoeft het een en ander wat geregeld is over de adviesmissie in hoofdstuk 4 van de CER-richtlijn geen implementatie in de Wwke. In de CER-richtlijn wordt hier, zie vooral artikel 18, best uitgebreid op ingegaan. Zo'n adviesmissie brengt echter verplichtingen met zich mee voor kritieke entiteiten van Europees belang en soms ook voor ‘normale’ kritieke entiteiten. Is het dan niet belangrijk hier iets over op te nemen in de Wwke?