

VOORONTWERP VAN WET

Voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten

HOOFDSTUK 1 – Algemene bepalingen

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2. Deze wet voorziet in de omzetting van de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG van de Raad.

HOOFDSTUK 2 – Definities

Art. 3. Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° "OCAD": Coördinatieorgaan voor de dreigingsanalyse ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging;

2° "sectorale overheid": de bevoegde autoriteit, aangewezen in bijlage of door de Koning, bij besluit vastgesteld na overleg in de Ministerraad, voor de in Bijlage vermelde sectoren en deelsectoren;

3° "kritieke entiteit": een publieke of particuliere entiteit die behoort tot het toepassingsgebied uit bijlage I, en die overeenkomstig Hoofdstuk 4, Afdeling 1, is geïdentificeerd als behorende tot een van de categorieën die zijn vermeld in de Bijlage;

4° "weerbaarheid": het vermogen van een kritieke entiteit om een incident te voorkomen, zich ertegen te beschermen, erop te reageren, er weerstand aan te bieden, en het mitigeren, absorberen, verwerken en herstellen van een incident;

5° "incident": elke gebeurtenis die het verlenen van een essentiële dienst aanzienlijk kan verstoren of verstoort, ook wanneer de gebeurtenis gevolgen heeft voor de nationale systemen die de rechtsstaat waarborgen;

6° "kritieke infrastructuur": een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, of een onderdeel van een voorziening, een faciliteit, apparatuur, een netwerk of een systeem, hetgeen noodzakelijk is voor de verlening van een essentiële dienst;

7° "essentiële dienst": een dienst die van cruciaal belang is voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu;

AVANT-PROJET DE LOI

Avant-projet de loi concernant la résilience des entités critiques

CHAPITRE 1^{er} – Dispositions générales

Article 1^{er}. La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2. Cette loi transpose la Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques et abrogeant la Directive 2008/114/CE du Conseil.

CHAPITRE 2 – Définitions

Art. 3. Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par:

1° "OCAM" : Organe de coordination pour l'analyse de la menace institué par la loi du 10 juillet 2006 relative à l'analyse de la menace;

2° "autorité sectorielle" : l'autorité compétente désignée à l'annexe de la présente loi ou par le Roi, par arrêté pris après avis du Conseil des Ministres, pour les secteurs et sous-secteurs désignés dans la même Annexe;

3° "entité critique" : une entité publique ou privée identifiée comme telle conformément au Chapitre 4, Section 1^{ère}, appartenant à l'une des catégories énumérées en Annexe;

4° "résilience" : la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir;

5° "incident" : un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit;

6° "infrastructure critique" : un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel;

7° "service essentiel" : un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement;

8° "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, dat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of een dergelijke verstoring en de waarschijnlijkheid dat het incident zich voordoet;

9° "risicobeoordeling": het gehele proces ter bepaling van de aard en omvang van een risico door potentiële relevante dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden, in kaart te brengen en te analyseren, en door het verlies of de verstoring van een essentiële dienst die dat incident zou kunnen veroorzaken in te schatten;

10° "SICAD": Communicatie- en informatiedienst van het arrondissement, zoals bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

11° "overheidsinstantie": een administratieve overheid als bedoeld in artikel 14, §1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

- 1° zij hangt af van de Federale Staat;
- 2° zij is niet van industriële of commerciële aard;
- 3° zij oefent niet hoofdzakelijk een activiteit uit die tot een van de andere sectoren of deelsectoren uit de bijlage behoren;
- 4° zij is geen privaatrechtelijke rechtspersoon.

12° "NIS 2-wet": de wet van [xx xxxx xxxx] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

HOOFDSTUK 3 – Toepassingsgebied

Art. 4. §1. Deze wet is van toepassing op de sectoren en deelsectoren zoals vermeld in Bijlage.

Deze wet is echter niet van toepassing op de nucleaire installaties bedoeld bij de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

Art. 5. §1. De bepalingen van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en Hoofdstuk 7 van deze wet zijn niet van toepassing op de als kritiek geïdentificeerde entiteiten in de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuur, tenzij de Koning anders bepaalt om tot een hoger weerbaarheidsniveau van die kritieke entiteiten te komen.

§2. Wanneer specifieke wetgeving voor sectoren of deelsectoren vereist dat kritieke entiteiten maatregelen dienen te nemen om hun weerbaarheid te vergroten, kan de Koning bepalen dat deze maatregelen als gelijkwaardig worden beschouwd aan de verplichtingen uit hoofde van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en Hoofdstuk 7 van

8° "risque" : le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise;

9° "évaluation des risques" : l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident;

10° "SICAD" : Service d'information et de communication de l'arrondissement, tel que visé par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

11° "entité de l'administration publique" : une autorité administrative visée à l'article 14, §1^{er}, alinéa 1^{er}, des lois coordonnées sur le Conseil d'Etat qui satisfait aux critères suivants:

- 1° elle dépend de l'Etat fédéral;
- 2° elle n'a pas de caractère industriel ou commercial;
- 3° elle n'exerce pas à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs de l'annexe;
- 4° elle n'est pas une personne morale de droit privé.

12° "loi NIS 2" : la loi du [xx xxxx xxxx] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

CHAPITRE 3 – Champ d'application

Art. 4. Cette loi s'applique à tous les secteurs et sous-secteurs mentionnés à l'Annexe de la présente loi.

Cette loi ne s'applique toutefois pas aux installations nucléaires au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence Fédérale du Contrôle Nucléaire, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité.

Art. 5. §1^{er}. Les dispositions du Chapitre 4, Section 2, du Chapitre 5 et du Chapitre 7 de la présente loi ne s'appliquent pas aux entités identifiées comme critiques dans les secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques, sauf si le Roi en décide autrement pour atteindre un niveau de résilience plus élevé de ces entités critiques.

§2. Lorsqu'une législation spécifique à des secteurs ou sous-secteurs impose aux entités critiques de prendre des mesures pour accroître leur résilience, le Roi peut déterminer que ces mesures sont considérées comme équivalentes aux obligations prévues au Chapitre 4, Section 2, au Chapitre 5 et au Chapitre 7 de la présente loi.

deze wet. In dat geval zijn deze bepalingen niet van toepassing op deze sectoren of deelsectoren.

Art. 6. §1. Deze wet is voor de sector overheid niet van toepassing op:

1° de inlichtingen- en veiligheidsdiensten bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten;

2° het Coördinatieorgaan voor de dreigingsanalyse opgericht bij artikel 5 van de wet van 10 juli 2006 betreffende de analyse van de dreiging;

3° het Ministerie van Landsverdediging bedoeld in artikel 1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten;

4° de politiediensten en de algemene inspectie bedoeld in artikel 2, 2° en 3° van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;

5° de rechterlijke overheden, begrepen als de organen van de rechterlijke macht, met inbegrip van het Openbaar Ministerie;

6° de Federale Overheidsdienst Justitie opgericht bij het koninklijk besluit van 23 mei 2001 houdende oprichting van de Federale Overheidsdienst Justitie, wanneer deze databanken beheert voor de rechterlijke overheden bedoeld in 5°;

7° diplomatieke en consulaire missies in landen buiten de Europese Unie;

8° NCCN;

9° nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van NIS2-wet.

§2. Hoofdstuk 4, Afdeling 2, en Hoofdstukken 5 en 7 van deze wet zijn in elk geval niet van toepassing op kritieke entiteiten die geïdentificeerd werden op grond van Hoofdstuk 4, Afdeling 1, van deze wet, die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten, of die uitsluitend diensten verlenen aan de in paragraaf 1 bedoelde overheidsinstanties.

HOOFDSTUK 4 – Identificatieprocedure

Afdeling 1. Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructuren

Art. 7. §1 De sectorale overheid stelt een lijst op van essentiële diensten van de in Bijlage genoemde sectoren en deelsectoren.

Dans ce cas, les présentes dispositions ne s'appliquent pas à ces secteurs ou sous-secteurs.

Art. 6. §1^{er}. Pour le secteur des administrations publiques, cette loi ne s'applique pas :

1° aux services de renseignement et de sécurité visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité;

2° à l'Organe de coordination pour l'analyse de la menace créé par l'article 5 de la loi du 10 juillet 2006 relative à l'analyse de la menace;

3° au Ministère de la Défense visé à l'article 1^{er} de l'arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités;

4° aux services de police et à l'inspection générale visés à l'article 2, 2°, et 3°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux;

5° aux autorités judiciaires, entendues comme les organes du pouvoir judiciaire, le Ministère public inclus;

6° au Service public fédéral Justice créé par l'arrêté royal du 23 mai 2001 portant création du Service public fédéral Justice, lorsqu'il gère des banques de données pour les autorités judiciaires visés au 5°;

7° aux missions diplomatiques et consulaires belges dans des pays tiers à l'Union européenne;

8° au NCCN;

9° à l'Autorité nationale de cybersécurité visée à l'article 16 de la loi NIS2.

§2. En tout état de cause, le Chapitre 4, Section 2, et les Chapitres 5 et 7 de la présente loi ne s'appliquent pas aux entités critiques identifiées conformément au Chapitre 4, Section 1^{ère} de la présente loi, qui exercent des activités dans le domaine de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales, ou qui fournissent des services exclusivement aux autorités publiques visées au paragraphe 1^{er}.

CHAPITRE 4 – Procédure d'identification

Section 1^{ère}. Identification et désignation des entités critiques et des infrastructures critiques

Art. 7. §1^{er} L'autorité sectorielle prépare une liste de services essentiels des secteurs et sous-secteurs énumérés en Annexe.

§2 De sectorale overheid voert uiterlijk op 17 januari 2026, een risicobeoordeling uit, gebruikmakend van de lijst bedoeld in paragraaf 1, en vervolgens telkens wanneer dat nodig is en ten minste om de vier jaar, teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuur overeenkomstig deze Afdeling te identificeren, en die kritieke entiteiten te assisteren bij het nemen van maatregelen uit hoofde van artikel 18.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

§3. In de risicobeoordeling wordt rekening gehouden met relevante natuurlijke en door de mens veroorzaakte risico's, met inbegrip van intersectorale of grensoverschrijdende risico's, ongevallen, natuurrampen, noodsituaties op het gebied van volksgezondheid, hybride dreigingen en andere vijandelijke dreigingen, waaronder terroristische misdrijven als bedoeld in Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad.

§4. Bij de uitvoering van de risicobeoordeling houdt de sectorale overheid, wanneer relevant voor haar sector of deelsector, ten minste rekening met het volgende:

1° de algemene risicobeoordeling die is uitgevoerd overeenkomstig artikel 6, lid 1 van Besluit 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming;

2° andere relevante risicobeoordelingen, uitgevoerd overeenkomstig de voorschriften van de relevante sectorspecifieke wetgeving van de Europese Unie, met inbegrip van Verordening (EU) 2019/941 van het Europees Parlement en de Raad van 5 juni 2019 betreffende risicoparaatheid in de elektriciteitssector en tot intrekking van Richtlijn 2005/89/EG, Verordening (EU) 2017/1938 van het Europees Parlement en de Raad van 25 oktober 2017 betreffende maatregelen tot veiligstelling van de gasleveringszekerheid en houdende intrekking van Verordening (EU) 994/2010, en de Richtlijnen 2007/60/EG van het Europees Parlement en de Raad van 23 oktober 2007 over beoordeling en beheer van overstromingsrisico's en 2012/18/EU van het Europees Parlement en de Raad van 4 juli 2012 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken, houdende wijziging en vervolgens intrekking van Richtlijn 96/82/EG van de Raad;

3° de relevante risico's die voortvloeien uit de afhankelijkheden tussen de in de Bijlage bedoelde sectoren, met inbegrip van de afhankelijkheid van in andere Lidstaten en derde landen gevestigde entiteiten en de gevolgen die een significante verstoring in één sector

§2. L'autorité sectorielle procède, à l'aide de la liste visée au paragraphe 1^{er}, à une évaluation des risques au plus tard le 17 janvier 2026, et par la suite chaque fois que nécessaire et au moins tous les quatre ans, en vue d'identifier les entités critiques et leurs infrastructures critiques respectives conformément à la présente Section, et afin d'assister ces entités critiques à prendre des mesures en vertu de l'article 18.

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées, pour les entités critiques potentielles relevant de leurs compétences pour d'autres aspects.

§3. L'évaluation de risques tient compte des risques naturels et d'origine humaine pertinents, en ce compris les risques intersectoriels ou transfrontaliers, les accidents, les catastrophes naturelles, les urgences en matière de santé publique, les menaces hybrides et les autres menaces à caractère hostile, notamment les infractions terroristes visées par la Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la Décision-cadre 2002/475/JAI du Conseil et modifiant la Décision 2005/671/JAI du Conseil.

§4. Lors de l'évaluation des risques, l'autorité sectorielle prend au moins en compte les éléments suivants, lorsque cela est pertinent pour son secteur ou sous-secteur:

1° l'évaluation des risques effectuée conformément à l'article 6, paragraphe 1^{er}, de la Décision. 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union;

2° d'autres évaluations de risques pertinentes réalisées conformément aux exigences de la législation pertinente de l'Union européenne, notamment le Règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin relatif à la préparation aux risques dans le secteur de l'électricité et abrogeant la Directive 2005/89/CE, le Règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz et abrogeant le Règlement (UE) 994/2010, et les Directives 2007/60/CE du Parlement européen et du Conseil du 23 octobre 2007 relative à l'évaluation et la gestion des risques d'inondation et 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses, modifiant puis abrogeant la Directive 96/82/CE du Conseil ;

3° les risques pertinents découlant des dépendances entre les secteurs visés en Annexe, y compris les dépendances à l'égard d'entités établies dans d'autres États membres et dans des pays tiers, et l'impact qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris les risques importants pour les citoyens et le marché intérieur ;

kan hebben voor andere sectoren, met inbegrip van significante risico's voor de burgers en de interne markt ;

4° alle informatie over incidenten waarvan op grond van artikel 20, paragraaf 1 is kennisgegeven.

Art. 8. §1. Binnen een termijn van negen maanden, te rekenen vanaf de inwerkingtreding van deze wet, voert het OCAD een dreigingsanalyse uit voor de sectoren of deelsectoren vermeld in de Bijlage.

Deze dreigingsanalyse blijft gedurende maximaal vier jaar geldig vanaf de datum van voltooiing zoals aangegeven in artikel 77. Deze analyse wordt telkens wanneer nodig en ten minste één keer om de vier jaar vernieuwd.

Elke dreigingsanalyse die binnen vier jaar wordt uitgevoerd op basis van andere wetgeving voor de in Bijlage vermelde (deel-)sectoren moet voldoen aan de verplichtingen van dit artikel.

§2. De dreigingsanalyse in de zin van dit hoofdstuk bestaat uit een strategische gemeenschappelijke evaluatie zoals bedoeld in artikel 8, eerste lid, 1° van de wet van 10 juli 2006 betreffende de dreigingsanalyse.

De dreigingsanalyse heeft betrekking op elk type van dreiging die door het OCAD pertinent worden geacht ten aanzien van de sector of deelsector, die vallen onder de bevoegdheid van de ondersteunende diensten opgesomd in artikel 2, 2° van voornoemde wet van 10 juli 2006.

§3. De autoriteit bedoeld in artikel 21, §1, de sectorale overheden en de ondersteunende diensten van het OCAD delen de informatiegegevens die nuttig zijn voor de uitvoering van de dreigingsanalyse bedoeld in paragraaf 1 mee aan het OCAD.

§4. Onverminderd artikel 10, § 1 van de voornoemde wet van 10 juli 2006 en artikel 8 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst, wordt deze evaluatie meegedeeld aan de sectorale overheden zodat zij de conclusies van deze dreigingsanalyse kunnen opnemen in de risicoanalyse die zij krachtens artikel 7 moeten uitvoeren.

Art. 9. §1. 1° Teneinde de kritieke entiteiten en hun respectievelijke kritieke infrastructuren die onder haar bevoegdheid vallen te identificeren, overlegt de sectorale overheid vooraf met de autoriteit bedoeld in artikel 21, §1, en raadpleegt zij de potentiële kritieke entiteiten en desgevallend de vertegenwoordigers van de sector.

De potentiële kritieke entiteiten zijn gehouden tot een degelijke informatie-uitwisseling met de sectorale overheid tijdens het identificatieproces.

De sectorale overheid kan overgaan tot een voorafgaande raadpleging van de gefedereerde entiteiten, voor de potentiële kritieke entiteiten die voor andere aspecten onder hun bevoegdheden vallen.

4° toute information sur les incidents notifiés en vertu de l'article 20, paragraphe 1^{er}.

Art. 8. §1^{er}. Dans un délai de neuf mois à compter de l'entrée en vigueur de la présente loi, l'OCAM procède à une analyse de la menace pour les secteurs ou sous-secteurs énumérés en Annexe.

Cette analyse de la menace reste valable pour un maximum de quatre ans à compter de sa réalisation comme prévu à l'article 77. Cette analyse est renouvelée chaque fois que nécessaire et au moins une fois tous les quatre ans.

Toute analyse de la menace réalisée endéans les quatre ans sur base d'une autre législation pour les (sous)-secteurs énumérés en Annexe doit être conforme aux obligations du présent article.

§2. L'analyse de la menace au sens du présent chapitre consiste en une évaluation stratégique commune telle que visée à l'article 8, alinéa 1^{er}, 1° de la loi du 10 juillet 2006 relative à l'analyse de la menace.

L'analyse de la menace vise tout type de menace jugée pertinente par l'OCAM en ce qui concerne le secteur ou le sous-secteur, qui relèvent de la compétence des services d'appui, énumérés à l'article 2, 2° de la loi du 10 juillet 2006 susmentionnée.

§3. L'autorité visée à l'article 21, §1^{er}, les autorités sectorielles et les services d'appui de l'OCAM communiquent à l'OCAM les informations utiles pour effectuer l'analyse de la menace visée au paragraphe 1^{er}.

§4. Sans préjudice de l'article 10, § 1^{er} de la loi du 10 juillet 2006 susmentionnée et de l'article 8 de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé, cette évaluation est communiquée aux autorités sectorielles afin de leur permettre d'intégrer les conclusions de cette analyse de la menace dans l'analyse de risques qu'elles sont tenues d'effectuer en vertu de l'article 7.

Art. 9. §1^{er}. 1° Afin d'identifier les entités critiques et leurs infrastructures critiques respectives relevant de sa compétence, l'autorité sectorielle consulte au préalable l'autorité visée à l'article 21, §1^{er}, les entités critiques potentielles et, le cas échéant, les représentants du secteur.

Les entités critiques potentielles sont tenues à des échanges d'informations appropriés avec l'autorité sectorielle au cours du processus d'identification.

L'autorité sectorielle peut procéder à une consultation préalable des entités fédérées pour les entités critiques potentielles relevant pour d'autres aspects de leurs compétences.

2° De sectorale overheid past de criteria, zoals bedoeld in artikel 10, §1, toe teneinde een selectie te maken tussen de entiteiten die in haar sector bestaan en stelt een lijst op van de aldus geïdentificeerde potentiële kritieke entiteiten.

3° Of een incident een aanzienlijk verstorend effect heeft wordt bepaald in functie van de karakteristieken van de betrokken sector, op basis van de criteria bedoeld in artikel 10, §2.

4° De sectorale overheid kan, in voorkomend geval, de sectorale criteria bedoeld in artikel 11 toepassen op deze lijst.

§2. De potentiële kritieke entiteit bezorgt aan de sectorale overheid binnen zes maanden na de raadpleging zoals bedoeld in de eerste paragraaf, een gemotiveerde lijst op van de bijhorende kritieke infrastructuren die noodzakelijk zijn voor de verlening van essentiële diensten. Deze lijst wordt gevalideerd door de bevoegde sectorale overheid, rekening houdende met de criteria uit artikel 10, paragraaf 2.

De sectorale overheid behoudt zich het recht voor om deze lijst te wijzigen, met opgave van motivatie hiervoor.

De kritieke entiteit is ten allen tijde verantwoordelijk voor het actualiseren van deze lijst, en stelt binnen 30 dagen na de wijziging de bevoegde sectorale overheid daarvan op de hoogte, met opgave van motivatie hiervoor. Elke wijziging dient gevalideerd te worden door de sectorale overheid. De sectorale overheid stelt op zijn beurt de autoriteit bedoeld in artikel 21, §1, in kennis van deze wijziging.

De sectorale overheid waakt over de coherentie in haar sector of deelsector voor wat betreft de identificatie van kritieke infrastructuren.

§3. De Koning kan de voorwaarden en modaliteiten bepalen voor de informatie uitwisseling in het kader van de identificatieprocedure.

§4. Tijdens het identificatieproces als bedoeld in deze Afdeling wordt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de wet tot vaststellen van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hierna: NIS 2-Wet), betrokken bij het door de sectorale overheden en de autoriteit bedoeld in artikel 21, §1, gevoerde overleg voor de identificatie van de kritieke entiteiten met betrekking tot de cyberbeveiliging van netwerk- en informatiesystemen.

Art. 10. §1. De sectorale overheid houdt bij de identificatie van kritieke entiteiten overeenkomstig deze Afdeling rekening met de resultaten van de risicobeoordeling uit hoofde van artikel 7, en past alle volgende criteria toe:

- 1° De entiteit verleent één of meer essentiële diensten;
- 2° De entiteit is actief en haar kritieke infrastructuur bevindt zich op het Belgisch grondgebied;
- 3° Een incident zou een aanzienlijk verstorend effect hebben op de verlening van deze essentiële diensten of andere essentiële diensten van de sectoren die onder het toepassingsgebied vallen van deze wet, zoals bepaald in de Bijlage.

2° L'autorité sectorielle applique les critères, tels que visés à l'article 10, §1^{er}, afin d'effectuer une sélection parmi les entités existantes dans son secteur, et établit une liste des entités critiques potentielles ainsi identifiées.

3° L'importance de l'effet perturbateur d'un incident est déterminée en fonction des caractéristiques du secteur concerné, sur la base des critères visés à l'article 10, §2.

4° L'autorité sectorielle peut, le cas échéant, appliquer les critères sectoriels visés à l'article 11 à cette liste.

§2. L'entité critique potentielle transmet à l'autorité sectorielle, dans un délai de six mois à compter de la consultation visée au premier paragraphe, une liste motivée des infrastructures critiques qui y sont associées et qui sont nécessaires à la fourniture des services essentiels. Cette liste est validée par l'autorité sectorielle compétente, en tenant compte des critères énoncés à l'article 10, paragraphe 2.

L'autorité sectorielle se réserve le droit de modifier cette liste, en motivant sa décision.

L'entité critique est en tout temps responsable de la mise à jour de cette liste et notifie l'autorité sectorielle compétente endéans les 30 jours de la modification, en motivant sa décision. Toute modification doit être validée par l'autorité sectorielle. L'autorité sectorielle notifie à son tour cette modification à l'autorité visée à l'article 21, §1^{er}.

L'autorité sectorielle assure la cohérence dans son secteur ou sous-secteur en ce qui concerne l'identification des infrastructures critiques.

§3. Le Roi peut déterminer les conditions et les modalités concernant l'échange d'informations dans le cadre de la procédure d'identification.

§4. Lors du processus d'identification visé à la présente Section, l'autorité nationale de cybersécurité visée à l'article 16 de la loi du établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après : loi NIS 2) est associée aux consultations menées par les autorités sectorielles et l'autorité visée à l'article 21, §1^{er}, pour l'identification des entités critiques en ce qui concerne la cybersécurité des réseaux et des systèmes d'information.

Art. 10. §1^{er}. Lors de l'identification d'entités critiques conformément à la présente Section, l'autorité sectorielle tient compte des résultats de l'évaluation de risques prévue à l'article 7, et applique tous les critères suivants:

- 1° L'entité fournit un ou plusieurs services essentiels;
- 2° L'entité exerce ses activités sur le territoire belge et son infrastructure critique sont situées sur ledit territoire;
- 3° Un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels ou d'autres services essentiels des secteurs relevant du champ d'application de la présente loi, tels que définis en Annexe.

§2. De sectorale overheid bepaalt, in overleg met de autoriteit bedoeld in artikel 21, §1, en in voorkomend geval, na raadpleging van de betrokken gefedereerde entiteiten, of een incident een aanzienlijk verstoringseffect kan hebben op de verlening van essentiële diensten, rekening houdend met de volgende criteria:

- 1° het belang van de entiteit om de essentiële dienst op een voldoende niveau te houden, rekening houdend met de beschikbare alternatieven voor het verlenen ervan;
- 2° het aantal gebruikers dat afhankelijk is van de door de entiteit verleende essentiële dienst;
- 3° het marktaandeel van de entiteit op de markt voor dergelijke diensten;
- 4° de mate waarin andere in Bijlage genoemde sectoren afhankelijk zijn van die essentiële dienst;
- 5° de ernst en duur van de gevolgen die incidenten kunnen hebben voor de economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging en volksgezondheid;
- 6° het geografische gebied dat door een incident kan worden getroffen, met inbegrip van eventuele grensoverschrijdende gevolgen.

In het geconsolideerd dossier, zoals bedoeld in artikel 12, §1, onderbouwt de sectorale overheid deze criteria op kwantitatieve en sectorspecifieke of deel-sectorspecifieke wijze, voor zover deze gegevens beschikbaar zijn. De autoriteit bedoeld in artikel 21, §1, kan hierover gemotiveerd relevante informatie opvragen aan de sectorale overheid.

Art. 11. De sectorale overheid kan sectorale criteria bepalen waaraan de kritieke entiteiten moeten voldoen, rekening houdend met de bijzondere eigenschappen van de betrokken sector, in overleg met de autoriteit bedoeld in artikel 21, §1, en, in voorkomend geval, na raadpleging van de betrokken gefedereerde entiteiten.

Art. 12. §1. De sectorale overheid stelt een geconsolideerd dossier op, bestaande uit de volgende informatie:

- 1° een lijst van de geïdentificeerde potentiële kritieke entiteiten;
- 2° een lijst van de geïdentificeerde potentiële kritieke infrastructuren;
- 3° in voorkomend geval, de gebruikte sectorale criteria;
- 4° de gebruikte criteria zoals bedoeld in artikel 10, §2;
- 5° een uiteenzetting van de redenen.

De sectorale overheid zendt het geconsolideerd dossier ter advies over aan de autoriteit bedoeld in artikel 21, §1, en, in voorkomend geval, ter informatie aan de betrokken gefedereerde entiteiten.

Nadat de sectorale overheid het advies bedoeld in het tweede lid ontvangen heeft, duidt zij de kritieke entiteiten en de respectievelijke kritieke infrastructuren aan, in voorkomend geval, na raadpleging van de betrokken gefedereerde entiteiten.

§2. L'autorité sectorielle, en concertation avec l'autorité visée à l'article 21, §1^{er}, et, le cas échéant, après consultation des entités fédérées concernées, détermine si un incident pourrait avoir un effet perturbateur important sur la fourniture des services essentiels, en tenant compte des critères suivants:

- 1° l'intérêt de l'entité à maintenir un niveau adéquat de fourniture de service essentiel, en tenant compte des alternatives disponibles pour sa fourniture;
- 2° le nombre d'utilisateurs dépendant du service essentiel fourni par l'entité;
- 3° la part de marché de l'entité sur le marché de ces services;
- 4° la mesure dans laquelle d'autres secteurs énumérés en Annexe dépendent de ce service essentiel;
- 5° la gravité et la durée de l'impact que les incidents peuvent avoir sur les activités économiques et sociales, l'environnement, la sûreté et la sécurité publiques et la santé publique;
- 6° la zone géographique susceptible d'être affectée par un incident, y compris d'éventuels impacts transfrontaliers.

Dans le dossier consolidé, visé à l'article 12, §1^{er}, l'autorité sectorielle justifie ces critères de manière quantitative et de manière spécifique au secteur ou sous-secteur, lorsque ces données sont disponibles. L'autorité visée à l'article 21, §1^{er}, peut demander des informations pertinentes à ce sujet à l'autorité sectorielle, au moyen d'une demande motivée.

Art. 11. L'autorité sectorielle peut déterminer des critères sectoriels auxquels doivent répondre les entités critiques en tenant compte des particularités du secteur concerné, en concertation avec l'autorité visée à l'article 21, §1^{er}, et, le cas échéant, après avoir consulté les entités fédérées.

Art. 12. §1^{er}. L'autorité sectorielle prépare un dossier consolidé composé des informations suivantes:

- 1° une liste des entités critiques potentiellement identifiées;
- 2° une liste des infrastructures critiques potentiellement identifiées;
- 3° le cas échéant, les critères sectoriels utilisés;
- 4° les critères utilisés tels que visés à l'article 10, §2;
- 5° une justification motivée.

L'autorité sectorielle envoie le dossier consolidé pour avis à l'autorité visée à l'article 21, §1^{er} et, le cas échéant, pour information aux entités fédérées.

Après avoir reçu l'avis visé au deuxième alinéa, l'autorité sectorielle désigne les entités critiques et les infrastructures critiques respectives et, le cas échéant, après consultation des entités fédérées.

De autoriteit bedoeld in artikel 21, §1, geeft bij elke substantiële wijziging in het geconsolideerde dossier opnieuw advies over die wijziging.

§2. Indien geen kritieke entiteit gelegen op het Belgisch grondgebied geïdentificeerd werd binnen een sector of deelsector, zet de bevoegde sectorale overheid, in een schrijven ter attentie van de autoriteit bedoeld in artikel 21, §1, de redenen uiteen die geleid hebben tot deze afwezigheid van identificatie.

§3. De sectorale overheid duidt uiterlijk op 17 juli 2026 de kritieke entiteiten aan. De sectorale overheid voert het identificatieproces zoals beschreven in deze Afdeling minstens één keer om de vier jaar uit, voor wat betreft de kritieke entiteiten die tot haar sector behoren.

Art. 13. §1. De sectorale overheid betekent, aan de entiteit, de met redenen omklede beslissing tot de aanduiding ervan als kritieke entiteit, met inbegrip van de kritieke infrastructuur, binnen een maand na de aanduiding als bedoeld in artikel 12. De sectorale overheid bezorgt aan de autoriteit bedoeld in artikel 21, §1, een kopie van deze beslissing met de vermelding van de datum van betekening aan de desbetreffende kritieke entiteit.

§2. De autoriteit bedoeld in artikel 21, §1, brengt op de hoogte van deze aanduiding:

1. De burgemeester van de gemeente op het grondgebied waarvan de kritieke infrastructuur van de kritieke entiteit zich bevindt;
2. De gouverneur van de provincie op het grondgebied waarvan de kritieke entiteit of haar kritieke infrastructuur zich bevindt of, wanneer de kritieke entiteit zich op het grondgebied van de Brusselse agglomeratie bevindt, de bevoegde overheid krachtens artikel 48 van de bijzondere wet van 12 januari 1989 met betrekking tot de Brusselse instellingen.

§3. De autoriteit bedoeld in artikel 21, §1, bezorgt na de aanduiding van een kritieke entiteit en zijn respectievelijke kritieke infrastructuur, en daarna minstens jaarlijks, aan de door de Koning aangewezen dienst de gemeente waarin de kritieke infrastructuur zich bevindt of, in voorkomend geval, een lijst van de gemeenten waarin de kritieke infrastructuren zich bevinden voor de toepassing van artikel 126/3 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

§4. De autoriteit bedoeld in artikel 21, §1, brengt de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-wet op de hoogte van de aanduiding van de kritieke entiteiten.

Afdeling 2. Kritieke entiteiten van bijzonder Europees belang

Art. 14. §1. Een entiteit wordt als een kritieke entiteit van bijzonder Europees belang beschouwd wanneer zij overeenkomstig artikel 12 als kritieke entiteit werd aangeduid, essentiële diensten verleent aan of in meer

Chaque fois qu'il y a un changement substantiel, l'autorité visée à l'article 21, §1^{er}, émet un nouvel avis sur toute modification substantielle du dossier consolidé.

§2. Si aucune entité critique située sur le territoire belge n'a été identifiée dans un secteur ou sous-secteur, l'autorité sectorielle compétente expose, dans un écrit à l'attention de l'autorité visée à l'article 21, §1^{er}, les raisons qui ont conduit à cette absence d'identification.

§3. L'autorité sectorielle désigne les entités critiques au plus tard le 17 juillet 2026. L'autorité sectorielle renouvelle le processus d'identification tel que décrit dans cette Section au moins une fois tous les quatre ans en ce qui concerne les entités critiques appartenant à son secteur.

Art. 13. §1^{er}. L'autorité sectorielle notifie à l'entité, dans un délai d'un mois après la désignation visée à l'article 12, la décision motivée de la désigner comme entité critique, y compris l'infrastructure critique. L'autorité sectorielle fournit à l'autorité visée à l'article 21, §1^{er}, une copie de cette décision avec mention de la date de la notification à l'entité critique concernée.

§2. L'autorité visée à l'article 21, §1^{er}, doit informer de cette désignation :

1. Le bourgmestre de la commune sur le territoire de laquelle se trouvent les infrastructures critiques de l'entité critique ;
2. Le gouverneur de la province sur le territoire de laquelle l'entité critique ou son infrastructure critique se situe ou, lorsque l'entité critique se situe sur le territoire de l'agglomération bruxelloise, l'autorité compétente en vertu de l'article 48 de la loi spéciale du 12 janvier 1989 sur les institutions bruxelloises.

§3. Après la désignation d'une entité critique et de son infrastructure critique respective, et au moins une fois par an par la suite, l'autorité visée à l'article 21, §1^{er}, communique au service désigné par le Roi la commune dans laquelle l'infrastructure critique se situe ou, le cas échéant, une liste des communes dans lesquelles les infrastructures critiques sont situées aux fins de l'article 126/3 de la loi du 13 juin 2005 relative aux communications électroniques.

§4. L'autorité visée à l'article 21, §1, informe l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 de la désignation des entités critiques.

Section 2. Entités critiques revêtant une importance européenne particulière

Art. 14. §1^{er}. Une entité est considérée comme une entité critique revêtant une importance européenne particulière pour autant qu'elle ait été désignée comme une entité critique conformément à l'article 12, qu'elle fournisse des services essentiels à ou dans plus de 6 États membres, et

dan 6 lidstaten, en op grond van artikel 13, §1 in kennis gesteld werd van haar aanduiding als kritieke entiteit.

§2. Na de kennisgeving van haar aanduiding overeenkomstig artikel 13, §1, dient de kritieke entiteit de bevoegde sectorale overheid te informeren wanneer zij essentiële diensten verleent aan of in meer dan 6 lidstaten, welke essentiële diensten zij levert aan of in die lidstaten en aan of in welke lidstaten zij die essentiële diensten verleent.

De sectorale overheid stelt de autoriteit bedoeld in artikel 21, §1, hiervan onverwijld in kennis.

§3. De bevoegde sectorale overheid stelt, nadat zij hiervan op de hoogte gebracht werd door de autoriteit bedoeld in artikel 21, §1, de betrokken entiteit er onverwijld van in kennis dat zij als kritieke entiteit van bijzonder Europees belang wordt beschouwd.

Art. 15. Het Centraal Contactpunt, zoals bedoeld in artikel 21, §1, is belast met het voeren van bilateraal en multilateraal overleg met de Lidstaten van de Europese Unie inzake kritieke entiteiten:

- a) die gebruik maken van een kritieke infrastructuur die fysiek verbonden is met twee of meer Lidstaten;
- b) die deel uitmaken van bedrijfsstructuren die verbonden zijn met of gekoppeld zijn aan kritieke entiteiten in andere Lidstaten;
- c) die in een Lidstaat als zodanig zijn aangemerkt en essentiële diensten verlenen aan of in andere Lidstaten.

Het overleg is erop gericht de weerbaarheid van kritieke entiteiten te vergroten en, waar mogelijk, de administratieve lasten voor de kritieke entiteiten te verminderen.

HOOFDSTUK 5 – Interne weerbaarheidsmaatregelen van de kritieke entiteit

Art. 16. §1. De kritieke entiteit duidt een "contactpunt kritieke entiteit" aan en maakt de contactgegevens ervan over aan de sectorale overheid binnen een termijn van zes maanden vanaf de betekening van de aanduiding als kritieke entiteit, alsook na elke wijziging van deze gegevens.

Het "contactpunt kritieke entiteit" oefent de functie uit van contactpunt ten aanzien van de sectorale overheid, de autoriteit bedoeld in artikel 21, §1, de burgemeester, de gouverneur, de politiediensten en elke andere bevoegde overheid of openbare dienst voor elke vraag in verband met de weerbaarheid van de entiteit en zijn infrastructuur.

§2. Indien er reeds een "contactpunt kritieke entiteit" werd aangeduid krachtens nationale of Europese bepalingen, maakt de kritieke entiteit de contactgegevens ervan over aan de sectorale overheid.

§3. Het "contactpunt kritieke entiteit" is te allen tijde beschikbaar.

qu'elle ait été notifiée en vertu de l'article 13, § 1^{er} de sa désignation en tant qu'entité critique.

§2. Suite à la notification de sa désignation conformément à l'article 13, §1^{er}, l'entité critique doit informer l'autorité sectorielle compétente lorsqu'elle fournit des services essentiels à ou dans plus de 6 États membres, quels sont les services essentiels qu'elle fournit à ou dans ces États membres, et à quels États membres elle fournit ces services essentiels.

L'autorité sectorielle en informe l'autorité visée à l'article 21, §1^{er}, sans délai.

§3. L'autorité sectorielle compétente, après avoir été informée par l'autorité visée à l'article 21, §1^{er}, notifie sans délai à l'entité concernée qu'elle est considérée comme une entité critique revêtant une importance européenne particulière.

Art. 15. Le Point de Contact Central, visé à l'article 21, §1^{er}, est chargé de mener des discussions bilatérales et multilatérales avec les États membres de l'Union européenne sur des entités critiques :

- a) qui ont recours à une infrastructure critique qui est physiquement connectée avec deux États membres ou plus;
- b) qui font partie de structures d'entreprise connectées ou liées à des entités critiques dans d'autres États membres;
- c) qui sont identifiées comme telles dans un État membre et fournissent des services essentiels à ou dans d'autres États membres.

La concertation vise à accroître la résilience des entités critiques et, dans la mesure du possible, à réduire la charge administrative reposant sur les entités critiques.

CHAPITRE 5 – Mesures internes de la résilience de l'entité critique

Art. 16. §1^{er}. L'entité critique désigne un "point de contact de l'entité critique" et transfère ses coordonnées à l'autorité sectorielle dans un délai de six mois à compter de la notification de la désignation en tant qu'entité critique, ainsi qu'après chaque modification de ces données.

Le "point de contact de l'entité critique" remplit la fonction de point de contact vis-à-vis de l'autorité sectorielle, de l'autorité visée à l'article 21, §1^{er}, du bourgmestre, du gouverneur, des forces de police, et de tout autre autorité ou service public compétent, pour toute question liée à la résilience de l'entité et de son infrastructure.

§2. Si un "point de contact de l'entité critique" a été déjà désigné en vertu de dispositions nationales ou européennes, l'entité critique transfère ses coordonnées à l'autorité sectorielle.

§3. Le "point de contact de l'entité critique" est disponible à tout moment.

Art. 17. §1. De kritieke entiteit maakt een risicobeoordeling van alle relevante risico's die de levering van haar essentiële diensten kunnen verstoren, binnen negen maanden na ontvangst van de in artikel 13, §1, bedoelde kennisgeving, en vervolgens telkens wanneer dat nodig is, en ten minste om de vier jaar. Daarbij houdt ze rekening met de risicobeoordeling bedoeld in artikel 7, §2, de dreigingsanalyse bedoeld in artikel 8 die het OCAD opstelt en andere relevante informatie.

§2. De risicobeoordeling van de kritieke entiteit zoals bedoeld in paragraaf 1, neemt de in artikel 7, §3 bedoelde relevante risico's in aanmerking die tot een incident zouden kunnen leiden. De risicobeoordeling houdt rekening met de mate waarin andere in Bijlage beschreven sectoren afhankelijk zijn van de door de kritieke entiteit verleende essentiële dienst, en de mate waarin die kritieke entiteit afhankelijk is van essentiële diensten van andere entiteiten in andere sectoren, in voorkomend geval tevens in naburige Lidstaten en derde landen.

§3. Indien een kritieke entiteit reeds risicobeoordelingen heeft uitgevoerd of documenten heeft opgesteld krachtens andere wettelijke bepalingen die relevant zijn voor haar risicobeoordeling bedoeld in paragraaf 1, kunnen die beoordelingen en documenten gebruikt worden om aan de voorschriften van dit artikel te voldoen, voor zover deze betrekking hebben op de in artikel 7, §3 bedoelde risico's.

Art. 18. §1. De kritieke entiteit werkt een weerbaarheidsplan van de entiteit uit, hierna W.P.E. genaamd, met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke entiteit en de weerbaarheid ervan te waarborgen, door het op punt stellen van interne passende en evenredige technische, veiligheids- en organisatorische maatregelen.

§2. Het W.P.E. bevat weerbaarheidsmaatregelen die toegepast worden in functie van de risico's waaraan de entiteit kan worden blootgesteld, rekening houdend met de mogelijkheid tot wijzigende omstandigheden.

Voor een bepaalde sector, of in voorkomend geval, per deelsector, kan de Koning deze maatregelen specificeren en opleggen om bepaalde informatie op te nemen in het W.P.E.

§3. Het W.P.E. bevat minstens:

1° Een opsomming van weerbaarheidsmaatregelen, met inbegrip van maatregelen die nodig zijn om:

- a) te voorkomen dat incidenten zich voordoen, rekening houdend met maatregelen ter beperking van het risico op rampen en maatregelen voor aanpassing aan de klimaatverandering;
- b) te zorgen voor adequate fysieke bescherming van de gebouwen en kritieke infrastructuur, rekening houdend met het plaatsen van omheiningen, het oprichten van barrières, instrumenten en routines voor bewaking van de omgeving, detectieapparatuur en toegangscontroles;
- c) de gevolgen van incidenten te bestrijden, te beperken en ertegen bestand te zijn, door te voorzien in aangepaste materiële en organisatorische noodmaatregelen en naar

Art. 17. §1^{er}. L'entité critique procède à une évaluation de tous les risques pertinents susceptibles de perturber la fourniture de ses services essentiels, dans les neuf mois suivant la réception de la notification visée à l'article 13, §1^{er}, et par la suite chaque fois que nécessaire, et au moins tous les quatre ans. Ce faisant, elle tient compte de l'évaluation des risques visée à l'article 7, §2, de l'analyse de la menace effectuée par l'OCAM et visée à l'article 8 et d'autres informations pertinentes.

§2. L'évaluation des risques de l'entité critique, visée au paragraphe 1^{er}, prend en considération les risques pertinents visés à l'article 7, §3 qui pourraient conduire à un incident. L'évaluation des risques tient compte de la mesure dans laquelle d'autres secteurs décrits en Annexe dépendent du service fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités dans d'autres secteurs, y compris, le cas échéant, dans les États membres voisins et les pays tiers.

§3. Si une entité critique a déjà effectué des évaluations de risques ou préparé des documents en vertu d'autres dispositions légales pertinentes pour son évaluation de risques visée au paragraphe 1^{er}, ces évaluations et documents peuvent être utilisés pour se conformer aux exigences du présent article, dans la mesure où ils concernent les risques visés à l'article 7, §3.

Art. 18. §1^{er}. L'entité critique élabore un plan de résilience de l'entité, ci-après dénommé P.R.E., en vue de prévenir, atténuer et neutraliser les risques d'interruption du fonctionnement ou de destruction de l'entité critique et d'assurer la résilience par la mise en place de mesures techniques, sécuritaires et organisationnelles internes appropriées et proportionnées.

§2. Le P.R.E. contient des mesures de résilience appliquées en fonction des risques auxquels l'entité peut être exposée, en tenant compte de la possibilité de changements de circonstances.

Pour un secteur donné, ou, le cas échéant, par sous-secteur, le Roi peut préciser ces mesures et imposer d'inclure certaines informations dans le P.R.E.

§3. Le P.R.E. contient au moins:

1° Un énumération des mesures de résilience, y compris les mesures nécessaires pour:

- a) prévenir les incidents, en tenant compte des mesures de réduction des risques de catastrophes et des mesures d'adaptation au changement climatique;
- b) assurer une protection physique adéquate des bâtiments et des infrastructures critiques, en tenant compte de l'installation de clôtures, de barrières, d'outils et de routines de surveillance des environs, d'équipements de détection et de contrôles d'accès;
- c) traiter, atténuer et résister aux conséquences des incidents, en prévoyant des mesures d'urgence matérielles et organisationnelles appropriées et en tenant dûment compte de la mise en œuvre des

behoren rekening houdend met de uitvoering van de risico- en crisisbeheersingsprocedures en protocollen en waarschuwingroutines, hetgeen de vorm kan aannemen van een intern noodplan;

- d) te herstellen van incidenten, rekening houdend met bedrijfscontinuïteitsmaatregelen en de identificatie van alternatieve toeleveringsketens, teneinde de verlening van de essentiële dienst te hervatten;
- e) te zorgen voor adequaat beheer van personeelsbeveiliging, rekening houdend met maatregelen zoals het vaststellen van categorieën personeelsleden die kritieke functies vervullen, het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en gevoelige informatie, het instellen van procedures voor veiligheidsverificaties zoals bedoeld in artikel 18 en het aanwijzen van categorieën van personen die aan een dergelijke veiligheidsverificatie moeten worden onderworpen, en het vaststellen van passende opleidingsvoorschriften en kwalificaties ;
- f) het relevante personeel bewust te maken van de hierboven vermelde maatregelen, naar behoren rekening houdend met opleidingen, informatiemateriaal en oefeningen.

2° De inventaris en de ligging van de kritieke infrastructuur, zoals bedoeld in artikel 9, §2;

3° De risicobeoordeling vermeld in artikel 17;

§4. Binnen een termijn van uiterlijk tien maanden, te rekenen vanaf de betekening van de aanduiding van haar entiteit als kritieke entiteit zoals bedoeld in artikel 13, past de entiteit de weerbaarheidsmaatregelen uit het W.P.E. toe.

§5. Wanneer kritieke entiteiten uit hoofde van nationale of Europese wetgeving, documenten hebben opgesteld en maatregelen hebben genomen die van belang zijn voor de in paragraaf 3 bedoelde maatregelen, dan kunnen zij deze maatregelen en documenten gebruiken om te voldoen aan de voorschriften van dit artikel.

§6. De kritieke entiteit organiseert oefeningen en actualiseert het W.P.E. in functie van de lessen die getrokken worden uit deze oefeningen.

De Koning bepaalt, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de actualiseringen van het W.P.E.

De Koning bepaalt voor een bepaalde sector of, in voorkomend geval, per deelsector, de nadere regels van de deelneming van de relevante overheidsdiensten aan de oefeningen georganiseerd door de kritieke entiteit.

Art. 19. Op vraag van de bevoegde sectorale overheid of op eigen initiatief kunnen de kritieke entiteiten de procedure uit artikel 22 *quinquies* van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereuleerde dienst opstarten, teneinde de uitoefening van een beroep, functie,

procedures en protocollen de gestion des risques et des crises et des routines d'alerte, ce qui peut prendre la forme d'un plan interne d'urgence;

- d) pour se remettre d'un incident, en prenant en compte les mesures de continuité de l'activité et l'identification de chaînes d'approvisionnement alternatives afin de reprendre la fourniture du service essentiel;
- e) assurer une gestion adéquate de la sécurité du personnel, en tenant compte de mesures telles que l'identification des catégories de personnel exerçant des fonctions critiques, l'établissement de droits d'accès aux bâtiments, aux infrastructures critiques et aux informations sensibles, l'établissement de procédures d'enquête de sécurité visée à l'article 18 et l'identification des catégories de personnes devant faire l'objet d'une telle enquête, ainsi que l'établissement d'exigences appropriées en matière de formation et de qualifications;
- f) sensibiliser le personnel concerné aux mesures énumérées ci-dessus, en tenant dûment compte de la formation, du matériel d'information et des exercices.

2° L'inventaire et la localisation des infrastructures critiques visées à l'article 9, §2;

3° L'évaluation des risques visée à l'article 17;

§4. Dans un délai maximum de dix mois à compter de la notification de la désignation de son entité comme entité critique visée à l'article 13, l'entité met en œuvre les mesures de résilience du P.R.E.

§5. Lorsque les entités critiques ont préparé des plans et des documents en vertu du droit national ou européen qui sont pertinents pour les mesures visées au paragraphe 3, elles peuvent utiliser ces documents pour se conformer aux exigences du présent article.

§6. L'entité critique organise des exercices et met à jour le P.R.E., en fonction des enseignements tirés de ces exercices.

Le Roi détermine, pour un secteur ou sous-secteur donné, la fréquence des exercices et des mises à jour du P.R.E.

Le Roi détermine, pour un secteur donné ou, le cas échéant, par sous-secteur, les modalités de la participation des services publics concernés aux exercices organisés par l'entité critique.

Art. 19. A la demande de l'autorité sectorielle compétente ou de leur propre initiative, les entités critiques peuvent initier la procédure prévue à l'article 22 *quinquies* de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé afin de soumettre l'exercice d'une profession, d'une fonction, d'une mission

opdracht of mandaat, of toegang tot lokalen, gebouwen of terreinen afhankelijk te stellen van het ondergaan van een veiligheidsverificatie.

Art. 20. §1. Onverminderd de wettelijke of reglementaire bepalingen die, in een bepaalde sector of deelsector, opleggen bepaalde diensten te informeren, is de kritieke entiteit ertoe gehouden, wanneer zich een gebeurtenis voordoet die van aard is om de verlening van essentiële diensten aanzienlijk te verstoren of kunnen verstoren, onmiddellijk het SICAD, via een rechtstreeks specifiek voorbehouden communicatiekanaal, de door de bevoegde sectorale overheid aangewezen dienst en de autoriteit bedoeld in artikel 21, §1, te verwittigen.

Deze melding bevat alle beschikbare informatie die nodig is om te bepalen wat de aard, oorzaak en mogelijke gevolgen van het incident zijn, waaronder alle beschikbare informatie die nodig is om te bepalen of er grensoverschrijdende gevolgen zijn.

Om te bepalen of een verstoring aanzienlijk is, wordt rekening gehouden met:

- 1° het aantal getroffen gebruikers en hun aandeel;
- 2° de duur van de gebeurtenis;
- 3° het getroffen geografisch gebied.

In het geval van grensoverschrijdende gevolgen voor de verlening van essentiële diensten in andere Lidstaten, meldt de kritieke entiteit dat aan de autoriteit bedoeld in artikel 21, §1.

§2. Overeenkomstig de nadere regels bepaald door de Minister van Binnenlandse Zaken, verwittigt het SICAD de autoriteit bedoeld in artikel 21, §1, van elke gebeurtenis waarvan het kennis heeft en die van aard is de verlening van essentiële diensten van de kritieke entiteit aanzienlijk te verstoren en, in voorkomend geval, de autoriteit bedoeld in artikel 16 van de [NIS 2 wet].

§3. Indien de gebeurtenis van aard is om de verstoring van de werking of de vernietiging van de betrokken kritieke entiteit als gevolg te hebben, verwittigt het Centraal Contactpunt de bevoegde sectorale overheid en, in het geval het incident aanzienlijke gevolgen heeft of kan hebben voor kritieke entiteiten en voor de continuïteit van de verlening van essentiële diensten in één of meer Lidstaten, de bevoegde overheid van de betrokken Lidstaten.

HOOFDSTUK 6 – Rapportage en informatie-uitwisseling

Afdeling 1. De bevoegde autoriteiten

Art. 21. §1. De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit bedoeld in het eerste lid is ook het Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de Lidstaten van de Europese Unie.

ou d'un mandat, ou l'accès à des locaux, des bâtiments ou des terrains à une vérification de sécurité.

Art. 20. §1^{er}. Sans préjudice des dispositions légales ou réglementaires qui imposent, dans un secteur ou sous-secteur donné, d'informer certains services, l'entité critique est tenue, lorsque survient un événement de nature à perturber ou risquant de perturber de manière importante la fourniture de services essentiels, d'en informer immédiatement le SICAD, par un canal de communication direct et spécifiquement réservé, le service désigné par l'autorité sectorielle compétente et l'autorité visée à l'article 21, §1^{er}.

Cette notification contient toutes les informations disponibles nécessaires pour déterminer la nature, la cause et les conséquences éventuelles de l'incident, y compris toutes les informations disponibles nécessaires pour déterminer s'il y a des implications transfrontalières.

Pour déterminer si une perturbation a un caractère important, il convient de prendre en compte des éléments suivants:

- 1° le nombre d'utilisateurs concernés et leur proportion;
- 2° la durée de l'événement;
- 3° la zone géographique concernée.

En cas d'effets transfrontaliers sur la fourniture de services essentiels dans d'autres États membres, l'entité critique en notifie l'autorité visée à l'article 21, §1^{er}.

§2. Conformément aux modalités fixées par le Ministre de l'Intérieur, le SICAD notifie à l'autorité visée à l'article 21, §1^{er}, tout événement dont il a connaissance et qui est de nature à perturber de manière importante la fourniture des services essentiels de l'entité critique et, le cas échéant, l'autorité visée à l'article 16 de la [loi NIS 2].

§3. Si l'événement est de nature à entraîner l'interruption du fonctionnement ou la destruction de l'entité critique concernée, le Point de Contact Central en informe l'autorité sectorielle compétente et, dans le cas où l'incident a ou peut avoir un impact important sur les entités critiques et sur la continuité de la fourniture des services essentiels dans un ou plusieurs États membres, l'autorité compétente des États membres concernés.

CHAPITRE 6 – Rapports et échange d'informations

Section 1^{ère}. Les autorités compétentes

Art. 21. §1^{er}. Le Roi désigne l'autorité qui, en tant qu'autorité nationale, est chargée du suivi et de la coordination de la mise en œuvre de la présente loi.

L'autorité visée au premier alinéa est également le Point de Contact Central National pour la résilience des entités critiques, pour l'ensemble des secteurs et sous-secteurs, pour la Belgique dans sa relation avec la Commission européenne et les États membres de l'Union européenne.

Daartoe vertegenwoordigt het contactpunt België binnen de Groep voor de weerbaarheid van kritieke entiteiten.

§2. De autoriteit bedoeld in de eerste paragraaf coördineert en voldoet aan de rapportageverplichtingen die voortvloeien uit hoofde van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad inzake de weerbaarheid van kritieke entiteiten.

§3. De Koning kan de coördinerende rol van de autoriteit als bedoeld in de eerste paragraaf voor wat betreft de weerbaarheid van kritieke entiteiten verder preciseren.

§4. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de nadere regels bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst deze wet zelf de bij wet opgerichte en geregelde sectorale overheden aan.

Art. 22. De Koning wijst de autoriteit aan die belast is met het opstellen van een nationale strategie om de weerbaarheid van kritieke entiteiten te verbeteren. Deze strategie wordt uiterlijk op 17 januari 2026, en daarna ten minste om de vier jaar opgesteld.

De autoriteit bedoeld in het eerste lid raadpleegt, in voorkomend geval, de sectorale overheden, de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de NIS 2-wet en de gefedereerde entiteiten.

De nationale strategie bevat minstens:

- 1° strategische doelstellingen en prioriteiten ter vergroting van de algehele weerbaarheid van kritieke entiteiten, met inachtneming van grensoverschrijdende, intersectorale en onderlinge afhankelijkheden;
- 2° een *governance* kader ter verwezenlijking van de strategische doelstellingen en prioriteiten, met inbegrip van een beschrijving van de taken en verantwoordelijkheden van de verschillende autoriteiten, kritieke entiteiten en andere partijen die bij de uitvoering van de strategie betrokken zijn;
- 3° een beschrijving van de maatregelen die nodig zijn om de algehele weerbaarheid van kritieke entiteiten te vergroten, inclusief een beschrijving van de nationale risicobeoordeling;
- 4° een beschrijving van het proces waarmee kritieke entiteiten worden geïdentificeerd;
- 5° een beschrijving van het proces waarmee kritieke entiteiten worden ondersteund, met inbegrip van maatregelen ter verdieping van de samenwerking tussen de publieke sector enerzijds en de particuliere sector en de publieke en particuliere entiteiten anderzijds;
- 6° een lijst van de belangrijkste autoriteiten en belanghebbenden, met uitzondering van de kritieke entiteiten, die betrokken zijn bij de uitvoering van de strategie;

A cette fin, le point de contact représente la Belgique au sein du Groupe pour la résilience des entités critiques.

§2. L'autorité visée au premier paragraphe coordonne et respecte les obligations d'information découlant de la Directive (UE) 2022/2557 du Parlement européen et du Conseil relative à la résilience des entités critiques.

§3. Le Roi peut préciser le rôle de coordination de l'autorité visée au paragraphe 1^{er} en ce qui concerne la résilience des entités critiques.

§4. Le Roi désigne, par arrêté pris après avis du Conseil des ministres, les autorités sectorielles chargées, pour leur secteur respectif, de veiller à l'exécution des dispositions de la présente loi.

Le Roi peut instituer des autorités sectorielles composées de représentants de l'État fédéral, des Communautés et des Régions, selon les modalités prévues à l'article 92ter de la loi spéciale du 8 août 1980 sur la réforme institutionnelle.

Nonobstant le premier alinéa, cette loi désigne elle-même les autorités sectorielles établies et réglementées par la loi.

Art. 22. Le Roi désigne l'autorité chargée d'établir une stratégie nationale visant à améliorer la résilience des entités critiques. Cette stratégie est établie au plus tard le 17 janvier 2026, et au moins tous les quatre ans par la suite.

L'autorité visée à l'alinéa 1^{er} consulte, le cas échéant, les autorités sectorielles, l'autorité nationale de cybersécurité visée à l'article 16 de la loi NIS 2 et les entités fédérées.

La stratégie nationale comprend au moins:

- 1° des objectifs et priorités stratégiques visant à renforcer la résilience globale des entités critiques en tenant compte des aspects transfrontaliers, intersectoriels et des interdépendances;
- 2° un cadre de gouvernance pour atteindre les objectifs et priorités stratégiques, y compris une description des rôles et responsabilités des différentes autorités, entités critiques et autres parties impliquées dans la mise en œuvre de la stratégie;
- 3° une description des mesures nécessaires pour accroître la résilience globale des entités critiques, y compris une description de l'évaluation nationale des risques;
- 4° une description du processus d'identification des entités critiques;
- 5° une description du processus de soutien, y compris les mesures visant à approfondir la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part;
- 6° une liste des principales autorités et parties concernées, à l'exclusion des entités critiques, qui participent à la mise en œuvre de la stratégie;
- 7° un cadre politique pour la coordination entre les autorités compétentes en vertu de la présente loi et les autorités compétentes désignées conformément à la loi NIS 2, aux fins de l'échange d'informations sur les risques, les menaces et les incidents liés à la cybersécurité et les

7° een beleidskader voor de coördinatie tussen de in deze wet bevoegde autoriteiten en de overeenkomstig de NIS 2 wet aangewezen bevoegde autoriteiten, met het oog op de uitwisseling van informatie over cyberbeveiligingsrisico's, cyberdreigingen en -incidenten en niet-cyber gerelateerde risico's, dreigingen en incidenten en de uitoefening van toezichthoudende taken;

8° een beschrijving van de reeds bestaande maatregelen om de uitvoering van de verplichtingen uit hoofde van Hoofdstuk 5 door kleine en middelgrote ondernemingen in de zin van de bijlage bij de Commissieaanbeveling 2003/361/EC25, die de lidstaten als kritieke entiteiten hebben aangemerkt, te vergemakkelijken

Afdeling 2. Informatie-uitwisseling

Art. 23. De autoriteit bedoeld in artikel 21, §1, het OCAD en, in voorkomend geval, de autoriteit bedoeld in artikel 16 [NIS 2 Wet] en de sectorale overheid wisselen vanuit hun eigen bevoegdheden, alle nuttige informatie uit voor het nemen van externe beschermingsmaatregelen voor de kritieke entiteiten.

Art. 24. §1. De kritieke entiteit, het contactpunt kritieke entiteit, de sectorale overheid, de autoriteit bedoeld in artikel 21, §1, het OCAD, en, in voorkomend geval, de autoriteit bedoeld in artikel 16 [NIS 2 wet], werken te allen tijde samen, vanuit hun eigen opdracht en bevoegdheden, door middel van een adequate informatie-uitwisseling betreffende de weerbaarheid van de kritieke entiteiten, teneinde te waken over een overeenstemming tussen de interne weerbaarheidsmaatregelen en de externe beschermingsmaatregelen.

§2. De sectorale overheid, de autoriteit bedoeld in artikel 21, §1, en de kritieke entiteit kunnen, in voorkomend geval, informatie uitwisselen met de gefedereerde entiteiten, voor de kritieke entiteiten die onder hun bevoegdheden vallen.

Art. 25. De Koning kan, voor een bepaalde sector, of in voorkomend geval, per deelsector, de informatie bepalen die pertinent kan zijn voor het vervullen van de opdrachten van de autoriteit bedoeld in artikel 21, §1, en van het OCAD op het vlak van de weerbaarheid van kritieke entiteiten, en de nadere regels van de toegang tot die informatie bepalen.

Art. 26. De autoriteit bedoeld in artikel 21, §1, kan aan de kritieke entiteit informatie over de dreiging en over de externe beschermingsmaatregelen overmaken die de entiteit toelaten zijn weerbaarheidsmaatregelen op gepaste wijze toe te passen en ze in overeenstemming te brengen met de externe beschermingsmaatregelen.

De autoriteit bedoeld in artikel 21, §1, kan een kopie van deze informatie aan de bevoegde sectorale overheid verzenden.

Art. 27. De sectorale overheid, de autoriteit bedoeld in artikel 21, §1, het OCAD, en de autoriteit bedoeld in artikel 16 [NIS 2 wet] beperken de toegang tot de informatie bedoeld in Hoofdstukken 4 en 5, tot de personen die er kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun

risques, menaces et incidents non liés à la cybersécurité et l'exercice des fonctions de surveillance ;

8° une description des mesures déjà en place pour faciliter la mise en œuvre des obligations du Chapitre 5 par les petites et moyennes entreprises au sens de l'annexe de la Recommandation 2003/361/CE25 de la Commission, que les États membres ont identifiées comme des entités critiques.

Section 2. Echange d'informations

Art. 23. L'autorité visée à l'article 21, §1^{er}, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi du [NIS 2] et l'autorité sectorielle s'échangent, dans le cadre de leurs compétences, toute information utile pour la prise de mesures externes de protection des entités critiques.

Art. 24. §1^{er}. L'entité critique, le point de contact de l'entité critique, l'autorité sectorielle, l'autorité visée à l'article 21, §1^{er}, l'OCAM et, le cas échéant, l'autorité visée à l'article 16 de la loi du [NIS 2] collaborent en tout temps, dans le cadre de leurs mandat et compétences, par un échange adéquat d'informations concernant la résilience de l'entité critique, afin de veiller à une concordance entre les mesures internes de résilience et les mesures externes de protection.

§2. L'autorité sectorielle, l'autorité visée à l'article 21, §1^{er}, et l'entité critique peuvent, le cas échéant, échanger des informations avec les entités fédérées, pour les entités critiques relevant de leur compétence.

Art. 25. Le Roi peut déterminer, pour un secteur déterminé ou, le cas échéant, par sous-secteur, les informations qui peuvent être pertinentes pour l'accomplissement des missions de l'autorité visée à l'article 21, §1^{er}, et de l'OCAM en matière de protection des entités critiques, ainsi que les modalités d'accès à ces informations.

Art. 26. L'autorité visée à l'article 21, §1^{er}, peut communiquer à l'entité critique des informations relatives à la menace et aux mesures externes de protection qui permettent à l'entité d'appliquer ses mesures de résilience de manière appropriée et de les mettre en concordance avec les mesures externes de protection.

L'autorité visée à l'article 21, §1^{er}, peut transmettre une copie de ces informations à l'autorité sectorielle compétente.

Art. 27. L'autorité sectorielle, l'autorité visée à l'article 21, §1^{er}, l'OCAM, et l'autorité visée à l'article 16 de la loi [NIS 2] limitent l'accès aux informations visées aux Chapitres 4 et 5, aux personnes ayant besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission, dans le contexte de la résilience des entités critiques, telle que visée dans la présente loi.

opdracht in het kader van de weerbaarheid van de kritieke entiteiten, zoals bedoeld in deze wet.

Art. 28. §1. Onverminderd artikel 25 is de kritieke entiteit gehouden tot het beroepsgeheim voor wat de inhoud van het W.P.E. betreft en mag zij enkel toegang geven tot het W.P.E. aan personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht.

De kritieke entiteit is aan hetzelfde geheim gehouden voor wat betreft alle informatie die haar ter kennis wordt gebracht met toepassing van Hoofdstuk 4, artikel 18, §6, en de artikelen 20, 24, en 26.

§2. Inbreuken op paragraaf 1 worden bestraft met de straffen voorzien bij artikel 458 van het Strafwetboek.

Art. 29. De wet van 11 april 1994 betreffende de openbaarheid van bestuur en de wet van 5 augustus 2006 betreffende de toegang van het publiek tot milieu-informatie zijn niet van toepassing op informatie, documenten of gegevens, in welke vorm ook, bedoeld in artikel 27.

Art. 30. §1. De sectorale overheid waakt erover dat minstens één iemand van zijn personeel dat toegang heeft tot informatie inzake de weerbaarheid van kritieke entiteiten, zoals bedoeld in de Hoofdstukken 4 en 5 van deze wet, beschikt over een veiligheidsmachtiging van het niveau GEHEIM, als bedoeld in Hoofdstuk III van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst. De Koning kan, voor een bepaalde sector of deelsector, nadere regels hieromtrent vastleggen.

§2 De Koning kan, op voordracht van de bevoegde Minister, de classificatie van een deel of van het geheel van het W.P.E. voorzien. Hij houdt er rekening mee dat de bevoegde personen binnen de kritieke entiteit ten allen tijde toegang hebben tot hun volledige W.P.E.

HOOFDSTUK 7 – Controle en sancties

Afdeling 1. Inspecties en audits

Art. 31. §1. De Koning stelt per sector, of, in voorkomend geval, per deelsector, een inspectiedienst aan, belast met de controle op de naleving, door de kritieke entiteiten van die sector of deelsector, van de bepalingen van deze wet en van haar uitvoeringsbesluiten.

§2. De Koning legt de nadere regels van deze controle vast. Deze nadere regels bevatten onder andere de opdrachten van de inspectiedienst, de frequentie van de controles, de minimale voorwaarden waaraan de inspectieleden moeten voldoen en de punten waarop de controle dient te gebeuren, of de rapportering die aan de sectorale overheid moeten worden gedaan.

Art. 32. De Koning legt, voor een bepaalde sector, of in voorkomend geval, per deelsector, nadere regels vast met

Art. 28. §1^{er}. Sans préjudice de l'article 25, l'entité critique est tenue au secret professionnel en ce qui concerne le contenu du P.R.E. et ne peut donner accès au P.R.E. qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès dans l'exercice de leurs fonctions ou de leur mission.

L'entité critique est tenue au même secret en ce qui concerne toutes les informations portées à sa connaissance en application du Chapitre 4, article 18, §6, et des articles 20, 24, et 26.

§ 2. Les infractions au paragraphe 1^{er} sont punies des peines prévues à l'article 458 du Code pénal.

Art. 29. La loi du 11 avril 1994 relative à la publicité de l'administration et la loi du 5 août 2006 relative à l'accès du public à l'information en matière d'environnement ne s'appliquent pas aux informations, documents ou données, sous quelque forme que ce soit, visés à l'article 27.

Art. 30. §1^{er}. L'autorité sectorielle veille à ce qu'au moins une personne de son personnel ayant accès aux informations relatives à la résilience des entités critiques, visées aux Chapitres 4 et 5 de la présente loi, dispose d'une habilitation de sécurité de niveau SECRET, telle que visée au Chapitre III de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité et au service public réglementé. Le Roi peut, pour un secteur ou sous-secteur déterminé, fixer d'autres règles à cet égard.

§2 Le Roi peut, sur proposition du Ministre compétent, prévoir la classification de tout ou partie du P.R.E. Ce faisant, il tient compte du fait que les personnes compétentes au sein de l'entité critique ont à tout moment accès à l'ensemble de leur P.R.E.

CHAPITRE 7 – Contrôle et sanctions

Section 1^{ère}. Inspections et audits

Art. 31. §1^{er}. Le Roi institue un service d'inspection par secteur, ou, le cas échéant, par sous-secteur, chargé du contrôle du respect des dispositions de la présente loi et de ses arrêtés d'exécution par les entités critiques dudit secteur ou sous-secteur.

§2. Le Roi fixe les modalités de ce contrôle. Ces modalités comprennent notamment les missions du service d'inspection, la fréquence des inspections, les conditions minimales à remplir par les membres de l'inspection et les points à inspecter, ou le rapportage à faire aux autorités sectorielles.

Art. 32. Le Roi fixe, pour un secteur particulier ou, le cas échéant, par sous-secteur, des règles supplémentaires

betrekking tot het opleggen en de uitvoering van audits ten aanzien van kritieke entiteiten

Afdeling 2. Procedure van de sancties

Art. 33. §1. Wanneer een of meer inbreuken op de eisen van de wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, kan de inspectiedienst de betrokken kritieke entiteit in gebreke stellen om zijn verplichtingen na te komen binnen een door hem vastgestelde termijn.

De termijn wordt bepaald, rekening houdend met de werkings-voorwaarden van de kritieke entiteit en met de te nemen maatregelen.

§2. De inspectiedienst kan de overtreder vooraf, op een met redenen omklede wijze, meedelen dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de inspectiedienst.

Art. 34. §1. Als de inspectiedienst vaststelt dat de kritieke entiteit geen gevolg geeft aan de ingebrekestelling binnen de vastgestelde termijn, worden de feiten vastgesteld in een door de inspectiedienst opgesteld proces-verbaal. Een kopie van het proces-verbaal wordt naar de bevoegde sectorale overheid gestuurd.

§2. De inspectiedienst stuurt het origineel van het proces-verbaal naar de Procureur des Konings.

Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.

§3. De processen-verbaal hebben bewijskracht tot het tegendeel bewezen is.

Art. 35. Inbreuken op deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke of administratieve sancties.

Art. 36. De Procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging is ingesteld.

De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten voor het verstrijken van voorgemelde termijn, behalve wanneer de Procureur des Konings vooraf meedeelt dat hij geen gevolg aan de inbreuk wenst te geven.

Wanneer de Procureur des Konings geen kennis geeft van zijn beslissing binnen de vastgestelde termijn of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.

Art. 37. In afwijking van deze afdeling kan voor de sector vervoer over water, voor inbreuken op deze wet en haar

concernant l'imposition et la réalisation d'audits à l'égard d'entités critiques.

Section 2. Procédure de sanctions

Art. 33. §1^{er}. Lorsqu'une ou plusieurs infractions aux exigences de la loi, de ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes sont constatées, le service d'inspection peut mettre en demeure l'entité critique concernée de remplir ses obligations dans un délai qu'elle fixe.

Le délai est déterminé en tenant compte des conditions d'exploitation de l'entité critique et des mesures à prendre.

§2. Le service d'inspection peut notifier préalablement au contrevenant, de manière motivée, son intention de lui adresser une mise en demeure et l'informer qu'il a le droit, dans un délai de trente jours à compter de la réception de cette information, de présenter ses moyens de défense par écrit ou de demander à être entendu. L'information est réputée avoir été reçue par le contrevenant le sixième jour après son envoi par le service d'inspection.

Art. 34. §1^{er}. Si le service d'inspection constate que l'entité critique ne se conforme pas à la mise en demeure dans le délai imparti, les faits sont constatés dans un rapport officiel rédigé par le service d'inspection. Une copie du rapport officiel est envoyée à l'autorité sectorielle compétente.

§2. Le service d'inspection envoie l'original du procès-verbal au Procureur du Roi.

En même temps, une copie du procès-verbal est envoyée à l'auteur de l'infraction.

§3. Les procès-verbaux ont valeur probante jusqu'à preuve du contraire.

Art. 35. Les violations de cette loi ou de ses décrets d'application peuvent donner lieu à des sanctions pénales ou administratives.

Art. 36. Le Procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour informer l'autorité sectorielle que des poursuites pénales ont été engagées.

L'autorité sectorielle ne peut entamer la procédure d'imposition d'une amende administrative avant l'expiration du délai susmentionné, à moins que le Procureur ne notifie au préalable qu'il ne souhaite pas donner suite à l'infraction.

Si le Procureur du Roi ne notifie pas sa décision dans le délai imparti ou s'il renonce aux poursuites pénales, l'autorité sectorielle peut décider d'engager la procédure administrative.

Art. 37. Par dérogation à la présente section, pour le secteur du transport par voie d'eau, en cas d'infraction à la

uitvoeringsbesluiten, een administratieve geldboete worden opgelegd met toepassing boek 4 van het Belgisch scheepvaartwetboek en de wet van 25 december 2016 tot instelling van administratieve geldboetes van toepassing in geval van inbreuken op de scheepvaartwetten. De minimale en maximale bedragen van de administratieve geldboete stemmen overeen met de respectieve minimale en maximale bedragen voorzien in afdeling 4.

Afdeling 3. Strafrechtelijke sancties

Art. 38. §1. Wordt gestraft met een gevangenisstraf van acht dagen tot een jaar en met een geldboete van 26 euro tot 10.000 euro of met één van die straffen alleen, de kritieke entiteit die de verplichtingen opgelegd door of krachtens deze wet betreffende de interne weerbaarheidsmaatregelen uit Hoofdstuk 3 en de uitwisseling van informatie uit Hoofdstuk 4, Afdeling 2, niet naleeft.

In geval van herhaling wordt de geldboete verdubbeld en wordt de overtreder gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.

§2. Wordt gestraft met gevangenisstraf van acht dagen tot een maand en met geldboete van 26 euro tot 1.000 euro of met één van die straffen alleen, eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt.

In geval van herhaling, wordt de geldboete verdubbeld en de overtreder gestraft met een gevangenisstraf van vijftien dagen tot een jaar.

§3. De bepalingen van Boek I van het Strafwetboek, met inbegrip van Hoofdstuk VII en artikel 85, zijn van toepassing op de vermelde inbreuken.

Afdeling 4. Administratieve sancties

Art. 39. §1. Elke inbreuk op deze wet, op de uitvoeringsbesluiten of op de administratieve beslissingen die krachtens deze wet genomen worden, kan aanleiding geven tot een administratieve sanctie.

§2. Niet-naleving van de verplichtingen betreffende informatie-uitwisseling opgelegd krachtens artikel 9, §3, wordt bestraft met een geldboete van 500 tot 75 000 euro.

§3. Niet-naleving van de verplichtingen betreffende de weerbaarheidsmaatregelen opgelegd door of krachtens Hoofdstuk 5 van deze wet, wordt bestraft met een geldboete van 500 tot 100 000 euro.

§4. Niet-naleving van de verplichtingen betreffende de uitwisseling van informatie uit Hoofdstuk 6, Afdeling 2, worden bestraft met een geldboete van 500 tot 100 000 euro.

§5. Niet-naleving van de verplichtingen betreffende de uitvoering van inspecties en audits opgelegd krachtens

présente loi et à ses arrêtés d'exécution, une amende administrative peut être imposée en application du livre 4 du Code de la marine marchande et de la loi du 25 décembre 2016 fixant les amendes administratives applicables en cas d'infraction à la législation sur la marine marchande. Les montants minimum et maximum de l'amende administrative correspondent aux montants minimum et maximum respectifs prévus à la section 4.

Section 3. Sanctions pénales

Art. 38. §1^{er}. Est punie d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 10.000 euros, ou de l'une de ces peines seulement, l'entité critique qui ne respecte pas les obligations imposées par ou en vertu de la présente loi, relatives aux mesures internes de résilience prévues au Chapitre 2 et à l'échange d'informations prévu au Chapitre 4, Section 2.

En cas de récidive, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans.

§2. Est puni d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 euros à 1.000 euros, ou de l'une de ces peines seulement, quiconque empêche ou entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou communique sciemment des informations inexacts ou incomplètes.

En cas de récidive, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à un an.

§3. Les dispositions du Livre 1^{er} du Code pénal, en ce compris le Chapitre VII et l'article 85, sont applicables aux dites infractions.

Section 4. Sanctions administratives

Art. 39. §1^{er}. Toute violation de la présente loi, des décrets d'application ou des décisions administratives prises en vertu de la présente loi peut donner lieu à une sanction administrative.

§2. Le non-respect des obligations en matière d'échange d'informations imposées en vertu de l'article 9, §3, est puni d'une amende allant de 500 à 75 000 euros.

§3. Le non-respect des obligations relatives aux mesures de résilience imposées par ou en vertu du chapitre 5 de la présente loi est puni d'une amende de 500 à 100 000 euros.

§4. Le non-respect des obligations relatives à l'échange d'informations prévues au Chapitre 6, Section 2, est puni d'une amende de 500 à 100 000 euros.

§5. Le non-respect des obligations relatives à la conduite des inspections et des audits imposées en vertu du Chapitre

Hoofdstuk 7 van deze wet, wordt bestraft met een geldboete van 500 tot 125 000 euro.

Eenieder die de uitvoering van de controle uitgevoerd door de leden van de inspectiedienst vrijwillig verhindert of belemmert, die informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt bestraft met een geldboete van 500 tot 125 000 euro.

Art. 40. §1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§2. De sectorale overheid bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de dertig dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te zijn ontvangen door de overtreder op de zesde dag na de verzending ervan door de sectorale overheid.

§3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen dezelfde termijn, kan de sectorale overheid een in artikel 39 bedoelde administratieve sanctie opleggen.

§4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.

De administratieve geldboete wordt verdubbeld in geval van herhaling binnen een termijn van drie jaar.

§5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 41. De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.

Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.

Art. 42. §1. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de sectorale overheid of door een daartoe gemachtigd personeelslid.

§2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

7 de la présente loi est puni d'une amende de 500 à 125 000 euros.

Quiconque empêche ou gêne volontairement la réalisation de l'inspection effectuée par les membres du service d'inspection, qui refuse de communiquer les informations qui lui sont demandées à la suite de cette inspection, ou qui communique délibérément des informations erronées ou incomplètes, est puni d'une amende de 500 à 125 000 euros.

Art. 40. §1^{er}. La décision d'infliger une amende administrative est motivée. Elle indique également le montant de l'amende administrative et les infractions visées.

§2. L'autorité sectorielle communique au préalable au contrevenant sa proposition motivée de sanction administrative et l'informe qu'il a le droit, dans un délai de trente jours à compter de la réception de la proposition, de présenter ses moyens de défense par écrit ou de demander à être entendu. La proposition est réputée avoir été reçue par le contrevenant le sixième jour suivant son envoi par l'autorité sectorielle.

§3. En tenant compte des moyens de défense soulevés dans le délai visé au paragraphe 2 ou en l'absence de réponse du contrevenant dans le même délai, l'autorité sectorielle peut imposer une sanction administrative visée à l'article 39.

§4. L'amende administrative est proportionnelle à la gravité, à la durée, aux moyens utilisés, aux dommages causés et aux circonstances de l'infraction.

L'amende administrative est doublée en cas de récidive dans un délai de trois ans.

§5. La concomitance de plusieurs infractions peut donner lieu à une seule amende administrative proportionnelle à la gravité de l'infraction dans son ensemble.

Art. 41. La décision est notifiée au contrevenant par lettre recommandée.

Une demande de paiement de l'amende dans un délai d'un mois est jointe à la décision.

Art. 42. §1^{er}. Si le contrevenant ne paie pas l'amende administrative dans le délai imparti, la décision d'imposer une amende administrative est exécutoire et l'autorité sectorielle peut émettre une injonction.

L'injonction est délivrée par le représentant légal de l'autorité sectorielle ou par un agent habilité.

§2. L'injonction est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un ordre de payer dans les vingt-quatre heures sous peine d'exécution par saisie, ainsi qu'un relevé des sommes réclamées et une copie de la déclaration constatant la force exécutoire.

§3. L'auteur de l'infraction peut faire opposition à l'injonction auprès du juge des saisies.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het dient gedaan te worden door middel van een dagvaarding aan de sectorale overheid bij deurwaarderexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van Hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging van het dwangbevel, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§4. De sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§5. De betekeningkosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Deze kosten worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 43. De sectorale overheid kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

De betaling volgens de administratieve procedures doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.

HOOFDSTUK 8 – Sector overheid

Art. 44. De Koning bepaalt voor de sector overheid, op voordracht van de sectoraal bevoegde Minister, de wijze van uitvoering van de verplichtingen uit tenminste onderstaande bepalingen uit deze wet:

- Artikel 7;
- Artikel 9, §1 en §4;
- Artikel 10;
- Artikel 12, §3;
- Artikel 13;
- Artikel 14;
- Artikel 16;
- Artikel 17;
- Artikel 18, §§1 t.e.m. 5;
- Artikel 19;
- Artikel 20;
- Artikel 31;
- Artikelen 32.

Sous peine de nullité, l'opposition est motivée. Elle doit être faite par voie d'assignation à l'autorité sectorielle par exploit d'huissier dans les quinze jours à compter de la signification de l'injonction.

Les dispositions du Chapitre VIII de la première partie du Code judiciaire s'appliquent à ce délai, y compris les prolongations prévues à l'article 50, deuxième alinéa, et à l'article 55 de ce Code.

Le recours à l'opposition à l'injonction suspend l'exécution de l'injonction, ainsi que la prescription des créances visées par l'injonction, jusqu'à ce qu'il soit statué sur son bien-fondé. Les saisies déjà effectuées maintiennent leur caractère conservatoire.

§4. L'autorité sectorielle peut ordonner des saisies conservatoires et exécuter l'injonction en utilisant les moyens d'exécution prévus dans la Cinquième partie du Code Judiciaire.

Les paiements partiels effectués à la suite de la signification d'une injonction ne font pas obstacle à la poursuite de l'action publique.

§5. Les frais de signification de l'injonction ainsi que les frais d'exécution ou de mesures conservatoires sont à la charge du contrevenant.

Ces frais sont déterminés selon les règles applicables aux actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 43. L'autorité sectorielle ne peut imposer une amende administrative après l'expiration d'une période de trois ans à compter du jour où l'infraction a été commise.

Le paiement dans le cadre de procédures administratives rend également caduque la possibilité de poursuites pénales pour les infractions en question.

CHAPITRE 8 – Secteur des administrations publiques

Art. 44. Le Roi détermine pour le secteur des administrations publiques, sur proposition du Ministre sectoriel compétent, les modalités d'exécution des obligations découlant au moins des dispositions suivantes de la présente loi:

- Article 7;
- Article 9, §1^{er} et §4;
- Article 10;
- Article 12, §3;
- Article 13;
- Article 14;
- Article 16;
- Article 17;
- Article 18, §§ 1 à 5;
- Article 19;
- Article 20;
- Article 31;
- Article 32.

HOOFDSTUK 9 – Diverse bepalingen

Afdeling 1. Wijzigingen van de wet van 13 juni 2005 betreffende de elektronische communicatie

Art. 45. In artikel 28/3, §2, eerste lid, de bepaling onder 4° van de wet van 13 juni 2005 betreffende de elektronische communicatie, ingevoegd bij wet van 21 december 2021, worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

Art. 46. In artikel 105, §2, de bepaling onder 2° van dezelfde wet, ingevoegd bij wet van 17 februari 2022, worden de woorden "exploitant van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "kritieke entiteit in de zin van de wet [datum] betreffende de weerbaarheid van kritieke entiteiten".

Art. 47. In artikel 126/3, §3, de bepaling onder j), van dezelfde wet, ingevoegd bij wet van 20 juli 2022, worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en de uitvoeringsbesluiten ervan" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 2. Wijzigingen van de wet van 14 februari 2023 houdende de instemming met het samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen

Art. 48 In artikel 4, van de wet van 14 februari 2023 houdende de instemming met het samenwerkingsakkoord van 30 november 2022 tussen de Federale Staat, het Vlaamse Gewest, het Waals Gewest, het Brussels Hoofdstedelijk Gewest, de Vlaamse Gemeenschap, de Franse Gemeenschap, de Duitstalige Gemeenschap, de Franse Gemeenschapscommissie en de Gemeenschappelijke Gemeenschapscommissie tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, 2°, de bepaling onder a) worden de woorden "kritieke infrastructuur" vervangen door de woorden "kritieke entiteiten";

2° in paragraaf 2, 2°, de bepaling onder a) wordt het zinsdeel "in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, en in het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer" vervangen als volgt: "in de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

CHAPITRE 9 – Dispositions diverses

Section 1^{ère}. Modification de la loi du 13 juin 2005 relative aux communications électroniques

Art. 45. À l'article 28/3, §2, premier alinéa, la disposition sous 4° de la loi du 13 juin 2005 relative aux communications électroniques, insérée par la loi du 21 décembre 2021, les mots « la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « la loi du [date] relative à la résilience des entités critiques »;

Art. 46. À l'article 105, §2, la disposition sous 2° de la même loi, insérée par la loi du 17 février 2022, les mots « exploitant d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « entité critique au sens de la loi [date] relative à la résilience des entités critiques ».

Art. 47. À l'article 126/3, paragraphe 3, la disposition sous j), de la même loi, insérée par la loi du 20 juillet 2022, les mots « la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et leurs décrets d'application » sont remplacés par les mots « la loi du [date] relative à la résilience des entités critiques ».

Section 2. Modification de la loi du 14 février 2023 portant approbation de l'accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire mixte instituant un mécanisme de filtrage des investissements directs étrangers

Art. 48. A l'article 4 de la loi du 14 février 2023 portant approbation de l'accord de coopération du 30 novembre 2022 entre l'État fédéral, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire française et la Commission communautaire mixte instituant un mécanisme de filtrage des investissements directs étrangers, sont apportées les modifications suivantes:

1° au paragraphe 2, 2°, la disposition prévue au point a), les mots « infrastructures critiques » sont remplacés par les mots « entités critiques »;

2° au paragraphe 2, 2°, la disposition prévue au point a), le membre de phrase « dans la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, et dans l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien » est remplacé comme suit : « dans la loi du [date] relative à la résilience des entités critiques ».

Art. 49. In artikel 7 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° In paragraaf 4 worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

2° in paragraaf 4 worden de woorden "kritieke infrastructuur" vervangen door de woorden "kritieke entiteiten".

Afdeling 3. Wijziging van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit

Art. 50 In artikel 3, §3, van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit worden de woorden "in artikel 6, 2°, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, in artikel 3, 3°, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur en in artikel 2, eerste lid, 1°, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer" vervangen door de woorden "in artikel 3, 2°, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Art. 51. In artikel 6 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de paragrafen 2 en 3 worden de woorden "de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur" vervangen door de woorden "de artikelen 3, 2°, en 31, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

2° in dezelfde paragrafen worden de woorden "in artikel 7, § 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" telkens vervangen door de woorden "in artikel 15, § 2, van de wet van [...] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

3° in paragraaf 3 worden de woorden "en 15, § 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer" opgeheven.

4° in dezelfde paragraaf worden de woorden "de artikelen 20, 21, § 1, en 33, van de voormelde wet van 7 april 2019" vervangen door de woorden "de artikel 30 van de voormelde wet van [...]".

Art. 52. In artikel 16, §4, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "artikel 13 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur" vervangen

Art. 49. Les modifications suivantes sont apportées à l'article 7 de la même loi:

1° Au paragraphe 4, les mots « la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « la loi du [date] relative à la résilience des entités critiques »;

2° au paragraphe 4, les mots « infrastructures critiques » sont remplacés par les mots « entités critiques ».

Section 3. Modification de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l'information et la communication et désignant une autorité nationale de certification de cybersécurité

Art. 50. Dans l'article 3, §3, de la loi du 20 juillet 2022 relative à la certification de la cybersécurité des technologies de l'information et de la communication et désignant une autorité nationale de certification de cybersécurité, les mots « l'article 6, 2°, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, de l'article 3, 3°, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques et de l'article 2, alinéa 1^{er}, 1°, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien » sont remplacés par les mots

« à l'article 3, 2°, de la loi du [date] relative à la résilience des entités critiques ».

Art. 51. A l'article 6 de la même loi, les modifications suivantes sont apportées:

1° aux paragraphes 2 et 3, les mots « articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « articles 3, 2° et 31 de la loi du [date] relative à la résilience des entités critiques »;

2° dans les mêmes paragraphes, les mots « à l'article 7, § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » sont chaque fois remplacés par les mots « ou à l'article 15, § 2, de la loi du [...] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » ;

3° au paragraphe 3, les mots « et 15, § 1 à 3, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien » sont supprimés.

4° dans le même paragraphe, les mots « aux articles 20, 21, § 1^{er}, et 33, de la loi précitée du 7 avril 2019 » sont remplacés par les mots « à l'article 30 de la loi précitée du [...] ».

Art. 52. A l'article 16, § 4, de la même loi, les modifications suivantes sont apportées:

1° dans le premier alinéa, les mots « article 13 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots

door de woorden "artikel 18 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

2° in het eerste lid worden de woorden "de artikelen 3, 3°, en 24, § 2, van de voormelde wet van 1 juli 2011" vervangen door de woorden "de artikelen 3, 2° en 31, van de voormelde wet van [datum]";

3° in het eerste lid worden de woorden "de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en", "en in artikel 7, § 3 en 5, van de voormelde wet van 7 april 2019", " , een aanbieder van essentiële diensten of een digitaal dienstverlener" en "of de voormelde wet van 7 april 2019" opgeheven;

4° in het tweede lid worden de woorden "kritieke infrastructuur" vervangen door de woorden "kritieke entiteiten";

5° in het tweede lid wordt de bepaling onder 2° vervangen als volgt: "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

Art. 53. In artikel 17, § 3, van dezelfde wet, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden "en de artikelen 20, 21, § 1, en 33 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" opgeheven;

2° in hetzelfde lid worden de woorden "n in artikel 7, § 3 en 5, van de voormelde wet van 7 april 2019" opgeheven;

3° in hetzelfde lid worden de woorden " , aanbieder van essentiële diensten of digitaal dienstverlener" opgeheven;

4° in hetzelfde lid worden de woorden "of de voormelde wet van 7 april 2019" opgeheven;

5° in het tweede lid, in de bepaling onder 2° worden de woorden " , de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" opgeheven;

Art. 54. In artikel 36, §1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 4° worden de woorden "de artikelen 3, 3°, en 24, § 2, van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur, in artikel 7, § 3 en 5, van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" vervangen door de woorden "de artikelen 3, 2° en 31, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten of de artikel 15, § 2, van de wet van [...] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid";

2° in de bepaling onder 4° worden de woorden "en 15, § 1 tot 3, van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuur in de deelsector van het luchtvervoer" opgeheven;

3° in de bepaling onder 4° worden de woorden "in de artikelen 7, § 3, eerste lid, § 5, en 42, § 1, van de voormelde wet van 7 april 2019" vervangen door de woorden "in artikelen 15, § 2, en 24 van de voormelde wet van [...]".

« article 18 de la loi du [date] relative à la résilience des entités critiques »;

2° dans le même alinéa, les mots « articles 3, 3° et 24, § 2, de la loi du 1er juillet 2011 précitée » sont remplacés par les mots « articles 3, 2° et 31 de la loi du [date] précitée » ;

3° dans le premier alinéa, les mots « des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et », « et à l'article 7, § 3 et 5, de la loi précitée du 7 avril 2019 », « , d'un opérateur de services essentiels ou d'un fournisseur de service numérique » et « ou de la loi précitée du 7 avril 2019 » sont abrogés;

4° dans le deuxième alinéa, les mots « infrastructures critiques » sont remplacés par les mots « entités critiques »;

5° dans le deuxième alinéa, le 2° est remplacé par ce qui suit : « la loi du [date] relative à la résilience des entités critiques »;

Art. 53. A l'article 17, § 3, de la même loi, les modifications suivantes sont apportées :

1° dans l'alinéa 1er, les mots « et des articles 20, 21, § 1er, et 33 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » sont abrogés;

2° dans le même alinéa, les mots « et à l'article 7, § 3 et 5, de la loi précitée du 7 avril 2019 » sont abrogés;

3° dans le même alinéa, les mots « , d'un opérateur de services essentiels ou d'un fournisseur de service numérique » sont abrogés ;

4° dans le même alinéa, les mots « ou de la loi précitée du 7 avril 2019 » sont abrogés

5° dans le deuxième alinéa, le 2°, les mots « , de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » sont abrogés.

Art. 54. A l'article 36, § 1er, de la même loi, les modifications suivantes sont apportées:

1° dans le 4°, les mots « articles 3, 3°, et 24, § 2, de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, à l'article 7, § 3 et 5, de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » sont remplacés par les mots « articles 3, 2° et 31, de la loi du [date] relative à la résilience des entités critiques ou à l'article 15, § 2, de la loi du [...] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique » ;

2° dans le 4°, les mots « en 15, § 1 à 3, de l'arrêté royal du 2 décembre 2011 relatif aux infrastructures critiques dans le sous-secteur du transport aérien » sont abrogés ;

3° dans le 4°, les mots « aux articles 7, § 3, alinéa 1er, § 5, et 42, § 1er, de la loi précitée du 7 avril 2019 » sont remplacés par les mots « aux articles 15, § 2, et 24 de la loi précitée du [...] ».

Afdeling 4. Wijziging van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 55. In artikel 14 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, laatstelijk gewijzigd bij wet van 20 juli 2022, worden de volgende wijzigingen aangebracht:

1° In paragraaf 1, eerste lid, worden de volgende wijzigingen aangebracht:

a) in de eerste zin worden de woorden "met betrekking tot de sectoren elektronische communicatie en digitale infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuur" vervangen door de woorden "met betrekking tot de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, in de zin van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

b) in de bepaling onder 3°, wordt de bepaling onder g) vervangen als volgt:

"de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten, wat de sector digitale infrastructuur, met uitzondering van de verleners van vertrouwensdiensten, betreft;

2° de bepaling onder 7° in paragraaf 2, eerste lid, wordt opgeheven.

Afdeling 5. Wijziging van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 56. In artikel 36/14 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, worden in de bepaling onder 20° de woorden "artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur zults vereist" vervangen door de woorden "artikel 24 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten zults vereist".

Art. 57. In artikel 36/49 van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "kritieke infrastructuur" worden vervangen door de woorden "kritieke entiteit";

2° de woorden "wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuur" worden vervangen door de woorden "wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 6. Wijziging van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen

Art. 58. In artikel 15/2sexies, §3, van de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

Section 4. Modification de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications

Art. 55. A l'article 14, de la loi du 17 janvier 2003 relative au statut du régulateur du secteur belge des postes et télécommunications, modifiée en dernier lieu par la loi du 20 juillet 2022, les modifications suivantes sont apportées :

1° Au paragraphe 1^{er}, premier alinéa, les modifications suivantes sont apportées:

a) dans la première phrase, les mots « relevant des secteurs des communications électroniques et des infrastructures numériques aux sens de la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « relevant du secteur des infrastructures numériques, à l'exception des fournisseurs de services de confiance, au sens de la loi du [date] relative à la résilience des entités critiques » ;

b) dans la disposition sous 3°, la dispositions sous g) est remplacée comme suit :

« la loi du [date] relative à la résilience des entités critiques, en ce qui concerne le secteur de l'infrastructure numérique, à l'exception des fournisseurs de services de confiance »;

2° la disposition prévue au paragraphe 2, point 1, sous 7° est abrogée.

Section 5. Modification de la loi du 22 février 1998 portant le statut organique de la Banque nationale de Belgique

Art. 56. A l'article 36/14 de la loi du 22 février 1998 portant statut organique de la Banque nationale de Belgique, dans la disposition du 20°, les mots « l'article 19 de la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques l'exige » sont remplacés par les mots « l'article 24 de la loi du [date] relative à la résilience des entités critiques l'exige ».

Art. 57. A l'article 36/49 de la même loi, les modifications suivantes sont apportées:

1° les mots « infrastructure critique » sont remplacés par les mots « entité critique »;

2° les mots « loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « loi du [date] relative à la résilience des entités critiques ».

Section 6. Modification de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations

Art. 58. A l'article 15/2sexies, §3, de la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, modifiée en dernier lieu par la loi du 31 juillet 2017, sont apportées les modifications suivantes:

1° in de bepaling onder 4° worden de woorden "kritieke nationale infrastructuur" vervangen door de woorden "kritieke entiteit";

2° in de bepaling onder 4° worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 7. Wijziging van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt

Art. 59. In artikel 14/1, §3, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt, laatstelijk gewijzigd bij de wet van 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 4° worden de woorden "kritieke nationale infrastructuur" vervangen door de woorden "kritieke entiteit";

2° in de bepaling onder 4° worden de woorden "de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren" vervangen door de woorden "de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 8. Wijziging van het Strafwetboek

Art. 60. In artikel 546/2, §1, van het Strafwetboek, ingevoegd bij wet van 20 mei 2016, wordt de bepaling onder 6° vervangen als volgt:

"6° Indien een kritieke entiteit, in de zin van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten werd binnengegaan of binnengedrongen".

Art. 61. In artikel 550ter, §1, van het Strafwetboek, ingevoegd bij wet van 28 november 2000 en gewijzigd bij de wet van 6 juli 2017, wordt het derde lid vervangen als volgt:

"Dezelfde straf wordt toegepast wanneer het in het eerste lid bedoelde misdrijf gepleegd wordt tegen een informatiesysteem van een kritieke entiteit zoals bedoeld in artikel 3, 3°, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 9. Wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle

Art. 62. In artikel 15bis, lid 1, van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, ingevoegd door de wet van 7 april 2019, worden de volgende wijzigingen aangebracht:

1°) de woorden "artikel 24 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren" worden vervangen door de woorden "artikel 31 van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten";

1° dans la disposition sous 4°, les mots « infrastructure nationale critique » sont remplacés par les mots « entité critique »;

2° dans la disposition sous 4°, les mots « la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « la loi du [date] relative à la résilience des entités critiques ».

Section 7. Modification de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité

Art. 59. A l'article 14/1, §3, de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, modifiée en dernier lieu par la loi du 31 juillet 2017, sont apportées les modifications suivantes:

1° dans la disposition sous 4°, les mots « infrastructure nationale critique » sont remplacés par les mots « entité critique »;

2° dans la disposition sous 4°, les mots « la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « la loi du [date] relative à la résilience des entités critiques ».

Section 8. Modification du Code Pénal

Art. 60. A l'article 546/2, §1^{er}, du Code pénal, inséré par la loi du 20 mai 2016, la disposition sous 6° est remplacée comme suit :

« 6° Si une entité critique, au sens de la loi du [date] sur la résilience des entités critiques, a fait l'objet d'une entrée ou d'une intrusion ».

Art. 61. A l'article 550ter, § 1^{er}, du Code pénal, inséré par la loi du 28 novembre 2000 et modifié par la loi du 6 juillet 2017, le troisième alinéa est remplacé comme suit :

« La même peine est appliquée lorsque l'infraction visée à l'alinéa 1^{er} est commise à l'encontre d'un système d'information d'une entité critique telle que visée à l'article 3, 3°, de la loi du [date] relative à la résilience des entités critiques ».

Section 9. Modification de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 62. À l'article 15bis, alinéa 1, de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, inséré par la loi du 7 avril 2019, les modifications suivantes sont apportées :

1°) les mots « l'article 24 de la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques » sont remplacés par les mots « l'article 31 de la loi du [date] relative à la résilience des entités critiques » ;

2°) de worden "aangeduid als kritieke infrastructuur krachtens bovengenoemde wet van 1 juli 2011" worden vervangen door de woorden "aangeduid als kritieke entiteit krachtens de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten".

Afdeling 10. Wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging

Art. 63. In artikel 6, §1, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, gewijzigd bij de wet van 31 mei 2022, wordt een derde lid als volgt ingevoegd:

"Onverminderd de verplichtingen die zijn vastgelegd in de internationale instrumenten waardoor zij gebonden zijn, zijn de ondersteunende diensten verplicht om ambtshalve of op verzoek van de directeur van het OCAD, de persoonsgegevens bedoeld in artikel 142 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en de informatie waarover zij beschikken in het kader van hun wettelijke opdrachten en die relevant blijkt met het oog op de verwezenlijking van de doelstellingen van de dreigingsanalyse als bedoeld in artikel 8, §2, van de wet van [datum] betreffende de weerbaarheid van kritieke entiteiten, te communiceren."

Afdeling 11. Wijziging van de wet van [...] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Art. 64. In artikel 3, § 4, van de wet van [...] tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid worden de woorden "exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren" vervangen door de woorden "kritieke entiteiten als bedoeld in de wet van [...] betreffende de weerbaarheid van kritieke entiteiten".

Art. 65. In artikel 8 van dezelfde wet wordt 43° vervangen door:

"43° "wet van [xx xxxx xxxx]": de wet van [...] betreffende de weerbaarheid van kritieke entiteiten".

Art. 66. In artikel 15, § 2, tweede lid, van dezelfde wet worden de woorden "wet van 1 juli 2011" vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 67. In artikel 25 van dezelfde wet worden de volgende wijzigingen aangebracht:

- 1° in paragraaf 2 worden de woorden "wet van 1 juli 2011" vervangen door de woorden "wet van [xx xxxx xxxx]";
- 2° in paragraaf 4 wordt "wet van 1 juli 2011" vervangen door "wet van [xx xxxx xxxx]";
- 3° in dezelfde paragraaf worden de woorden "exploitanten van infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur zijn aangemerkt" vervangen door de woorden "kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]".

2°) les mots « désignés comme infrastructure critique en vertu de la loi du 1^{er} juillet 2011 susmentionnée » sont remplacés par les mots « désignés comme entité critique en vertu de la loi du [date] relative à la résilience des entités critiques ».

Section 10. Modification de la loi du 10 juillet 2006 relative à l'analyse de la menace

Art. 63. À l'article 6, § 1^{er} de la loi du 10 juillet 2006 relative à l'analyse de la menace, modifié par la loi du 31 mai 2022, est inséré un alinéa 3 rédigé comme suit :

« Sans préjudice des obligations prévues dans les instruments internationaux qui les lient, les services d'appui sont tenus de communiquer à l'OCAM, d'office ou à la demande de son directeur, les données à caractère personnel visées à l'article 142 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'article 8, § 2, de la loi du [date] relative à la résilience des entités critiques. ».

Section 11. Modification de la loi du [...] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Art. 64. Dans l'article 3, § 4, de la loi du [...] établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, les mots "exploitants d'une infrastructure critique au sens de la loi du 1^{er} juillet 2011 relative à la sécurité et la protection des infrastructures critiques" sont remplacés par les mots "entités critiques au sens de la loi du [...] relative à la résilience des entités critiques".

Art. 65. Dans l'article 8 de la même loi, le 43° est remplacé par ce qui suit:

"43° "loi du [xx xxxx xxxx]": la loi du [...] relative à la résilience des entités critiques"

Art. 66. Dans l'article 15, § 2, alinéa 2, de la même loi, les mots "loi du 1^{er} juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 67. A l'article 25 de la même loi, les modifications suivantes sont apportées:

- 1° dans le paragraphe 2, les mots "loi du 1^{er} juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]";
- 2° dans le paragraphe 4, les mots "loi du 1^{er} juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]";
- 3° dans le même paragraphe, les mots "exploitants d'infrastructures recensées en tant qu'infrastructures critiques en vertu de la loi du 1^{er} juillet 2011" sont remplacés par les mots "entités critiques au sens de la loi du [xx xxxx xxxx]".

Art. 68. In artikel 28, § 2, 7°, van dezelfde wet worden de woorden "wet van 1 juli 2011" vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 69. In artikel 37, § 5, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "wet van 1 juli 2011" worden vervangen door de woorden "wet van [xx xxxx xxxx]";

2° de woorden "exploitanten van infrastructuur die uit hoofde van de wet van 1 juli 2011 als kritieke infrastructuur zijn aangemerkt" worden vervangen door de woorden "kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]".

Art. 70. In artikel 40, § 1, tweede lid, van dezelfde wet worden de woorden "exploitanten van een kritieke infrastructuur als bedoeld in de wet van 1 juli 2011" vervangen door de woorden "kritieke entiteiten als bedoeld in de wet van [xx xxxx xxxx]".

Art. 71. In artikel 45, § 1, van dezelfde wet worden de volgende wijzigingen aangebracht:

1° de woorden "dat een exploitant van een infrastructuur die op grond van de wet van 1 juli 2011 als kritieke infrastructuur wordt aangemerkt" worden vervangen door de woorden "dat een kritieke entiteit als bedoeld in de wet van [xx xxxx xxxx]";

2° de woorden "een exploitant van een infrastructuur die is aangemerkt als kritieke infrastructuur uit hoofde van de wet van 1 juli 2011" worden vervangen door de woorden "een kritieke entiteit als bedoeld in de wet van [xx xxxx xxxx]";

3° de woorden "wet van 1 juli 2011" worden telkens vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 72. In artikel 67, 5°, van dezelfde wet worden de woorden "wet van 1 juli 2011" telkens vervangen door de woorden "wet van [xx xxxx xxxx]".

Art. 73. In artikel 68, 5°, van dezelfde wet worden de woorden "wet van 1 juli 2011" vervangen door de woorden "wet van [xx xxxx xxxx]".

HOOFDSTUK 10 – Slotbepalingen

Art. 74. De Koning neemt, bij een in Ministerraad overlegd besluit, de nodige maatregelen, met inbegrip van de opheffing, de aanvulling, de wijziging of de vervanging van wetsbepalingen, om de omzetting van de Europese richtlijnen betreffende de kritieke entiteiten te verzekeren.

Hij kan, bij een in Ministerraad overlegd besluit, de bepalingen van Hoofdstukken 4 tot en met 7 en de uitvoeringsbesluiten ervan volledig of gedeeltelijk van toepassing maken op andere sectoren dan diegene bedoeld in de Bijlage.

Art. 75. De wet van 1 juli 2011 betreffende de bescherming en beveiliging van kritieke infrastructuur wordt opgeheven.

Art. 76. §1. Entiteiten die op grond van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur werden aangeduid als exploitanten van een Europese of nationale kritieke infrastructuur,

Art. 68. Dans l'article 28, § 2, 7°, de la même loi, les mots "loi du 1er juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 69. A l'article 37, § 5, de la même loi, les modifications suivantes sont apportées:

1° les mots "loi du 1er juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]";

2° les mots "exploitants d'infrastructures identifiées comme infrastructures critiques en vertu de la loi du 1er juillet 2011" sont remplacés par les mots "entités critiques au sens de la loi du [xx xxxx xxxx]".

Art. 70. Dans l'article 40, § 1er, alinéa 2, de la même loi, les mots "exploitants d'une infrastructure critique au sens de la loi du 1er juillet 2011" sont remplacés par les mots "entités critiques au sens de la loi du [xx xxxx xxxx]".

Art. 71. A l'article 45, § 1er, de la même loi, les modifications suivantes sont apportées:

1° les mots "qu'un exploitant d'une infrastructure définie comme critique en vertu de la loi du 1er juillet 2011" sont remplacés par les mots "qu'une entité critique au sens de la loi du [xx xxxx xxxx]";

2° les mots "d'un exploitant d'une infrastructure qui est définie comme infrastructure critique en vertu de la loi du 1er juillet 2011" sont remplacés par les mots "d'une entité critique au sens de la loi du [xx xxxx xxxx]";

3° les mots "loi du 1er juillet 2011" sont à chaque fois remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 72. Dans l'article 67, 5°, de la même loi, les mots "loi du 1er juillet 2011" sont à chaque fois remplacés par les mots "loi du [xx xxxx xxxx]".

Art. 73. Dans l'article 68, 5°, de la même loi, les mots "loi du 1er juillet 2011" sont remplacés par les mots "loi du [xx xxxx xxxx]".

CHAPITRE 10 – Dispositions finales

Art. 74. Le Roi prend, par arrêté délibéré en Conseil des ministres, les mesures nécessaires, y compris l'abrogation, l'ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition des directives européennes concernant les entités critiques.

Il peut, par arrêté délibéré en Conseil des ministres, rendre applicables en tout ou en partie les dispositions des Chapitres 4 à 7 inclus et les arrêtés d'exécution à d'autres secteurs que ceux visés en Annexe.

Art. 75. La loi du 1er juillet 2011 relative à la protection et à la sécurité des infrastructures critiques est abrogée.

Art. 76. §1^{er}. Les entités qui ont été désignées comme exploitants d'une infrastructure critique européenne ou nationale en vertu de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques seront automatiquement considérées le 17 juillet 2026

worden op 17 juli 2026 van rechtswege beschouwd als kritieke entiteiten zoals bedoeld in artikel 12 van deze wet.

De lijst van kritieke infrastructuren zoals opgesteld volgens de wet van 1 juli 2011 zal, behoudens aanpassingen, voldoen aan artikel 12 van deze wet.

§2. De entiteiten bedoeld in paragraaf 1, lid 1, blijven tot 17 mei 2027 gehouden aan de verplichtingen uit de artikelen 13, 13/1, 13/2, 14, 24 en 25 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren, zoals deze op dat ogenblik van toepassing waren.

Art. 77. Met uitzondering van sectoren waarin nog geen kritieke entiteiten waren aangewezen voor de inwerkingtreding van deze wet, worden alle dreigingsanalyses geacht geldig te zijn voor een periode van maximaal vier jaar, overeenkomstig artikel 8, zelfs indien de datum waarop zij werden uitgevoerd voor de inwerkingtreding van deze wet valt.

Art. 78. Deze wet treedt in werking de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt.

Gegeven te

Van Koningswege:

De Minister van Binnenlandse zaken, Institutionele
Hervormingen en Democratische Vernieuwing

Annelies Verlinden

comme des entités critiques au sens de l'article 12 de la présente loi.

La liste des infrastructures critiques telle qu'établie par la loi du 1er juillet 2011 sera conforme à l'article 12 de cette loi, sous réserve d'adaptations.

§2. Les entités visées au paragraphe 1, alinéa 1 restent tenues par les obligations énoncées aux articles 13, 13/1, 13/2, 14, 24 et 25 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques jusqu'au 17 mai 2027, telles qu'applicables à ce moment-là.

Art. 77. A l'exception des secteurs dans lesquels aucune entité critique n'avait encore été désignée avant l'entrée en vigueur de la présente loi, toutes les analyses de la menace sont réputées valables pendant une durée maximale de quatre ans, en vertu de l'article 8 et cela, même si la date à laquelle elles ont été effectuées est antérieure à l'entrée en vigueur de la présente loi.

Art. 78. La présente loi entre en vigueur le jour de sa publication au Moniteur belge.

Donné à

Par le Roi:

La Ministre de l'Intérieur, des Réformes institutionnelles et
du Renouveau démocratique

Bijlage

Sector	Deelsector	Categorie van entiteit	Sectorale overheid
1. Energie	Elektriciteit	Elektriciteitsbedrijven als bedoeld in art. 2, punt 57, van Richtlijn (EU) 2019/944, die de taak van "levering" in de zin van artikel 2, punt 12, van die richtlijn verrichten	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
		Distributiesysteembeheerders als bedoeld in art. 2, punt 29, van Richtlijn (EU) 2019/944	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 35, van Richtlijn (EU) 2019/944	
		Producenten als bedoeld in art. 2, punt 38, van Richtlijn (EU) nr. 2019/944	
		Benoemde elektriciteitsmarktbeheerders als bedoeld in art. 2, punt 8, van Verordening (EU) 2019/943	
		Op de elektriciteitsmarkt actieve marktdeelnemer als bedoeld in art. 2, punt 25, van Verordening (EU) 2019/943, die diensten verleent op het gebied van aggregatie, vraagrespons of energieopslag als bedoeld in art. 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944	
	Aardolie	Exploitanten van oliepijpleidingen	
		Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport	
		Centrale entiteiten voor de voorraadvorming als bedoeld in art. 2, punt f), van Richtlijn 2009/119/EG	
	Aardgas	Leveringsbedrijven als bedoeld in art. 2, punt 8, van Richtlijn 2009/73/EG	
		Distributiesysteembeheerders als bedoeld in art. 2, punt 6, van Richtlijn 2009/73/EG	
		Transmissiesysteembeheerders als bedoeld in art. 2, punt 4, van Richtlijn 2009/73/EG	
		Opslagsysteembeheerders als bedoeld in art. 2, punt 10, van Richtlijn 2009/73/EG	
		LNG-systeembeheerders als bedoeld in art. 2, punt 12, van Richtlijn 2009/73/EG	
		Aardgasbedrijven als bedoeld in art. 2, punt 1, van Richtlijn 2009/73/EG	
2. Vervoer	Lucht	Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas	
		Stadsverwarming- en -koeling als bedoeld in art. 2, punt 19, van Richtlijn (EU) 2018/2001 ter bevordering van het gebruik van energie uit hernieuwbare bronnen	
		Waterstof	
		Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof	
	Spoor	Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) 300/2008, die voor commerciële doeleinden worden gebruikt	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
		Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, Richtlijn 2009/12/EG van het Europees Parlement en de Raad, luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, Afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad zijn opgenomen, alsook de entiteiten die bijhorende installaties bedienen welke zich op de luchthavens bevinden	
		Luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad	
	Spoor	Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, Richtlijn 2012/34/EU van het Europees Parlement en de Raad	
		Spoorwagondernemingen zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2012/34/EU, en exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die Richtlijn	

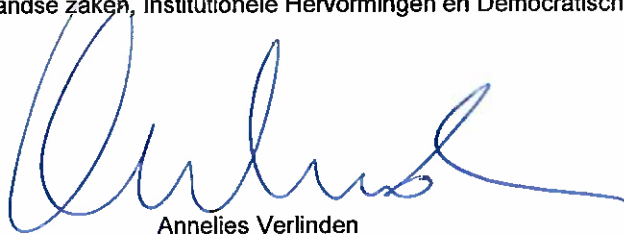
	water	Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht zoals gedefinieerd in bijlage I bij Verordening (EG) 725/2004, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen	
		Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, Richtlijn 2005/65/EG, incl. hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, Verordening (EG) 725/2004, alsook entiteiten die werken en uitrusting in havens beheren	
		Exploitanten van verkeersbegeleiding-systemen zoals gedefinieerd in artikel 3, punt o), Richtlijn 2002/59/EG van het Europees Parlement en de Raad	
	Weg	Beheerders van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1 van Richtlijn 2010/40/EU van het Europees Parlement en de Raad	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
		Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, Verordening (EU) 2015/962 van de Commissie die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties voor wie verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteiten is	
	Openbaar vervoer	Openbaar vervoer exploitanten van diensten zoals gedefinieerd in artikel 2, punt d), Verordening (EG) 1370/2007 van het Europees Parlement en de Raad, met uitzondering van de entiteiten die reeds door een andere deelsector gevat worden	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
3. Bankwezen		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) 575/2013	De Nationale Bank van België (NBB)
4. Infrastructuur voor de financiële markt		Centrale tegenpartijen (CTP's) zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) 648/2012	De Nationale Bank van België (NBB)
		Beheerders van handelsplatforms zoals gedefinieerd in artikel 4, punt 24, Richtlijn 2014/65/EU	De Autoriteit voor Financiële Diensten en Markten (FSMA)
5. Digitale infrastructuur		Aanbieders van internetknooppunten zoals gedefinieerd in artikel 6, punt 18 van Richtlijn (EU) 2022/2555	Het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.)
		DNS-dienstverleners zoals gedefinieerd in artikel 6, punt 20, van Richtlijn (EU) 2022/2555, met uitzondering van exploitanten van root-naamservers	
		Registers voor topleveldomeinnamen zoals gedefinieerd in artikel 6, punt 21 van Richtlijn (EU) 2022/2555	
		Aanbieders van openbare elektronische-communicatienetwerken zoals gedefinieerd in art. 2, punt 8, van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad	
		Aanbieders van elektronische-communicatiediensten als bedoeld in art. 2, punt 4, van Richtlijn (EU) 2018/1972, voor zover hun diensten publiek beschikbaar zijn.	
		Aanbieders van netwerken voor content delivery zoals gedefinieerd in artikel 6, punt 32, van Richtlijn 2022/2555	
		Aanbieders van datacentrumdiensten zoals gedefinieerd in artikel 6, punt 31, van richtlijn 2022/2555	
		Aanbieders van cloudcomputingdiensten zoals gedefinieerd in artikel 6, punt 30, van Richtlijn 2022/2555	

		Verleners van vertrouwensdiensten zoals gedefinieerd in artikel 3, punt 19, van Verordening (EU) 910/2014 van het Europees Parlement en de Raad	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in art. 2, punt 1, a), Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad, maar met uitzondering van distributeurs voor wie de distributie van water voor menselijke consumptie slechts een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen	De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
7. Afvalwater		Ondernemingen die stedelijk, huishoudelijk en industrieel afvalwater zoals gedefinieerd in art. 2, punten 1, 2 en 3, Richtlijn 91/271/EEG van de Raad opvangen, lozen of behandelen, met uitzondering van ondernemingen voor wie het opvangen, lozen of behandelen van stedelijk, huishoudelijk en industrieel afvalwater slechts een niet essentieel onderdeel van hun algemene activiteit is	De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
8. gezondheidszorg		Zorgaanbieders zoals gedefinieerd in art. 3, punt g), Richtlijn 2011/24/EG van het Europees Parlement en de Raad	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
		EU-referentielaboratoria zoals gedefinieerd in art. 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad	De overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
		Entiteiten die zich bezighouden met onderzoek en ontwikkeling van geneesmiddelen zoals gedefinieerd in art. 1, punt 2, Richtlijn 2001/83/EG van het Europees Parlement en de Raad	Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG)
		Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen zoals gedefinieerd in sectie C, afd. 21, van NACE rev. 2 vervaardigen	
		Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") zoals gedefinieerd in art. 22 Verordening (EU) 2022/123 van het Europees Parlement en de Raad	
9. Overheids		Entiteiten met een distributievergunning zoals gedefinieerd in art. 79 Richtlijn 2001/83/EG	
		Overheidsinstanties van federale regeringen, met uitzondering van de rechterlijke macht, parlementen en centrale banken	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad
10. Ruimtevaart		Exploitanten van grondfaciliteiten die in het bezit zijn van en beheerd en geëxploiteerd worden door de Lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronische	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad

		communicatie netwerken zoals gedefinieerd in art. 2, punt 8 Richtlijn (EU) 2018/1972	
11. Productie, verwerking en distributie van levensmiddelen		Voedingsbedrijven zoals gedefinieerd in punt 2) van artikel 3 van Verordening (EG) nr. 178/20021 van het Europees Parlement en de Raad die zich uitsluitend bezighouden met logistiek en groothandelsdistributie en industriële productie op grote schaal en de verwerking ervan	De Overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad

Gezien om te worden gevoegd bij het Voorontwerp van wet betreffende de weerbaarheid van kritieke entiteiten

Van Koningswege:
De Minister van Binnenlandse zaken, Institutionele Hervormingen en Democratische Vernieuwing



Annelies Verlinden

Annexe

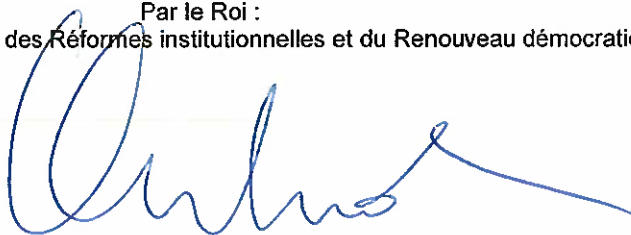
Secteur	Sous-secteur	Categorie d'entité	Autorité sectorielle
1. Energie	Electricité	Entreprises d'électricité au sens de l'article 2, point 57), de la Directive (UE) 2019/94445 du Parlement européen et du Conseil, qui assurent la fonction de "fourniture" au sens de l'article 2, point 12), de ladite Directive	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
		Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la Directive (UE) 2019/944	
		Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la Directive (UE) 2019/944	
		Producteurs au sens de l'article 2, point 38), de la Directive (UE) 2019/944	
		Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil	
		Acteurs du marché de l'électricité au sens de l'article 2, point 25), du règlement (UE) 2019/943, qui fournit des services en matière d'agrégation, de participation active de la demande ou de stockage de l'énergie au sens de l'article 2, points 18), 20) et 59), de la Directive (UE) 2019/944	
	Pétrole	Exploitants d'oléoducs	
		Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole	
		Entités centrales de stockage de pétrole au sens de l'article 2, point f), de la Directive 2009/119/CE du Conseil	
	Gaz	Entreprises de fourniture au sens de l'article 2, point 8), de la Directive 2009/73/CE du Parlement européen et du Conseil	
		Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la Directive 2009/73/CE	
		Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la Directive 2009/73/CE	
		Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la Directive 2009/73/CE	
		Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la Directive 2009/73/CE	
		Entreprises de gaz naturel au sens de l'article 2, point 1), de la Directive 2009/73/CE	
		Exploitants d'installations de raffinage et de traitement de gaz naturel	
	Réseaux de chaleur et de froid	Réseaux de chaleur ou de froid au sens de l'article 2, point 19), de la Directive (UE) 2018/200147 du Parlement européen et du Conseil	
	Hydrogène	Exploitants d'installations de production, de stockage et de transport d'hydrogène	
2. Transports	Transports aériens	Transporteurs aériens au sens de l'article 3, point 4), du Règlement (CE) n° 300/2008 utilisés à des fins commerciales	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
		Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la Directive 2009/12/CE du Parlement européen et du conseil, aéroports au sens de l'article 2, point 1), de ladite Directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du Règlement (UE) n° 1315/2013 du Parlement européen et du Conseil, et entités exploitant les installations annexes se trouvant dans les aéroports	
		Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du Règlement (CE) n° 549/2004 du Parlement européen et du Conseil	
	Transports ferroviaires	Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la Directive 2012/34/UE du Parlement européen et du Conseil	

	Transports par eau	Entreprises ferroviaires au sens de l'article 3, point 1), de la Directive 2012/34/UE, et exploitants d'installations de services au sens de l'article 3, point 12), de ladite Directive	
		Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'Annexe I du Règlement (CE) n° 725/2004, à l'exclusion des navires exploités à titre individuel par ces sociétés	
		Entités gestionnaires des ports au sens de l'article 3, point 1), de la Directive 2005/65/CE56, y compris les installations portuaires au sens de l'article 2, point 11), du Règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports	
		Exploitants de services de trafic maritime au sens de l'article 3, point o), de la Directive 2002/59/CE du Parlement européen et du Conseil	
	Transports routiers	Systèmes de transport intelligents au sens de l'article 4, point 1), de la Directive 2010/40/UE du Parlement européen et du Conseil	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
		Autorités routières au sens de l'article 2, point 12), du Règlement délégué (UE) 2015/962 de la Commission chargées du contrôle de gestion du trafic, à l'exclusion des entités publiques pour lesquelles la gestion du trafic ou l'utilisation des systèmes de transport intelligents ne constituent qu'une partie non essentielle de leur activité générale	
	Transport public	Exploitants de services de transport public au sens de l'article 2 point (d) du Règlement (CE) n°1370/2007 du Parlement européen et du Conseil, à l'exception des entités qui relèvent déjà d'un autre sous-secteur	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
3. Secteur bancaire -		Établissements de crédit au sens de l'article 4, point 1), du Règlement (UE) n° 575/2013 du Parlement européen et du Conseil	La Banque nationale de Belgique (BNB)
4. Infrastructures de marchés financiers		Contreparties centrales au sens de l'article 2, point 1), du Règlement (UE) n° 648/2012	La Banque nationale de Belgique (BNB)
		Opérateurs de plates-formes de négociation au sens de l'article 4, point 24), de la Directive 2014/65/UE	L'autorité des services et marchés financiers (FSMA)
5. Infrastructures numériques		Fournisseurs de points d'échange internet au sens de l'article 6, point 18), de la Directive (UE) 2022/2555	Institut belge des services postaux et des télécommunications (I.B.P.T.)
		Fournisseurs de services DNS au sens de l'article 6, point 20), de la Directive (UE) 2022/2555, à l'exclusion des opérateurs de serveurs racines de noms de domaines	
		Registres de noms de domaines de premier niveau au sens de l'article 6, point 21), de la Directive (UE) 2022/2555	
		Fournisseurs de services de centre de données au sens de l'article 6, point 31), de la Directive (UE) 2022/2555	
		Fournisseurs de réseaux de diffusion de contenu au sens de l'article 6, point 32), de la directive (UE) 2022/2555	
		Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la Directive (UE) 2018/1972 du Parlement européen et du Conseil	
		Fournisseurs de services de communications électroniques au sens de l'article 2, point 4), de la Directive (UE) 2018/1972 dans la mesure où leurs services sont accessibles au public	
		Fournisseurs de services d'informatique en nuage au sens de l'article 6, point 30), de la Directive (UE) 2022/2555	

		Prestataires de services de confiance au sens de l'article 3, point 19), du règlement (UE) n° 910/2014 du Parlement européen et du conseil	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la Directive (UE) 2020/2184 du Parlement européen et du Conseil, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie non essentielle de leur activité générale de distribution d'autres produits et biens	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
7. Eaux résiduaires		Entreprises assurant la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées et des eaux industrielles usées au sens de l'article 2, points 1) à 3), de la Directive 91/271/CEE du Conseil, à l'exclusion des entreprises pour lesquelles la collecte, l'élimination ou le traitement des eaux urbaines, ménagères et industrielles usées ne constituent qu'une partie non essentielle de leur activité générale	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
8. Santé		Prestataire de soins de santé au sens de l'article 3, point g), de la Directive 2011/24/UE du Parlement européen et du Conseil	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
		Laboratoires de référence de l'Union européenne au sens l'article 15 du Règlement (UE) 2022/2371 du Parlement européen et du conseil	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
		Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la Directive 2001/83/CE du Parlement européen et du Conseil	Agence fédérale des médicaments et des produits de santé (A.F.M.P.S.)
		Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la section C, division 21, de la NACE Rév. 2	
		Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique ("liste des dispositifs médicaux critiques en cas d'urgence de santé publique") au sens de l'article 22 du Règlement (UE) 2022/123 du Parlement européen et du Conseil	
		Entités titulaires d'une autorisation de distribution au sens de l'article 79 de la Directive 2001/83/CE	
9. Administrations publiques		Administrations publiques du niveau fédéral, – excluant le pouvoir juridique, les parlements, et les banques centrales	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
10. Espace		Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8), de la Directive (UE) 2018/1972	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres
11. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3 point 2 du Règlement (CE) n°178/2021 du Parlement européen et du Conseil impliquées exclusivement dans la logistique et la distribution en gros et la production et la transformation à grande échelle	L'autorité désignée par le Roi par arrêté pris en Conseil des ministres

Vu pour être annexé à l' Avant-projet de loi concernant la résilience des entités critiques.

Par le Roi :
La Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique

A handwritten signature in blue ink, consisting of a large, stylized 'V' followed by a series of loops and a long horizontal stroke extending to the right.

Annelies Verlinden

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

ALGEMENE OVERWEGINGEN

Het voorliggend wetsontwerp zorgt voor de omzetting in Belgisch recht van de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad inzake de weerbaarheid van kritieke entiteiten en tot intrekking van de Richtlijn 2008/114/EG van de Raad (hieronder "de CER-Richtlijn"). Zij heeft als doel de weerbaarheid te vergroten van kritieke entiteiten die diensten verlenen die essentieel zijn voor de vitale maatschappelijke functies of economische activiteiten op de interne markt.

De CER-Richtlijn beoogt de intrekking en vervanging van de Richtlijn 2008/114/EG van de Raad van 5 december 2008 inzake de identificatie en de aanduiding van Europese kritieke infrastructuren en de beoordeling van de noodzaak de beveiliging van dergelijke infrastructuren te verbeteren (ECI-Richtlijn). De ECI-Richtlijn was uitsluitend gericht op de beveiliging van Europese kritieke infrastructuren in de sectoren energie en transport, waarvan de ontwrichting of vernietiging aanzienlijke grensoverschrijdende gevolgen zou hebben voor ten minste twee Lidstaten. Deze Richtlijn werd in België omgezet in de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren (hieronder "KI-wet"). De KI-wet ging reeds verder dan wat de ECI-Richtlijn oplegde, daar op nationaal niveau niet enkel Europese kritieke infrastructuren werden geïdentificeerd, maar ook nationale kritieke infrastructuren. Het aantal sectoren dat onder het toepassingsgebied viel, werd tevens op grond van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid aanzienlijk uitgebreid op nationaal niveau met de sectoren drinkwater, ruimtevaart, gezondheidszorg, financiën, elektronische communicatie en digitale infrastructuren.

Na een evaluatie door de Europese Commissie van de ECI-Richtlijn in 2019, bleek dat door de steeds sterkere verwevenheid en grensoverschrijdende aard van activiteiten waarbij gebruik wordt gemaakt van kritieke infrastructuur, beschermende maatregelen met betrekking tot louter individuele activa niet volstaan om alle verstoringen te voorkomen. Er werd besloten dat een aanpak nodig was waarin meer oog was voor de risico's, waarin de rol en plichten van kritieke entiteiten die essentiële diensten aanbieden beter omschreven worden en samenhangend zijn, en waarin Unieregels worden vastgesteld om de weerbaarheid van kritieke entiteiten te vergroten.

Met de CER-Richtlijn wordt tegemoet gekomen aan de nood om kritieke entiteiten beter uit te rusten om het hoofd te bieden aan de risico's die de verlening van essentiële

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

CONSIDÉRATIONS GÉNÉRALES

Le présent projet de loi transpose en droit belge la Directive (UE) 2022/2557 du Parlement européen et du Conseil relative à la résilience des entités critiques et abrogeant la Directive 2008/114/CE du Conseil (ci-dessous "la Directive CER"). Elle a pour objectif d'accroître la résilience des entités critiques qui fournissent des services essentiels pour les fonctions sociétales ou les activités économiques vitales dans le marché intérieur.

La Directive CER vise à abroger et à remplacer la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (Directive ICE). La Directive ICE était exclusivement axée sur la protection des infrastructures critiques européennes dans les secteurs de l'énergie et des transports, dont l'arrêt ou la destruction aurait un impact transfrontalier significatif pour au moins deux Etats membres. Cette Directive a été transposée en Belgique dans la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (ci-dessous la "loi IC"). La loi IC allait déjà plus loin que ce qu'imposait la Directive ICE dans la mesure où non seulement des infrastructures critiques européennes étaient identifiées au niveau national, mais aussi des infrastructures critiques nationales. Le nombre de secteurs relevant du champ d'application a également été considérablement étendu à l'échelle nationale, sur base de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique afin d'inclure les secteurs de l'eau potable, de l'espace, des soins de santé, de la finance, des communications électroniques et des infrastructures numériques.

Suite à une évaluation de la Directive ICE par la Commission européenne en 2019, il s'est avéré qu'en raison de l'interconnexion et du caractère transfrontalier croissants des activités ayant recours aux infrastructures critiques, les mesures de protection relatives à des actifs purement individuels ne suffisent pas pour prévenir toutes les perturbations. Il a été décidé de la nécessité d'une approche qui tienne davantage compte des risques, qui définit mieux le rôle et les obligations des entités critiques fournissant des services essentiels, qui assure leur cohérence et qui prévoit des règles de l'Union destinées à renforcer la résilience des entités critiques.

La Directive CER répond au besoin de mieux équiper les entités critiques afin de faire face aux risques susceptibles de perturber la fourniture de services essentiels. Le

diensten zouden kunnen verstoren. Het dynamisch dreigingslandschap, met onder andere veranderende hybride en terroristische dreigingen, alsook de toenemende onderlinge afhankelijkheid tussen infrastructuur en sectoren, zorgt ervoor dat de huidige richtlijn niet meer volstaat om deze entiteiten voldoende te beschermen. Bovendien is er een toenemend risico wegens natuurrampen en klimaatverandering, waardoor zich vaker en op grotere schaal extreme weersomstandigheden zullen voordoen. De CER-Richtlijn creëert een overkoepelend en geharmoniseerd kader betreffende de weerbaarheid van kritieke entiteiten ten aanzien van alle gevaren, d.w.z. zowel natuurrampen als rampen die, accidenteel of opzettelijk, door de mens worden veroorzaakt, alsook noodsituaties op het gebied van volksgezondheid zoals pandemieën.

De CER Richtlijn stelt geharmoniseerde minimumvoorschriften vast om de verlening van essentiële diensten op de interne markt te waarborgen in de gehele Unie. Het is mogelijk dat lidstaten bijkomende voorschriften opleggen, doch blijft het gelijke speelveld gewaarborgd door het feit dat elke lidstaat gehouden is aan eenzelfde kader van basis voorschriften.

Waar voorheen in de ECI-Richtlijn gesproken werd over "kritieke infrastructuur", gebruikt de CER-Richtlijn hoofdzakelijk het concept "kritieke entiteit". De CER-Richtlijn gaat namelijk uit van een inclusieve visie van de entiteiten die essentiële diensten verlenen, en waar voorheen enkel naar de infrastructuur gekeken werd, zal vanaf nu focus liggen op de hele entiteit. Een kritieke entiteit is "een publieke of particuliere entiteit die overeenkomstig de CER-wet is geïdentificeerd als behorende tot één van de categorieën die zijn vermeld in de tabel in bijlage." Om geïdentificeerd te kunnen worden als kritieke entiteit moet er aan drie voorwaarden voldaan worden, nl. de entiteit verleent essentiële diensten, de kritieke infrastructuur bevindt zich op het Belgisch grondgebied en een incident zou een aanzienlijk verstorend effect hebben op de verlening van die essentiële dienstverlening.

In dit ontwerp werd er gekozen om ook het concept van "kritieke infrastructuur" te behouden, naast het concept van "kritieke entiteit". Eén van de hoofdvoorwaarden om als kritieke entiteit aangeduid te kunnen worden, is nl. de voorwaarde dat een kritieke infrastructuur van de entiteit zich bevindt op Belgisch grondgebied. De CER-Richtlijn focust zich onder meer op de fysieke bescherming, waardoor het opportuun is om beide concepten te hanteren aangezien er steeds fysieke kritieke infrastructuur aanwezig zal moeten zijn in de kritieke entiteit om als zodanig geïdentificeerd te worden. Bovendien is het zo dat niet elke infrastructuur van een kritieke entiteit dezelfde functie heeft en steeds essentiële diensten verleent, waardoor met het behouden van dit concept ook een duidelijk onderscheid kan gemaakt worden tussen niet-kritieke en kritieke infrastructuur van een kritieke entiteit, dewelke dan op gepaste wijze kunnen beschermd worden. Bovendien houdt de CER-Richtlijn in dat er zowel fysieke als organisatorische maatregelen genomen moeten worden, zoals bijvoorbeeld maatregelen die betrekking hebben op de bedrijfscontinuïteit. Deze maatregelen moeten op een passend niveau genomen kunnen worden in de kritieke entiteit. Fysieke

paysage dynamique des menaces, en ce compris l'évolution des menaces hybrides et terroristes, de même que l'interdépendance croissante entre les infrastructures et les secteurs impliquent que la directive actuelle ne suffit plus pour protéger adéquatement ces entités. Force est en outre de constater un risque accru lié aux catastrophes naturelles et aux changements climatiques, qui va induire des phénomènes météorologiques extrêmes plus fréquents et à plus grande échelle. La Directive CER crée un cadre global et harmonisé sur la résilience des entités critiques face à tous les dangers, à savoir tant les catastrophes naturelles que les catastrophes provoquées, de façon accidentelle ou intentionnelle, par l'homme, ainsi que les situations d'urgence en matière de santé publique, telles que les pandémies.

La directive CER établit des règles minimales harmonisées pour garantir la fourniture de services essentiels dans le marché intérieur dans toute l'Union. Les États membres peuvent imposer des règles supplémentaires, mais l'égalité des conditions de concurrence reste garantie par le fait que chaque État membre est lié par le même cadre de règles de base.

Si la Directive ICE parlait "d'infrastructures critiques", la Directive CER a principalement recours au concept d'"entité critique". La Directive CER se base en effet sur une vision inclusive des entités qui fournissent des services essentiels et, alors que seule l'infrastructure était auparavant prise en compte, l'accent est désormais mis sur l'entité dans son ensemble. Une entité critique est "une entité publique ou privée identifiée, conformément à la loi CER, comme faisant partie d'une des catégories mentionnées dans le tableau en annexe." Afin de pouvoir être identifiée comme entité critique, trois conditions doivent être remplies, à savoir: l'entité fournit des services essentiels, l'infrastructure critique se situe sur le territoire belge et un incident aurait un effet perturbateur important sur la fourniture de ces services essentiels.

Dans le présent projet, il a été décidé de maintenir également le concept d'"infrastructure critique", outre celui d'"entité critique". Une des conditions principales pour pouvoir être désignée comme entité critique est qu'une infrastructure critique de l'entité se situe sur le territoire belge. Étant donné que la Directive CER met notamment l'accent sur la protection physique, il est opportun d'avoir recours aux deux concepts dans la mesure où il devra toujours y avoir une infrastructure critique physique dans l'entité critique pour pouvoir être identifiée comme telle. Par ailleurs, toutes les infrastructures d'une entité critique n'ayant pas la même fonction et ne fournissant pas toujours des services essentiels, le maintien de ce concept permet également de distinguer clairement les infrastructures non critiques des infrastructures critiques d'une entité critique, qui peuvent alors être protégées de manière adéquate. En outre, la Directive CER implique que des mesures tant physiques, qu'organisationnelles soient prises, telles que des mesures de continuité des activités. Ces mesures doivent pouvoir être prises à un niveau approprié de l'entité critique. Les mesures de sécurité physique devront s'appliquer tant au niveau de l'entité qu'au niveau de l'infrastructure, tandis que les

beveiligingsmaatregelen zullen zowel op entiteit niveau als op het niveau van de infrastructuur moeten toegepast kunnen worden, terwijl organisatorische maatregelen eerder genomen zullen moeten worden op entiteit niveau. Het volstaat niet om enkel op entiteit niveau fysieke beveiligingsmaatregelen in te voeren wanneer de meest gevoelige plaatsen van de kritieke entiteit infrastructuur zijn die gelegen zijn op een andere locatie. Het onderscheid tussen kritieke entiteit en kritieke infrastructuur staat bijgevolg toe dat de verschillende soorten maatregelen in de praktijk op passend niveau genomen kunnen worden.

Kritieke entiteiten spelen als verleners van essentiële diensten een onmisbare rol bij het in stand houden van vitale maatschappelijke functies of economische activiteiten op de interne markt, in een economie die in de Europese Unie in toenemende mate onderling afhankelijk is. Het wetsontwerp heeft als doel te waken over het behoud en de weerbaarheid van vitale functies zoals onder andere de productie en transport van energie, de vitale vervoersinfrastructuur en -systemen, de onontbeerlijke schakels in het elektronische betalingsvervoer, de vitale verbindingen van elektronische communicatie, de onmisbare entiteiten in de gezondheidszorg en faciliteiten die ervoor zorgen dat burgers over drinkwater beschikken. Het wetsontwerp stelt een gemeenschappelijke benadering in werking, waarbij rekening wordt gehouden met het essentiële karakter van de sectoren waarop de CER-Richtlijn wordt toegepast, met name de sectoren: energie, vervoer, bankwezen, financiële marktinfrastructuur, digitale infrastructuur, drinkwater, afvalwater, volksgezondheid, overheidsinstellingen, ruimtevaart en voeding.

Deze wetgeving situeert zich hoofdzakelijk in het domein van de preventie. Het gaat om de organisatie van het nemen van weerbaarheidsmaatregelen door de kritieke entiteit, en indien noodzakelijk beschermingsmaatregelen door de bevoegde overheden, teneinde elk voorval dat van aard is om een aanzienlijk verstorend effect te hebben op de verlening van essentiële diensten door de kritieke entiteit, te voorkomen of te verhinderen. In het geval een incident zich toch voordoet, poogt deze wetgeving de kritieke entiteiten de nodige tools te geven om zich hiertegen te verdedigen. Kritieke entiteiten zullen echter wel een intern noodplan moeten opstellen, als onderdeel van hun weerbaarheidsplan van de kritieke entiteit (hierna: W.P.E.).

Dit wetsontwerp situeert zich verder niet in het raam van de voorbereiding op het beheer van een noodsituatie, waarvoor de ter zake reeds bestaande wettelijke en reglementaire bepalingen dienen te worden toegepast.¹

De Richtlijn legt de lidstaten de verplichting op om risicobeoordelingen uit te voeren met betrekking tot de

mesures organisationnelles sont plus susceptibles de devoir être prises au niveau de l'entité. Il ne suffit pas de mettre en œuvre des mesures de sécurité physique uniquement au niveau de l'entité lorsque les sites les plus sensibles de l'entité critique sont des infrastructures situées sur un autre site. La distinction entre entité critique et infrastructure critique permet aux différents types de mesures d'être prises à un niveau approprié dans la pratique.

En tant que fournisseurs de services essentiels, les entités critiques jouent un rôle indispensable dans le maintien des fonctions sociétales ou des activités économiques vitales sur le marché intérieur, dans une économie de plus en plus interdépendante au sein de l'Union européenne. Le projet de loi vise à veiller au maintien et à la résilience des fonctions vitales, entre autres la production et le transport d'énergie, les points nodaux vitaux du transport, les maillons indispensables dans le transport des paiements électroniques, les connexions vitales de la communication électronique, les entités indispensables aux soins de santé et les installations qui permettent aux citoyens de disposer d'eau potable. Le projet de loi met en place une approche commune, qui tient compte du caractère essentiel des secteurs auxquels la Directive CER s'applique, à savoir : l'énergie, les transports, le secteur bancaire, l'infrastructure des marchés financiers, l'infrastructure numérique, l'eau potable, les eaux usées, la santé publique, les institutions publiques, l'espace et l'alimentation.

Cette législation se situe principalement dans le domaine de la prévention. Il s'agit d'organiser la prise de mesures de résilience par l'entité critique et, si nécessaire, de mesures de protection par les autorités compétentes afin de prévenir ou d'empêcher tout événement de nature à perturber de manière significative la fourniture des services essentiels par l'entité critique. Au cas où un incident survient malgré tout, cette législation tente de fournir aux entités critiques les outils nécessaires pour s'en protéger. Toutefois, les entités critiques devront préparer un plan d'urgence interne dans le cadre de leur plan de résilience de l'entité critique (ci-après : P.R.E.).

Le présent projet de loi ne se situe pas davantage dans le cadre des préparatifs liés à la gestion d'une situation d'urgence. Le cas échéant, les dispositions légales et réglementaires existantes doivent être appliquées.¹

La Directive oblige les Etats membres à effectuer des évaluations de risques concernant les secteurs qui

¹ Wet van 31 december 1963 betreffende de civiele bescherming, BS, 16 januari 1964; Koninklijk besluit van 31 januari 2003 tot vaststelling van het noodplan voor de crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen, BS, 21 februari 2003; Wet van 15 mei 2007 betreffende de civiele veiligheid, BS 31 juli 2007; Koninklijk Besluit van 22 mei 2019 betreffende de noodplanning en het beheer van noodsituaties op gemeentelijk en provinciaal niveau en betreffende de rol van de burgemeesters en de provinciegouverneurs in geval van crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal niveau vereisen, BS 27 juni 2019.

¹ Loi du 31 décembre 1963 relative à la protection civile, M.B., 16 janvier 1964; Arrêté royal du 31 janvier 2003 portant fixation du plan d'urgence pour les événements et situations de crise nécessitant une coordination ou une gestion à l'échelon national, M.B., 21 février 2003; Loi du 15 mai 2007 relative à la sécurité civile, M.B. 31 juillet 2007; Arrêté Royal du 22 mai 2019 relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial et au rôle des bourgmestres et des gouverneurs de province en cas d'événements et de situations de crise nécessitant une coordination ou une gestion à l'échelon national, M.B. 27 juin 2019.

sectoren die onder het toepassingsgebied vallen. Het uitvoeren van deze sectorale risicobeoordeling valt onder de verantwoordelijkheid van de sectorale overheden, die bevoegd zijn voor hun welbepaalde (deel-)sectoren. Deze risicobeoordeling dient om de risico's per sector of deelsector te identificeren. Bij het uitvoeren van deze risicobeoordeling wordt tevens rekening gehouden met andere algemene of sectorspecifieke risicobeoordelingen die krachtens andere rechtshandelingen van de Unie zijn verricht, en moeten zij de onderlinge afhankelijkheid van sectoren in aanmerking nemen. De CER-Richtlijn verwijst hierbij ook naar de risicobeoordeling die is uitgevoerd overeenkomstig artikel 6, lid 1 van Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad. Dit betreft de Belgische Nationale Risicobeoordeling, en wordt gecoördineerd door het NCCN. De high level resultaten hiervan worden gedeeld met de sectorale overheden zodat zij deze kunnen gebruiken bij het opstellen van hun eigen sectorale risicobeoordeling, alsook met de kritieke entiteiten zodat deze gebruikt kunnen worden bij het uitvoeren van hun risicobeoordeling en het opstellen van het W.P.E.

Vooraleer weerbaarheidsmaatregelen verplicht kunnen gesteld worden, dienen entiteiten geïdentificeerd te worden op basis van de bepalingen uit deze wet. Het is belangrijk te benadrukken dat de identificatie van kritieke entiteiten niet gebeurt op basis van de sectorale risicobeoordeling, maar op basis van een impactanalyse, waar men onder meer rekening moet houden met de risico's geïdentificeerd in de sectorale risicobeoordeling.

Deze opdracht is toevertrouwd aan de sectorale overheid, met name de overheid die bevoegd is voor een welbepaalde sector of deelsector. De sectorale overheden werken samen met de vertegenwoordigers van de sector en zelfs met de potentiële kritieke entiteiten, aangezien ze samen over de nodige expertise beschikken met betrekking tot hun welbepaalde sector. De KI-wet introduceerde het concept van sectorale overheid, en de manier van identificatie wordt overgenomen in dit wetsontwerp mits de noodzakelijke aanpassingen gelet op de CER-Richtlijn, aangezien de sectorale overheden vertrouwd zijn met de procedure en zij het best geplaatst zijn om deze identificatie en aanduiding uit te voeren. Gelet op het feit dat er onder het toepassingsgebied van dit voorstel een aantal sectoren, zoals de drinkwater en afvalwater sector, onder het toepassingsgebied vallen waarvoor de bevoegdheid in België verdeeld werd tussen de federale en gefedereerde entiteiten, voeren de bevoegde federale overheden deze functie uit samen met de gefedereerde entiteiten voor zover de kritieke entiteiten onder hun bevoegdheden vallen. Daarna is het de taak voor de sectorale overheden om de kritieke entiteiten te gaan identificeren en aanduiden. Deze aanduiding is van belang omdat deze ervoor zorgt dat de verplichtingen uit deze wet op die entiteiten van toepassing zullen zijn.

Hierdoor is het dus mogelijk dat de omzetting van de CER-Richtlijn ook een impact heeft op sectoren die tot de bevoegdheid van de gefedereerde entiteiten behoren. Dit was echter reeds het geval bij de omzetting van de ECI-Richtlijn. In haar advies betreffende de KI-wet stelde de Raad van State dat maatregelen die op basis van het voorontwerp zullen worden getroffen, *“een weerslag zouden kunnen hebben op operatoren die een*

relèvent du champ d'application. La réalisation de ces évaluations sectorielles de risques relève de la responsabilité des autorités sectorielles, qui sont compétentes pour leurs (sous-)secteurs bien précis. Cette évaluation de risques sert à identifier les risques par secteur et sous-secteur. Dans le cadre de la réalisation de ces évaluations des risques, il est également tenu compte d'autres évaluations de risques générales ou sectorielles qui ont été effectuées en vertu d'autres actes juridiques de l'Union, ainsi que de l'interdépendance des secteurs. La Directive CER fait également référence ici à l'évaluation des risques réalisée conformément à l'article 6, paragraphe 1^{er}, de la décision n°1313/2013/UE du Parlement européen et du Conseil. Ceci concerne l'évaluation nationale belge des risques, coordonnée par le NCCN. Les résultats high level de ces évaluations seront partagés avec les autorités sectorielles afin qu'elles puissent les utiliser pour préparer leur propre évaluation des risques sectoriels, ainsi qu'avec les entités critiques afin qu'elles puissent les utiliser lors de l'évaluation des risques et de la préparation du P.R.E.

Avant de pouvoir prendre des mesures obligatoires de résilience, les entités doivent être identifiées sur la base des dispositions prévues dans la présente loi. Il est important de souligner que l'identification des entités critiques ne se fait pas sur la base de l'évaluation des risques sectoriels, mais sur la base d'une analyse d'impact, où il faut tenir compte, entre autres, des risques identifiés dans l'évaluation des risques sectoriels.

Cette mission est confiée aux autorités sectorielles, à savoir les autorités compétentes pour un secteur ou sous-secteur déterminé. Les autorités sectorielles collaborent avec les représentants du secteur, voire avec les entités critiques potentielles étant donné qu'elles disposent ensemble de l'expertise nécessaire concernant leur secteur déterminé. La loi IC a introduit le concept d'autorité sectorielle et le mode d'identification est repris dans le présent projet de loi, moyennant les ajustements nécessaires compte tenu de la Directive CER, étant donné que les autorités sectorielles sont familiarisées avec la procédure et qu'elles sont les mieux placées pour effectuer cette identification et cette désignation. Dans la mesure où le champ d'application de ce projet prévoit toute une série de secteurs, comme celui de l'eau potable ou du traitement des eaux résiduaires dont la compétence a été répartie en Belgique entre les entités fédérales et fédérées, les autorités fédérales compétentes remplissent cette fonction en collaboration avec les entités fédérées dans la mesure où les entités critiques relèvent de leurs compétences. Il revient par ailleurs aux autorités sectorielles d'identifier et de désigner les entités critiques. Cette désignation est importante parce qu'elle garantit que les obligations prévues par la présente loi s'appliqueront à ces entités.

Il est donc possible que la transposition de la Directive CER ait également un impact sur les secteurs relevant de la compétence des entités fédérées. Toutefois, cela était déjà le cas lors de la transposition de la Directive ICE. Dans son avis sur la loi ICE, le Conseil d'Etat a indiqué que les mesures à prendre sur base de l'avant-projet *« pourraient affecter les opérateurs exploitant des infrastructures qui, d'un autre point de vue, peuvent*

infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid *ratione materiae* van de gewesten kan behoren, waardoor werd aanvaard dat zij werden betrokken in het proces omschreven in de wet.² Daarnaast werd gesteld dat dit eveneens zou kunnen gelden voor andere sectoren waarop de KI-wet toepassing zou vinden.³

De Raad van State heeft dit advies recent bevestigd in 2019 in het kader van de NIS-wet. Deze wet heeft het toepassingsgebied van de KI-wet uitgebreid naar meer sectoren⁴, waaronder sectoren die (deels) onder de bevoegdheid van de gefedereerde entiteiten vallen.⁵ De Raad van State stelde in dit advies dat er voldoende rekening werd gehouden met de bevoegdheden van de gefedereerde entiteiten aangezien de gewesten betrokken werden bij de uitvoering van het voorontwerp.⁶ De gefedereerde entiteiten zullen dan ook betrokken worden bij de uitvoering van het huidige ontwerp van wet. Tijdens de identificatieprocedure zullen aldus de gefedereerde entiteiten steeds betrokken kunnen worden, zoals dat op basis van de huidige wetgeving reeds het geval is. Op deze manier wordt autonomie van de verschillende beleidsniveaus in acht genomen, aangezien de medewerking facultatief is en zulks niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen kan nemen.

Een breed inzicht in de mogelijke risico's die de verlening van hun essentiële diensten kunnen verstoren, is noodzakelijk om de betrokken kritieke entiteiten hiertegen op adequate wijze weerbaar te maken. Bijgevolg zullen ook de kritieke entiteiten zelf, minstens elke 4 jaar, een risicobeoordeling moeten uitvoeren. Op basis daarvan nemen zij technische, beveiligings-, en organisatorische maatregelen die gepast en evenredig zijn gelet op de risico's waarmee zij geconfronteerd worden, om incidenten te voorkomen, te beperken of te beheersen, en om bescherming te bieden of bestand te zijn ertegen, te reageren erop of daarvan te herstellen. Deze maatregelen moeten worden vastgelegd in het W.P.E.. Het W.P.E. mag bestaan uit plannen waarover de kritieke entiteit reeds beschikt op basis van andere wetgeving, zolang alle elementen die door de CER-Richtlijn worden opgelegd er maar in vervat werden.

In het kader van de weerbaarheid van kritieke entiteiten, wordt er een delegatie gegeven aan de Koning om de nationale autoriteit aan te duiden die belast is met de opvolging en coördinatie van de uitvoering van deze wet.

*relever de la compétence ratione materiae des régions, de sorte qu'il a été admis qu'elles soient incluses dans le processus décrit dans la loi ».*² En outre, il a été indiqué que cela pourrait également s'appliquer à d'autres secteurs auxquels la loi IC s'appliquerait.³

Le Conseil d'Etat a récemment confirmé cet avis en 2019 dans le cadre de la loi NIS. Cette loi a étendu le champ d'application de la loi IC à un plus grand nombre de secteurs⁴, y compris des secteurs qui relèvent (en partie) de la compétence des entités fédérées.⁵ Dans cet avis, le Conseil d'Etat indique que les compétences des entités fédérées ont été suffisamment prises en compte puisque les régions ont été impliquées dans la mise en œuvre de l'avant-projet.⁶ Les entités fédérées seront donc associées à la mise en œuvre du présent projet de loi. Ainsi, lors de la procédure d'identification, les entités fédérées pourront toujours être impliquées, comme cela est déjà le cas dans la législation actuelle. De cette manière, l'autonomie des différents niveaux politiques est respectée, puisque la coopération est facultative et que cela n'empêche pas le gouvernement fédéral compétent de prendre les mesures envisagées.

Une vaste compréhension des risques potentiels susceptibles de perturber la fourniture de leurs services essentiels est nécessaire pour que les entités critiques concernées puissent s'en prémunir de manière adéquate. C'est pourquoi les entités critiques devront elles-mêmes effectuer une évaluation des risques au moins tous les 4 ans. Sur cette base, elles prennent des mesures techniques, de sécurisation et organisationnelles qui sont appropriées et proportionnelles aux risques auxquels elles sont confrontées, afin de prévenir, de limiter ou de maîtriser les incidents et de s'en prémunir, d'y réagir ou de s'en rétablir. Ces mesures doivent être définies dans le P.R.E.. Le P.R.E. peut être constitué de plans déjà à la disposition de l'entité critique en vertu de toute autre législation, pour autant que tous les éléments requis par la Directive CER y aient été inclus.

Dans le cadre de la résilience des entités critiques, une délégation au Roi est prévue pour désigner l'autorité nationale chargée de la supervision et de la coordination de la mise en œuvre de cette loi. L'autorité qui remplit

² P. PIETERS, "Openbare veiligheid als exclusief federale bevoegdheid", *vigiles* 2012, afl. 4, 354.

³ Adv. RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuur en andere punten van federaal belang, *Parl.st. Kamer* 2010-11, nr. 53-1357/001, 55.

⁴ P. PIETERS, "Openbare veiligheid als exclusief federale bevoegdheid", *vigiles* 2012, afl. 4, 354.

⁵ Avis C.E. n° 48.989/VR du 9 décembre 2010 sur un avant-projet de loi sur les infrastructures critiques et autres points d'intérêt fédéral, *Doc. Parl.* 2010-11, n° 53-1357/001, 55.

⁶ De NIS-wet betrof naast de sectoren energie en transport ook onder meer de sectoren drinkwater, elektronische communicatie, gezondheidszorg, digitale infrastructuur en financiële marktinfrastructuur.

⁷ Adv.RvS nr. 63.296/4 van 2 mei 2018 over een voorontwerp van wet tot vaststelling van een kader voor de beveiliging van network- en informatiesystemen van algemeen belang voor de openbare veiligheid, *Parl.St. Kamer* 2018-2019, nr. 54-3340/1, 75-79

⁸ Adv. RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuur en andere punten van federaal belang, *Parl.st. Kamer* 2010-11, nr. 53-1357/001, 54.

⁹ Outre les secteurs de l'énergie et des transports, la loi NIS couvre également les secteurs de l'eau potable, des communications électroniques, de la santé, des infrastructures numériques et des infrastructures des marchés financiers, entre autres.

¹⁰ Avis C.E. n° 63.296/4 du 2 mai 2018 sur un avant-projet de loi établissant un cadre pour la sécurité des systèmes de réseaux et d'information d'intérêt général de sécurité publique, *Doc. Parl.* 201820191, n° 54-3340/1, 75-79.

¹¹ Avis C.E. n° 48.989/VR du 9 décembre 2010 sur un avant-projet de loi sur les infrastructures critiques et autres points d'intérêt fédéral, *Doc. Parl.* 2010-11, n° 53-1357/001, 54.

De autoriteit die deze rol vandaag al vervult en ook zal blijven vervullen is het Nationaal Crisiscentrum (hierna: NCCN). Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en op Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.

Het NCCN is verantwoordelijk voor de coördinatie met de politie- en veiligheidsdiensten, en kan extra maatregelen opleggen ter bescherming van de kritieke entiteiten wanneer nodig. Daarnaast ondersteunt het NCCN de sectorale overheden tijdens de identificatieprocedure van de kritieke entiteiten. Tevens verleent het NCCN een advies aan de sectorale overheden over het identificatiedossier van een kritieke entiteit, waarbij gewaarborgd wordt dat de criteria en drempelwaarden correct worden toegepast. Het NCCN vraagt ten slotte ook de dreigingsanalyses aan bij het OCAD, dewelke opgesteld worden voor elke sector of deelsector.

De KI-wet maakt nog een onderscheid tussen nationale kritieke infrastructuur en Europese Infrastructuur (hierna "EKI"), waarbij EKI's werden gedefinieerd als zijnde "de nationale kritieke infrastructuur waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in ten minste twee lidstaten van de Europese Unie zou hebben of de kritieke infrastructuur die niet gelegen is op het Belgische grondgebied, maar op het grondgebied van een andere lidstaat van de Europese Unie, waarvan de onderbreking van de werking of de vernietiging een aanzienlijke weerslag zou hebben in ten minste twee lidstaten van de Europese Unie, waaronder België". Deze categorie werd niet hernomen in de CER-Richtlijn. Echter wordt, gelet op de onderlinge afhankelijkheid en mogelijkheid tot grensoverschrijdende gevolgen, bijzondere aandacht gegeven aan kritieke entiteiten die essentiële diensten verlenen aan of in meer dan 6 lidstaten. De CER-Richtlijn legt aan deze entiteiten een apart statuut op van 'Kritieke Entiteit van Bijzonder Europees Belang'. De Commissie kan in dergelijk geval adviesmissies organiseren om de door die entiteit genomen weerbaarheidsmaatregelen te beoordelen. Gevolg is dat de kritieke entiteiten die in andere lidstaten essentiële diensten verlenen, maar niet aan de drempel van zes of meer lidstaten voldoen, in dit ontwerp geen speciaal statuut meer kunnen krijgen. Het spreekt voor zich dat het nog steeds mogelijk is om een bilaterale of multilaterale samenwerking op te richten. De CER-Richtlijn benadrukt deze mogelijkheid ook in artikel 11.

De kritieke entiteit zal een weerbaarheidsplan moeten opstellen, met daarin de weerbaarheidsmaatregelen die de entiteit neemt om tegemoet te komen aan de risico's waaraan zij blootgesteld kan worden, dewelke zij onderzocht heeft in haar risicobeoordeling. De kritieke entiteit zelf is steeds in de eerste plaats verantwoordelijk om haar eigen weerbaarheid te waarborgen alsook dat van haar infrastructuur. Haar rol is dus essentieel voor het voorkomen van en het weerbaar zijn tegen elke gebeurtenis die van aard is om een verstoring van de werking of de vernietiging van de structuur met zich mee te brengen. Naast de weerbaarheidsmaatregelen, die intern in de entiteit genomen en uitgevoerd moeten worden, bestaan er ook externe

déjà et continuera à remplir ce rôle aujourd'hui est le Centre de Crise National (ci-après : NCCN). Elle n'est pas directement mentionnée dans la loi car, comme l'a déjà relevé la section législative du Conseil d'Etat, notamment dans son avis 63.296/4, désigner directement les services de l'exécutif mis en place par le Roi et nommés auprès de lui serait une ingérence du pouvoir législatif dans l'organisation interne de l'exécutif.

Le NCCN est responsable de la coordination avec les forces de police et de sécurité, et peut, si nécessaire, imposer des mesures supplémentaires pour protéger les entités critiques. En outre, le NCCN soutient les autorités sectorielles au cours de la procédure d'identification des entités critiques. Le NCCN conseille également les autorités sectorielles sur le dossier d'identification d'une entité critique, en veillant à ce que les critères et les seuils soient correctement appliqués. Enfin, le NCCN demande également à l'OCAD des évaluations de la menace, qui sont établies pour chaque secteur ou sous-secteur.

La loi IC établit une autre distinction entre les infrastructures critiques nationales et les infrastructures critiques européennes (ci-après dénommées : « ICE »). Les ICE étaient définies comme étant « les infrastructures critiques nationales dont la perturbation du fonctionnement ou la destruction aurait un impact important dans au moins deux Etats membres de l'Union européenne, ou les infrastructures critiques qui ne sont pas situées sur le territoire belge, mais sur le territoire d'un autre Etat membre de l'Union européenne, dont la perturbation du fonctionnement ou la destruction aurait un impact important dans au moins deux Etats membres de l'Union européenne, y compris la Belgique. Toutefois, une attention particulière est accordée, compte tenu de l'interdépendance et de la possibilité de répercussions transfrontalières, aux entités critiques qui fournissent des services essentiels à six Etats membres ou plus. La Directive CER impose à ces entités un statut distinct d'entité critique revêtant une importance européenne particulière'. Le cas échéant, la Commission peut organiser des missions consultatives pour évaluer les mesures de résilience prises par cette entité. Par conséquent, les entités critiques qui fournissent des services essentiels dans d'autres Etats membres, mais qui n'atteignent pas le seuil de six Etats membres ou plus, ne peuvent plus bénéficier d'un statut spécial en vertu de ce projet. Bien entendu, il est toujours possible d'établir une coopération bilatérale ou multilatérale. La directive CER souligne également cette possibilité à l'article 11.

L'entité critique devra élaborer un plan de résilience contenant les mesures de résilience qu'elle adopte pour faire face aux risques auxquels elle peut être confrontée et qu'elle a examinés dans le cadre de son évaluation des risques. L'entité critique est toujours chargée en premier lieu de garantir sa propre résilience et celle de ses infrastructures. Son rôle est donc essentiel pour prévenir et pour résister à tout événement de nature à entraîner une interruption du fonctionnement ou la destruction de la structure. Outre les mesures de résilience qui doivent être prises et mises en œuvre au sein même de l'entité, il existe des mesures de protection externes que les autorités compétentes peuvent adopter.

beschermingsmaatregelen, dewelke door de bevoegde autoriteiten kunnen genomen worden.

De vermelding in deze wet van deze externe beschermingsmaatregelen is niet noodzakelijk aangezien deze hun wettelijke basis gekregen hebben in artikelen 7/1 tot 7/3, 14 en 17 van de wet op het politieambt van 5 augustus 1992, en artikelen 61, 62 en 97, eerste lid, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Bijgevolg bestaat de mogelijkheid tot externe beschermingsmaatregelen ongeacht of dit in de huidige wet wordt hernomen. Om de inhoud van de wet niet onnodig te verzwaren en om herhaling te voorkomen, werd ervoor gekozen om de bepalingen betreffende de externe beschermingsmaatregelen niet opnieuw op te nemen in het voorliggende voorstel.

Het NCCN is bevoegd om in functie van het type dreiging externe beschermingsmaatregelen ten aanzien van kritieke entiteiten te nemen, hetzij op basis van een dreigingsanalyse zoals bedoeld in artikel 8, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, op haar verzoek of ambtshalve uitgevoerd door het OCAD, hetzij op basis van een analyse uitgevoerd door de diensten van de federale politie of de inlichtingen- en veiligheidsdiensten voor de andere dreigingen dan die bedoeld in artikel 3 van de voormelde wet en die onder hun bevoegdheid vallen. De externe beschermingsmaatregelen staan los van de weerbaarheidsmaatregelen die op grond van deze wet genomen moeten worden.

De burgemeester, die als eerste verantwoordelijk is voor de veiligheid op het grondgebied van zijn gemeente, kan welteverstaan ertoe worden gebracht externe beschermingsmaatregelen te moeten nemen, mits deze niet strijdig zijn met die waartoe het NCCN heeft beslist.

Om te zorgen voor een integrale aanpak betreffende de weerbaarheid van kritieke entiteiten moet elke lidstaat tevens beschikken over een Strategie om de weerbaarheid van kritieke entiteiten te versterken. De strategie wordt opgesteld door het NCCN, op basis van input van de sectorale overheden, moet de uit te voeren strategische doelstellingen en beleidsmaatregelen bevatten, en wordt meegedeeld aan de Commissie. Deze strategie zal de realiteit beschrijven van het beleid dat gevoerd wordt betreffende de weerbaarheid van kritieke entiteiten.

De CER richtlijn is niet van toepassing op aangelegenheden die vallen onder Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad (hieronder "NIS 2 Richtlijn"), Echter, gelet op het belang van cyberbeveiliging voor de weerbaarheid van kritieke entiteiten en met het oog op consistentie, werd in dit wetsvoorstel gezorgd voor een aanpak die coherent is met zowel de CER-Richtlijn als met de NIS 2-Richtlijn. Gezien de hogere frequentie en bijzondere kenmerken van cyber risico's legt de NIS 2-Richtlijn een grote groep entiteiten brede voorschriften op om hun weerbaarheid te waarborgen. Gelet op de grote mate van verwevenheid van fysieke infrastructuur en cyber infrastructuur, kunnen deze twee wetgevende kaders niet los gezien worden van elkaar. Daarnaast zullen kritieke entiteiten die

La mention de ces mesures de protection externes dans la présente loi n'est pas nécessaire étant donné que leur base légale figure dans les articles 7/1 à 7/3, 14 et 17 de la loi du 5 août 1992 sur la fonction de police, et sur les articles 61, 62 et 97, paragraphe 1^{er}, de la loi du 7 décembre 1998 organisant police intégré et structuré à deux niveaux. Par conséquent, la possibilité de mesures de protection externe existe indépendamment du fait qu'elle soit rétablie dans la loi actuelle. Afin de ne pas alourdir inutilement le contenu de la loi et d'éviter les répétitions, il a été choisi de ne pas rétablir les dispositions relatives aux mesures de protection extérieure dans la présente proposition.

Le NCCN est autorisé à prendre des mesures de protection externe à l'égard des entités critiques, en fonction du type de menace, soit sur la base d'une analyse de la menace visée à l'article 8, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, effectuée à sa demande ou d'office par l'OCAM, soit sur base d'une analyse effectuée par les services de police fédérale ou les services de renseignement et de sécurité pour les menaces autres que celles visées à l'article 3 de la loi précitée et relevant de leur compétence. Les mesures de protection extérieure sont distinctes des mesures de résilience à prendre en vertu de cette loi.

Le bourgmestre, qui est le premier responsable de la sécurité sur le territoire de sa commune, peut être amené à prendre des mesures de protection extérieure, pour autant qu'elles ne soient pas contraires à celles décidées par le NCCN.

Afin de veiller à une approche intégrale sur la résilience des entités critiques, chaque Etat membre doit également disposer d'une Stratégie visant à renforcer la résilience des entités critiques. La stratégie est établie par le NCCN, sur la base des contributions des autorités sectorielles, doit contenir les objectifs stratégiques et les mesures à mettre en œuvre et est communiquée à la Commission. Cette stratégie décrira la réalité des politiques menées en matière de résilience des entités critiques.

La directive CER ne s'applique pas aux matières couvertes par la directive (UE) 2022/2555 du Parlement européen et du Conseil (ci-dessous Directive NIS 2), Toutefois, vu l'importance de la cybersécurité pour la résilience des entités critiques et par souci de cohérence, le présent projet de loi prévoit une approche qui est en cohérence tant avec la Directive CER qu'avec la Directive NIS 2. Etant donné la fréquence accrue et les particularités des cyber-risques, la Directive NIS 2 impose à un grand groupe d'entités des règles étendues afin de garantir leur résilience. Vu le degré élevé d'interconnexion entre l'infrastructure physique et la infrastructure cyber, ces deux cadres législatifs ne peuvent être dissociés. En outre, les entités critiques identifiées sur la base de la présente loi deviendront de plein droit des entités

geïdentificeerd worden op grond van deze wet, van rechtswege essentiële entiteiten worden onder de NIS 2-Richtlijn, waardoor een goede samenwerking en vlotte informatie-uitwisseling met het Centrum voor Cybersecurity België in dit kader belangrijk is.

Het Unierecht legt financiële entiteiten en digitale infrastructuur entiteiten vergaande voorschriften op om alle risico's waarmee zij te maken krijgen, te beheersen en bedrijfscontinuïteit te waarborgen.⁷ Dit specifieke regime voor de sectoren van de digitale infrastructuur, de financiële marktinfrastructuur en het bankwezen heeft als gevolg dat de CER-Richtlijn bepaalt dat de verplichtingen vastgelegd in artikel 11 en de Hoofdstukken III, IV en VI niet van toepassing zijn op entiteiten die behoren tot deze sectoren.

Men zal opmerken dat dit ontwerp de openbare veiligheid betreft en dus onder de bevoegdheid van de Federale Staat valt. In het federale België is het beleidsdomein veiligheid en ordehandhaving een quasi-integraal federale materie. Zo is de federale overheid op basis van haar residuaire bevoegdheid voor de preventieve bescherming op het gebied van openbare veiligheid bevoegd voor de beveiliging van kritieke infrastructuren.

In haar advies betreffende de KI-wet oordeelde de Raad van State dat "de omzetting van de ECI-Richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort."^{8,9} Naast de algemene preventieve bescherming van kritieke infrastructuren, is de federale overheid ook residuaire bevoegd voor de strijd tegen radicalisme, extremisme, terrorisme en de bescherming van de infrastructuur tegen terroristische aanslagen.¹⁰ De bevoegdheid van de federale overheid gaat dus verder dan het louter beschermen van kritieke infrastructuren tegen terroristische aanslagen. Het gaat om een algemene preventieve beschermingsbevoegdheid.

essentiële conformément à la Directive NIS 2. Dans ce contexte, une bonne collaboration et un échange fluide d'informations avec le Centre pour la Cybersécurité Belgique sont donc importants.

Le droit de l'Union impose aux entités financières et aux entités digitales des prescriptions poussées afin de maîtriser tous les risques auxquels elles sont confrontées et de garantir la continuité de leurs activités.⁷ En raison de ce régime spécifique pour les secteurs de l'infrastructure numérique, de l'infrastructure des marchés financiers et le secteur bancaire, la Directive CER stipule que les obligations prévues à l'article 11 et aux Chapitres III, IV et VI ne s'appliquent pas aux entités qui relèvent de ces secteurs.

On remarquera que ce projet porte sur la sécurité publique et relève dès lors de la compétence de l'Etat fédéral. En Belgique fédérale, le domaine politique de la sécurité et de l'ordre public est une matière fédérale quasi-intégrale. Le gouvernement fédéral est ainsi responsable de la sécurité des infrastructures critiques sur la base de sa compétence résiduelle en matière de protection préventive dans le domaine de la sécurité publique.

Dans son avis sur la loi IC, le Conseil d'Etat a jugé que "la transposition de la Directive ICE conduit essentiellement à la mise en œuvre de la matière de la protection préventive dans le domaine de la sécurité publique, qui relève de la compétence résiduelle exclusive du législateur fédéral".^{8,9}

Outre la protection préventive générale des infrastructures critiques, le gouvernement fédéral dispose également d'une compétence résiduelle en matière de lutte contre le radicalisme, l'extrémisme, le terrorisme et la protection des infrastructures contre les attaques terroristes.¹⁰ La compétence du gouvernement fédéral va donc au-delà de la simple protection des infrastructures critiques contre les attaques terroristes. Il s'agit d'une compétence générale de protection préventive. La nouvelle Directive CER réaffirme cette "approche tous risques", sans établir de

⁷ Verordeningen (EU) nr. 648/2012, (EU) nr. 575/2013, (EU) nr. 600/2014 van het Europees parlement en de Raad en Richtlijnen 2013/36/EU en 2014/65/EU van het Europees Parlement en de Raad, recent aangevuld met Verordening (EU) 2022/2554 van het Europees Parlement en de Raad.

⁸ Règlements (UE) n° 648/2012, (UE) n° 575/2013, (UE) n° 600/2014 du Parlement européen et du Conseil, et Directives 2013/36/UE et 2014/65/UE du Parlement européen et du Conseil, récemment complétées par le Règlement (UE) 2022/2554 du Parlement européen et du Conseil.

⁹ Zie o.m. Adv.RvS nr. 38.278/AV van 16 mei 2006 over een voorstel van decreet houdende wijziging en aanvulling van het decreet van 28 februari 2003 betreffende het Vlaamse inburgeringsbeleid met een hoofdstuk VIII houdende het verbieden van het dragen van gelaatsverhullende gewaden, doorgaans aangeduid als "boerka", Parl.St. VI.Parl. 2004-2005, nr. 159/2, 10; Adv.RvS nr. 44.771/3 van 15 juli 2008 over een ontwerp van besluit van de Vlaamse Regering houdende de normen voor de preventie van brand in de voorzieningen voor kinderopvang, 3; Adv.RvS nr. 48.989/VR van 9 december 2010 over een voorontwerp van wet betreffende de kritieke infrastructuur, de andere punten van federaal belang en de punten van lokaal belang, Parl.St. Kamer 2010-2011, nr. 53-1357/1, 54.

⁹ Adv.RvS nr. 48.989/VR, 53-54; Adv.RvS nr. 63.296/4 van 2 mei 2018 over een voorontwerp van wet tot vaststelling van een kader voor de beveiliging van network- en informatiesystemen van algemeen belang voor de openbare veiligheid, Parl.St. Kamer 2018-2019, nr. 54-3340/1, 75-79; K. REYBROUCK en S. SOTTIAUX, *De federale bevoegdheden*, 254-259.

¹⁰ Adv.RvS nr. 57.106/VR/3, 27-28; Adv.RvS nr. 64.489/3 van 22 november 2018 over een voorontwerp van decreet van de Vlaamse Gemeenschap houdende instemming met het verdrag van de Raad van Europa ter voorkoming van terrorisme, gedaan te Warschau op 16 mei 2005, Parl.St. VI.Parl. 2018-2019, nr. 1796/1, 17-18.

⁸ Avis C.E., n° 38.278/AV du 16 mai 2006 sur une proposition de décret modifiant et complétant le décret du 28 février 2003 relatif à la politique flamande d'intégration par un chapitre VIII interdisant le port de robes dissimulant le visage, communément appelées « burka », *Doc. Parl.* 2004-2005, n° 159/2, 10; Avis C.E. n° 44.771/3 du 15 juillet 2008 relatif à un projet d'arrêté du Gouvernement Flamand contenant les normes de prévention des incendies dans les structures d'accueil pour enfants, 3; Avis C.E. n° 48.989/VR du 9 décembre 2010 sur un avant-projet de loi sur les infrastructures critiques et autres points d'intérêt fédéral, *Doc. Parl.* 2010-11, n° 53-1357/001, 54.

⁹ Avis C.E. n° 63.296/4 du 2 mai 2018 sur un avant-projet de loi établissant un cadre pour la sécurité des systèmes de réseaux et d'information d'intérêt général de sécurité publique, *Doc. Parl.* 2018-2019, n° 54-3340/1, 75-79; K. REYBROUCK et S. SOTTIAUX, *De federale bevoegdheden*, 254-259.

¹⁰ Avis C.E., n° 57.106/VR/3, 27-28; Avis C.E., n° 64.489/3 du 22 novembre 2018 sur un avant-projet de décret de la Communauté flamande portant approbation de la Convention du Conseil de l'Europe pour la prévention du terrorisme, faite à Varsovie le 16 mai 2005, *Doc. Parl.* 2018-2019, n° 1796/1, 17-18.

De nieuwe CER-Richtlijn herneemt deze "alle-risico's aanpak", zonder enige prioritering tussen de soorten dreigingen, aangezien er sprake is van een dynamisch dreigingslandschap. Het is duidelijk dat beide richtlijnen uitgaan van eenzelfde "alle-risico's aanpak" al werd er in de huidige ECI-Richtlijn voorrang gegeven aan de bestrijding van terroristische dreigingen. De omzetting van de CER-Richtlijn valt daarom eveneens onder de bovengenoemde algemene preventieve beschermingsbevoegdheid van de federale overheid.

De in dit ontwerp te vinden evolutie van kritieke infrastructuur naar kritieke entiteit wijzigt niets aan de grondslag van de wetgeving. Deze blijft zich gronden in het gebied van de openbare veiligheid. Het doel van dit ontwerp is namelijk net om de bescherming en beveiliging van kritieke entiteiten te verhogen, en om deze entiteiten weerbaar te maken tegen alle mogelijke soorten risico's. Kritieke entiteiten zijn vitaal in onze samenleving, aangezien zij hieraan essentiële diensten verlenen die noodzakelijk zijn voor haar instandhouding en vooruitgang. De kritieke entiteiten moeten zich voorbereiden op de gevolgen die al deze soorten risico's kunnen hebben op hun infrastructuur door het nemen van gepaste maatregelen. Deze maatregelen worden niet genomen met het doel om de risico's zelf te mitigeren, wat een belangrijke nuance inhoudt. Zo zullen kritieke entiteiten maatregelen moeten nemen om natuurlijke risico's te mitigeren ten aanzien van hun eigen kritieke infrastructuur. Dit brengt niet met zich mee dat deze maatregelen genomen moeten worden om de klimaatverandering in het algemeen te mitigeren. De genomen maatregelen hebben steeds een duidelijke veiligheidsdimensie.

Voor wat betreft de inspecties van de weerbaarheidsmaatregelen, die uitgevoerd moeten worden door de inspectiedienst, dient fragmentatie te worden vermeden aangezien de maatregelen één geheel vormen, en als geheel beoordeeld moeten worden om efficiënt te kunnen controleren of deze maatregelen volstaan om de weerbaarheid van de kritieke entiteiten te waarborgen. De inspecties dienen aldus afgestemd en gecoördineerd te worden in één inspectiedienst. Doch is het op grond van de delegatie die gegeven wordt aan de Koning mogelijk dat sectorale overheden, indien zij dit opportuun en noodzakelijk achten, de gefedereerde entiteiten hierbij kunnen betrekken. De maatregelen zullen door de inspectiedienst niet ten gronde zelf worden beoordeeld, maar op basis van hun effectiviteit voor de bescherming van de kritieke entiteiten, in het kader van het reglementeren van de openbare veiligheid.

Artikel 26 van de CER-Richtlijn bepaalt dat de Richtlijn uiterlijk op 17 oktober 2024 omgezet moet zijn. Bijgevolg treedt deze wetgeving best van kracht voor of ten laatste op deze datum, zodat het proces van identificatie en aanduiding van start kan gaan. Zo niet, stelt de Belgische Staat zich bloot aan inbreukprocedures, ofwel omwille van laattijdige omzetting, ofwel wegens slechte uitvoering van het Europese recht, wat dient te worden vermeden.

De sectorale overheden zullen voor hun bevoegde sectoren de verplichtingen uit deze wet moeten implementeren. Bijgevolg is het waarschijnlijk dat er op

prioriteiten entre les types de menaces, étant donné que le paysage des menaces est dynamique. Il est clair que les deux directives reposent sur la même "approche tous risques", bien que la Directive ICE actuelle donnait la priorité à la lutte contre les menaces terroristes. Par conséquent, la transposition de la Directive CER relève également du pouvoir général de protection préventive susmentionné du gouvernement fédéral.

L'évolution de la notion d'infrastructure critique à celle d'entité critique que l'on trouve dans ce projet ne modifie pas la base de la législation. Celle-ci reste ancrée dans le domaine de la sécurité publique. En effet, l'objectif de ce projet est précisément d'accroître la protection et la sécurité des entités critiques et de les rendre résistantes à toutes sortes de risques. Les entités critiques sont vitales pour notre société, car elles lui fournissent des services essentiels à son maintien et à son progrès. Les entités critiques doivent se préparer aux conséquences que tous ces types de risques peuvent avoir sur leurs infrastructures, en adoptant des mesures adéquates. Ces mesures ne sont pas prises dans le but d'atténuer les risques proprement dits, ce qui constitue une nuance importante. Les entités critiques devront donc adopter des mesures pour atténuer les risques naturels en ce qui concerne leurs propres infrastructures critiques. Cela ne signifie pas que ces mesures doivent être prises pour atténuer le changement climatique en général. Les mesures prises ont toujours une dimension sécuritaire évidente.

En ce qui concerne les inspections des mesures de résilience, qui doivent être effectuées par le service d'inspection, il s'agit d'éviter toute fragmentation, car les mesures forment un tout et doivent être évaluées dans leur ensemble afin de pouvoir vérifier efficacement si elles sont suffisantes pour garantir la résilience des entités critiques. Les inspections devraient donc être alignées et coordonnées au sein d'un seul service d'inspection. Toutefois, en vertu de la délégation donnée au Roi, il est possible pour les autorités sectorielles, si elles le jugent opportun et nécessaire, d'y associer les entités fédérées. Ces mesures seront évaluées par le service d'inspection non pas sur le fond, mais sur la base de leur efficacité en termes de protection des entités critiques, dans le cadre de la réglementation de la sécurité publique.

L'article 26 de la Directive CER précise que la Directive doit être transposée au plus tard le 17 octobre 2024. Il est donc préférable que cette législation entre en vigueur avant ou au plus tard à cette date, afin que le processus d'identification et de désignation puisse être entamé. A défaut, l'Etat belge s'expose à des procédures d'infraction, soit pour transposition tardive, soit pour mauvaise application du droit européen, ce qu'il s'agit d'éviter.

Les autorités sectorielles doivent se conformer aux obligations découlant de la présente loi pour leurs secteurs de compétence. Par conséquent, il est probable

dat niveau een budgettaire impact bestaat. Dit ontwerp voorziet tevens voor verschillende bepalingen, zoals onder andere voor de inspecties en audits, een delegatie aan de Koning. Deze sectorale Koninklijke Besluiten kunnen een budgettaire impact met zich meebrengen, aangezien er bijvoorbeeld mogelijks nieuwe inspectiediensten moeten worden opgericht. De sectorale overheid is het best geplaatst om de budgettaire impact voor haar sector in te schatten.

ARTIKELSGEWIJZE BESPREKING

HOOFDSTUK 1

Algemene bepalingen

Artikel 1

Overeenkomstig artikel 83 van de Grondwet verduidelijkt artikel 1 van dit wetsontwerp welke aangelegenheid het voornemens is te regelen.

Artikel 2

Artikel 2 van het ontwerp omschrijft het voorwerp van de wet en geeft aldus uitvoering aan de verplichting van artikel 26, tweede lid, van de Richtlijn om naar deze laatste te verwijzen bij de publicatie van de aangenomen bepalingen door een lidstaat om zich aan deze te conformeren.

HOOFDSTUK 2

Definities

Artikel 3

Dit artikel bevat de definities die in het ontwerp van wet zijn gebruikt en zorgt daardoor voor de omzetting van artikel 2 van de Richtlijn.

1°: deze definitie behoeft geen opmerkingen.

2° "Sectorale overheid": deze definitie bepaalt welke overheid voor een bepaalde sector bevoegd is.

De sectorale overheden die, voor hun respectievelijke sector, belast zijn met de uitvoering en het toezicht op de uitvoering van de bepalingen van de wet, worden aangewezen door de wet of door de Koning bij in Ministerraad overleg besluit. Dit laat toe om nieuwe sectorale overheden op te richten, met name bestaande uit vertegenwoordigers van de federale en gefedereerde entiteiten, op basis van artikel 92^{ter} van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

Zo werd reeds het 'Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater' opgericht¹¹,

qu'il y ait un impact budgétaire à ce niveau. En effet, ce projet prévoit une délégation au Roi pour plusieurs dispositions, telles que les inspections et les audits, entre autres. Ces arrêtés royaux sectoriels peuvent avoir un impact budgétaire, car de nouveaux services d'inspection peuvent devoir être créés, par exemple. Le gouvernement sectoriel est le mieux placé pour évaluer l'impact budgétaire pour son secteur.

COMMENTAIRE DES ARTICLES

CHAPITRE 1^{er}

Dispositions générales

Article 1^{er}

Conformément à l'article 83 de la Constitution, l'article 1^{er} du présent projet précise la matière qu'il entend régler.

Article 2

L'article 2 du projet définit l'objet de la loi et exécute ainsi l'obligation imposée par l'article 26, alinéa 2, de la Directive de mentionner la référence à cette dernière lors de la publication des dispositions adoptées par un État membre en vue de se conformer à celle-ci.

CHAPITRE 2

Définitions

Article 3

Cet article contient les définitions utilisées dans le projet de loi et assure ce faisant la transposition de l'article 2 de la Directive.

1°: cette définition n'appelle pas de remarques particulières.

2° « Autorité sectorielle »: cette définition détermine l'autorité compétente pour un secteur déterminé.

Les autorités sectorielles qui sont chargées, pour leur secteur respectif, de la mise en œuvre et du contrôle de l'exécution des dispositions légales, sont désignées par la loi ou par le Roi dans un arrêté délibéré en Conseil des ministres. Cela permet la création de nouvelles autorités sectorielles, composées notamment de représentants des entités fédérales et fédérées, sur la base de l'article 92^{ter} de la loi spéciale du 8 août 1980 de réformes institutionnelles.

C'est ainsi qu'a déjà été créé le 'Comité national de la sécurité pour la fourniture et la distribution d'eau potable'

¹¹ KB van 31 juli 2020 houdende de oprichting en organisatie van het Nationaal comité voor de beveiliging van de levering en distributie van drinkwater, BS 20 augustus 2020.

dat dienst doet als sectorale overheid in de sector drinkwater en werd samengesteld uit vertegenwoordigers van de Federale Staat, het Vlaams Gewest, het Brussels Hoofdstedelijk Gewest en het Waals Gewest.

Punten 3° tot 9° beschrijven de verschillende basistermen die gebruikt worden in het wetsontwerp betreffende de weerbaarheid van kritieke entiteiten.

Punt 3° beschrijft het begrip kritieke entiteit. Dit is de definitie die in de Richtlijn staat. Het betreft een zeer algemene definitie, aangezien een entiteit, uit de bijlage, steeds de identificatieprocedure dient te doorlopen alvorens geïdentificeerd en aangeduid te kunnen worden als kritieke entiteit. Tijdens deze identificatieprocedure worden criteria verduidelijkt op basis waarvan de entiteit als kritiek kan worden beschouwd.

4°: "Weerbaarheid": de CER-Richtlijn introduceerde deze term. De definitie komt uit de Richtlijn. In tegenstelling tot de KI-wet, waar de focus ligt op fysieke beveiliging en bescherming, breidt de Richtlijn deze focus uit door het gebruik van deze term. "Weerbaarheid" betekent namelijk veel meer dan enkel de fysieke beveiliging en bescherming, het houdt ook in dat entiteiten weerstand kunnen bieden aan en het kunnen mitigeren en absorberen, verwerken en herstellen van incidenten, in het kader van de bescherming van de nationale veiligheid.

Punt 5° komt uit de CER-Richtlijn en behoeft geen specifieke opmerkingen.

Punt 6° beschrijft de term kritieke infrastructuur. Dit is de definitie die in de Richtlijn staat. Deze term dient, in combinatie met punt 3°, begrepen te worden als onderdeel van de kritieke entiteit. Het onderscheid tussen deze twee termen is belangrijk om voor ogen te houden bij het opstellen en implementeren van de weerbaarheidsmaatregelen. Beide termen zijn namelijk niet los te lezen van elkaar. Het is de kritieke entiteit die in de eerste plaats geïdentificeerd en aangeduid zal worden. Als logische aanvulling op de CER-Richtlijn, wordt er in dit wetsontwerp daarnaast ook de identificatie opgelegd van de kritieke infrastructuur van een kritieke entiteit. De kritieke entiteit zelf heeft namelijk steeds fysieke infrastructuur nodig die noodzakelijk is voor de verlening van zijn essentiële dienst, en deze infrastructuur moet zich bevinden op het Belgische grondgebied. Het kan voorkomen dat een kritieke entiteit op verschillende en andere locaties in België kritieke infrastructuur bezit, dan waar zijn hoofdzetel gevestigd is. Het volstaat niet om enkel de hoofdzetel fysiek te beveiligen als de essentiële dienstverlening hiernaast afhankelijk is van infrastructuur op andere locaties in het land. Het is ook mogelijk dat een kritieke entiteit naast kritieke infrastructuur, ook niet-kritieke infrastructuur bezit. Dankzij het gebruik van beide termen kunnen deze belangrijke nuances, dewelke ontbreken op Europees niveau, wel gelegd worden op nationaal niveau.

Punten 8° tot 11°: bij deze concepten zijn geen specifieke opmerkingen nodig.

¹¹, qui fait office d'autorité sectorielle dans le secteur de l'eau potable et est composé de représentants de l'Etat fédéral, de la Région flamande, de la Région de Bruxelles-Capitale et de la Région wallonne.

Les points 3° à 9° décrivent les différents termes de base qui sont utilisés dans le projet de loi sur la résilience des entités critiques.

Le point 3° décrit la notion d'entité critique. Il s'agit de la définition qui figure dans la Directive. Il s'agit d'une définition très générale, dans la mesure où une entité, de l'annexe, doit toujours parcourir la procédure d'identification avant de pouvoir être identifiée et désignée comme entité critique. Durant cette procédure, les critères sur la base desquels l'entité peut être considérée comme critique sont précisés.

4°: "Résilience": la Directive CER a introduit ce terme. La définition découle de cette Directive. Contrairement à la loi IC, qui met l'accent sur la sécurité physique et la protection, la Directive étend la définition de par l'utilisation de ce terme. En effet, la "résilience" va bien au-delà de la sécurité physique et de la protection, car elle implique également que les entités puissent faire face aux incidents, les mitiger et les absorber, les traiter et s'en rétablir, dans le cadre de la protection de la sécurité nationale.

Le point 5° est issu de la Directive CER et n'appelle pas de commentaires particuliers.

Le point 6° définit la notion d'infrastructure critique. Il s'agit de la définition qui figure dans la Directive. En combinaison avec le point 3°, ce terme doit être compris comme faisant partie de l'entité critique. Il est important de garder à l'esprit la distinction entre ces deux termes lors de l'élaboration et de la mise en œuvre des mesures de résilience. Ces deux termes sont en effet indissociables. C'est l'entité critique qui sera identifiée et désignée en premier lieu. En complément logique de la Directive CER, le présent projet de loi impose également l'identification de l'infrastructure critique d'une entité critique. L'entité critique a en effet toujours besoin de l'infrastructure physique nécessaire à la fourniture de ses services essentiels et cette infrastructure doit se situer sur le territoire belge. Il se peut qu'une entité critique possède des infrastructures critiques dans plusieurs endroits en Belgique et dans des lieux autres que le siège central. Il ne suffit pas de sécuriser physiquement le siège central si la fourniture de services essentiels dépend d'infrastructures situées dans d'autres endroits du pays. Il se peut également qu'une entité critique possède, outre une infrastructure critique, une infrastructure non-critique. Grâce à l'utilisation des deux termes, ces nuances importantes, qui font défaut au niveau européen, peuvent être mises en exergue au niveau national.

Les points 8° à 11°: ces concepts n'appellent aucune remarque spécifique.

¹¹ AR du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable, M.B. 20 août 2020.

Voor de definitie van een overheidsinstantie verduidelijkt artikel 2.10 van de CER-Richtlijn dat het begrip overeenkomstig het nationale recht als zodanig erkend moet zijn, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom werd er gekozen te verwijzen naar bestaande begrippen in het Belgisch recht die de betrokken entiteiten omvatten, zodat er niet te veel verschillende begrippen zouden worden toegepast.

In dit geval verwijst de definitie naar het begrip "administratieve overheid" als bedoeld in artikel 14, §1, eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, waaraan criteria zijn toegevoegd: zij behoort tot de federale staat, zij mag niet van industriële of commerciële aard zijn, niet hoofdzakelijk een activiteit uitvoeren die tot een van de andere sectoren of deelsectoren opgenomen in de bijlage bij dit wetsontwerp behoort en geen privaatrechtelijke rechtspersoon zijn.

Deze keuze wordt verklaard door het feit dat de meeste criteria in de definitie van de CER-Richtlijn terug te vinden zijn in de criteria die het begrip "administratieve overheid" als bedoeld in de gecoördineerde wetten op de Raad van State afbakenen.

HOOFDSTUK 3

Toepassingsgebied

Artikel 4

Dit artikel bepaalt het toepassingsgebied van dit ontwerp, namelijk de sectoren opgesomd in de bijlage. Dit artikel, in combinatie met de bijlage bij het ontwerp, zet aldus de bijlage van de Richtlijn om.

Wat betreft de energiesector, bepaalt de vijfde overweging van de Richtlijn dat de "elektriciteitsproductie ook de transmissieonderdelen van kerncentrales [kan] omvatten, maar niet de specifiek nucleaire elementen die vallen onder de vigerende nucleaire wetgeving". Het is deze uitsluiting die het tweede lid van deze paragraaf voorziet, verwijzend naar de nucleaire installaties bedoeld in de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortvloeiende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle. Enkel de elementen van een nucleaire installatie bestemd voor de industriële productie die dienen voor de transmissie van de elektriciteit kunnen dus vallen binnen het toepassingsgebied van deze wet. Dit werd op dezelfde manier geregeld in de KI-wet.

Artikel 5

Paragraaf 1 bepaalt dat wanneer bepalingen van sectorspecifieke rechtshandelingen van de Unie aan kritieke entiteiten uit de sectoren bankwezen, financiële markt infrastructuur en digitale infrastructuur, voorschrijven om maatregelen te nemen die hun

Pour la définition d'une entité de l'administration publique, l'article 2.10 de la directive CER précise que la notion doit être reconnue comme telle conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales. Ainsi, il a été choisi de faire référence à des notions existantes en droit belge qui couvrent les entités concernées afin de ne pas multiplier l'application de notions différentes.

En l'occurrence, la définition reprend la notion d'autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées du 12 janvier 1973 sur le Conseil d'État, à laquelle sont rajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs repris dans les annexes du présent projet de loi et de ne pas être une personne morale de droit privé.

Ce choix s'explique de par le fait que la plupart des critères repris dans la définition de la directive se retrouvent dans les critères qui délimitent la notion d'autorité administrative au sens des lois coordonnées sur le Conseil d'État.

CHAPITRE 3

Champ d'application

Article 4

Cet article définit le champ d'application du présent projet, à savoir les secteurs énumérés en annexe. Combiné à l'annexe du projet, cet article transpose donc l'annexe de la Directive.

En ce qui concerne le secteur de l'énergie, le cinquième considérant de la Directive énonce que "la production d'électricité [peut] englober les éléments des centrales nucléaires servant au transport de l'électricité, tout en excluant les éléments strictement nucléaires, qui relèvent de la réglementation pertinente en matière nucléaire". C'est cette exclusion que prévoit le deuxième alinéa de ce paragraphe, faisant référence aux installations nucléaires visées par la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire. Seuls les éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité peuvent donc relever du champ d'application de la présente loi. Ce point était réglementé de la même manière dans la loi IC.

Article 5

Le paragraphe 1^{er} prévoit que, lorsque des dispositions d'actes juridiques sectoriels de l'Union imposent aux entités critiques des secteurs de la banque, d'infrastructure des marchés financiers et d'infrastructure digitale de prendre des mesures pour accroître leur

weerbaarheid vergroten, de desbetreffende bepalingen uit dit ontwerp niet van toepassing zijn, teneinde dubbel werk en onnodige last te voorkomen, en harmonisatie tussen de lidstaten te waarborgen. In dat geval gelden de relevante rechtsbepalingen van dergelijke rechtshandelingen. Deze aanpak zorgt voor consistentie tussen de CER-Richtlijn, de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad en de Verordening (EU) 2022/2554 van het Europees Parlement en de Raad betreffende digitale operationele weerbaarheid van de financiële sector. De Koning kan evenwel bepalen dat er in deze sectoren tot een hoger weerbaarheidsniveau moet gekomen worden, wanneer blijkt dat de sectorspecifieke regelgeving niet hetzelfde weerbaarheidsniveau kan garanderen.

Paragraaf 2 bevat een algemene equivalentiebepaling, dewelke bepaalt dat wanneer bepalingen van sector en deel-sectorspecifieke wetgeving vereisen dat kritieke entiteiten maatregelen nemen om hun weerbaarheid te vergroten, en als gelijkwaardig geacht worden door de Koning, deze verplichtingen uit hoofde van Hoofdstuk 4, Afdeling 2, Hoofdstuk 5 en Hoofdstuk 7 uit dit ontwerp niet van toepassing zijn op die entiteiten.

Artikel 6

De CER-Richtlijn bepaalt dat de Richtlijn geen afbreuk doet aan de bevoegdheden van de Lidstaten en hun autoriteiten op het gebied van bestuurlijke autonomie, en evenmin aan hun verantwoordelijkheid om de nationale veiligheid en defensie te waarborgen of hun bevoegdheid om andere essentiële staatsfuncties te beschermen, met name op het gebied van openbare veiligheid, territoriale integriteit en het handhaven van de openbare orde. Bijgevolg worden overheidsinstanties volledig uitgesloten van het toepassingsgebied van de wet indien de activiteiten hoofdzakelijk worden uitgevoerd op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten. Wanneer de activiteiten van de overheidsinstantie slechts zijdelings verband houdt met die gebieden, moeten zij evenwel vallen onder het toepassingsgebied van de wet.

Het kan voorkomen dat kritieke entiteiten uit andere sectoren hoofdzakelijk activiteiten verrichten op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten, of uitsluitend diensten verlenen aan overheidsinstanties die hoofdzakelijk activiteiten verrichten op die gebieden. Voor deze entiteiten moet besloten worden dat de verplichtingen uit de wet voor de kritieke entiteiten die zijn vastgelegd in de wet in Hoofdstuk 4, Afdeling 2, en Hoofdstukken 5 en 7, niet van toepassing zijn op deze kritieke entiteiten.

HOOFDSTUK 4

Afdeling 1

Identificatie en aanduiding van de kritieke entiteiten en kritieke infrastructures

résilience, les dispositions pertinentes du présent projet ne s'appliquent pas, afin d'éviter les doubles emplois et les charges inutiles, et d'assurer l'harmonisation entre les États membres. Dans ce cas, les dispositions pertinentes de ces actes juridiques s'appliqueront. Cette approche garantit la cohérence entre la Directive CER, la Directive (UE) 2022/2555 du Parlement européen et du Conseil et le Règlement (UE) 2022/2554 du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier. Toutefois, le Roi peut déterminer qu'un niveau de résilience plus élevé doit être atteint dans ces secteurs s'il apparaît que les réglementations sectorielles ne peuvent pas garantir le même niveau de résilience.

Le paragraphe 2 contient une disposition générale d'équivalence, qui prévoit que lorsque des dispositions de la législation sectorielle et sous-sectorielle exigent des entités critiques qu'elles prennent des mesures pour renforcer leur résilience, et qu'elles sont jugées équivalentes par le Roi, les obligations prévues au chapitre 4, à la section 2, au chapitre 5 et au chapitre 7 du présent projet ne s'appliquent pas à ces entités.

Article 6

La Directive CER précise qu'elle n'affecte pas les compétences des États membres et de leurs autorités en termes d'autonomie administrative, ni leur responsabilité en matière de sauvegarde de la sécurité et de la défense nationales, ni leur compétence en matière de protection d'autres fonctions essentielles de l'État, notamment la sécurité publique, l'intégrité territoriale et le maintien de l'ordre public. En conséquence, les organismes publics sont totalement exclus du champ d'application de la loi si les activités sont menées principalement dans le domaine de la sécurité nationale, de la sûreté publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales. Toutefois, si les activités de l'organisme public ne sont qu'indirectement liées à ces domaines, elles doivent entrer dans le champ d'application de la loi.

Il peut arriver que des entités critiques d'autres secteurs exercent des activités principalement dans les domaines de la sécurité nationale, de la sûreté publique, de la défense ou de l'application de la loi, y compris la recherche, la détection et la poursuite d'infractions pénales, ou fournissent exclusivement des services aux autorités publiques qui exercent des activités principalement dans ces domaines. Pour ces entités, il convient de décider que les obligations prévues par la loi pour les entités critiques au Chapitre 4, Section 2, et aux Chapitres 5 et 7 ne s'appliquent pas à ces entités critiques.

CHAPITRE 4

Section 1^{ère}

Identification et désignation des entités critiques et des infrastructures critiques

Artikel 7

Artikel 7 van dit ontwerp zet artikel 5 van de Richtlijn om en betreft de risico gebaseerde aanpak die de identificatieprocedure uit dit ontwerp onderbouwt.

De sectorale overheid stelt, als startpunt in de identificatieprocedure, een lijst op van essentiële diensten van de in de bijlage genoemde sectoren en deelsectoren die onder hun bevoegdheid vallen. De sectorale overheid baseert deze lijst op de lijst van essentiële diensten die werd opgesteld door de Commissie in de gedelegeerde Verordening (EU) van 27 juli 2023, op grond van artikel 5, eerste lid van de CER-Richtlijn. De sectorale overheid kan indien nodig aan deze lijst nog andere essentiële diensten, die zij geïdentificeerd hebben in hun welbepaalde sector of deelsector, toevoegen.

Paragraaf 2 houdt de verplichting in voor de sectorale overheid om een sectorale risicobeoordeling uit te voeren, alvorens kritieke entiteiten te kunnen identificeren. De verantwoordelijkheid hiervoor valt op de sectorale overheden, aangezien zij beschikken over de nodige expertise in hun welbepaalde sectoren of deelsectoren. Deze risicobeoordeling moet voor de eerste maal uitgevoerd worden uiterlijk op 17 januari 2026, en vervolgens telkens wanneer nodig en ten minste om de vier jaar. Deze risicobeoordeling zal hierna tijdens de identificatieprocedure gebruikt kunnen worden. Tijdens de identificatieprocedure zal men zowel rekening moeten houden met de risico's waaraan een entiteit kan blootgesteld worden, als de impact dat een verstoring van de werking op de essentiële dienstverlening met zich mee kan brengen.

Deze risicobeoordeling wordt tevens nadien gedeeld met de geïdentificeerde kritieke entiteiten. De sectorale overheden staan de kritieke entiteiten bij aan de hand van informatie-uitwisseling bij het nemen van de weerbaarheidsmaatregelen zoals voorzien in artikel 18. De financiële verantwoordelijkheid voor het nemen van deze maatregelen blijft evenwel steeds volledig bij de kritieke entiteit liggen.

De derde paragraaf omschrijft de inhoud van deze risicobeoordeling, door o.a. te vermelden met welke risico's men rekening moet houden tijdens het uitvoeren ervan. Bij het uitvoeren van de risicobeoordeling moet tevens rekening gehouden worden met andere algemene of sectorspecifieke risicobeoordelingen die krachtens andere rechtshandelingen van de Unie zijn verricht. Hieronder valt bijvoorbeeld de Belgian National Risk Assessment¹² (BNRA), dewelke een algemene risicobeoordeling inhoudt over alle mogelijke risico's waaraan België kan blootgesteld worden. De BNRA wordt gecoördineerd door het NCCN, met behulp van tal van experts, en de relevante informatie hiervan wordt gedeeld aan de bevoegde sectorale overheden zodat dit mee opgenomen kan worden in de sectorale risicobeoordeling. Tijdens het uitvoeren van de risicobeoordeling kan de sectorale overheid ook rekening houden met de risicobeoordeling die wordt uitgevoerd op grond van artikel 12, §1, lid 2, 1° van de [Codificatiewet].

Article 7

L'article 7 du présent projet transpose l'article 5 de la Directive et concerne l'approche basée sur les risques qui sous-tend la procédure d'identification visée par le projet.

Comme point de départ de la procédure d'identification, l'autorité sectorielle établit une liste des services essentiels des secteurs et sous-secteurs visés en annexe qui relèvent de leur compétence. L'autorité sectorielle base cette liste sur la liste des services essentiels qui a été établie par la Commission dans le Règlement délégué (UE) du 27 juin 2023, en vertu de l'article 5, premier alinéa de la Directive CER. Si nécessaire, l'autorité sectorielle peut ajouter à cette liste d'autres services essentiels qu'elle a identifiés dans son secteur ou sous-secteur déterminé.

Le paragraphe 2 oblige l'autorité sectorielle à mener une évaluation des risques sectoriels avant de pouvoir identifier les entités critiques. La responsabilité à cet égard incombe aux autorités sectorielles étant donné qu'elles disposent de l'expertise nécessaire dans leurs secteurs ou sous-secteurs déterminés. Cette évaluation des risques doit être effectuée pour la première fois le 17 janvier 2026 au plus tard, ensuite chaque fois que cela s'avère nécessaire et au moins tous les quatre ans. Elle pourra servir ensuite durant la procédure d'identification. Au cours du processus d'identification, il sera nécessaire d'examiner à la fois les risques auxquels une entité peut être exposée et l'impact qu'une interruption de fonctionnement peut avoir sur les services essentiels.

Cette évaluation des risques est également communiquée par la suite aux entités critiques identifiées. Les autorités sectorielles fournissent leur aide aux entités critiques en partageant des informations lors de la prise des mesures de résilience prévues à l'article 18. Toutefois, la responsabilité financière de ces mesures incombe toujours entièrement à l'entité critique.

Le troisième paragraphe définit le contenu de cette évaluation des risques, en mentionnant notamment les risques à prendre en compte au moment de sa réalisation. Durant l'évaluation des risques, il y a également lieu de tenir compte d'évaluations des risques générales ou sectorielles qui ont été menées en vertu d'autres actes juridiques de l'Union. C'est notamment le cas du Belgian National Risk Assessment¹² (BNRA), qui porte sur l'évaluation générale de tous les risques potentiels auxquels la Belgique peut être confrontée. Le BNRA est coordonné par le NCCN, avec l'aide de nombreux d'experts, et les informations pertinentes sont partagées avec les autorités sectorielles compétentes pour pouvoir être intégrées dans l'évaluation sectorielle des risques. Dans le cadre de cette évaluation des risques, l'autorité sectorielle peut également tenir compte de l'évaluation des risques réalisée en vertu de l'article 12, §1^{er}, alinéa 2, 1° de la [loi de codification]. Il existe en outre, dans certains secteurs, des législations sectorielles spécifiques,

¹² Art. 6, eerste lid, van Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad.

¹² Art. 6, premier alinéa, de la Décision n° 1313/2013/UE du Parlement européen et du Conseil.

Hiernaast bestaat er in sommige sectoren nog sectorspecifieke wetgeving, op basis waarvan reeds risicobeoordelingen moet worden uitgevoerd.¹³

Artikel 8

Het OCAD voert een dreigingsanalyse uit voor de (deel)sectoren vermeld in bijlage. Deze dreigingsanalyse vond zijn oorsprong in de KI-wet maar past in het kader van de alle risico's benadering uit de Richtlijn. In de KI-wet werd deze dreigingsanalyse pas aangevraagd na de identificatie van de kritieke infrastructuur. Dit werd in dit ontwerp vervroegd, zodat de sectorale overheden de informatie uit deze dreigingsanalyse mee kunnen opnemen in hun risicobeoordeling zoals bedoeld in artikel 7. De dreigingsanalyse zal daarna ook gedeeld worden met de kritieke entiteiten, zodat ook zij de relevante informatie hieruit kunnen opnemen in hun eigen risicobeoordeling.

Alle dreigingsanalyses zijn vier jaar geldig. Dit betekent dat analyses die voor de inwerkingtreding van deze wet uitgevoerd werden, en niet ouder zijn dan deze vier jaar, nog steeds geldig zijn in het kader van dit ontwerp, tot dat deze termijn van vier jaar afloopt.

Alle dreigingsanalyses moeten worden vernieuwd wanneer dat nodig is, hetgeen wordt beoordeeld in overeenstemming met het OCAD, bijvoorbeeld wanneer een nieuwe gebeurtenis de analyse wijzigt, hetzij met betrekking tot een nieuw type dreiging of met betrekking tot inlichtingen die de waarschijnlijkheid of de impact van een type dreiging wijzigen.

Paragraaf 2 omschrijft de dreigingsanalyse in de zin van Hoofdstuk 4 van dit ontwerp.

De aard van de analyse wordt gepreciseerd: het gaat om een strategische gemeenschappelijke evaluatie in de zin van artikel 8, eerste lid, 1°, van de wet van 10 juli 2006 betreffende de dreigingsanalyse, zij het met een verschil in de draagwijdte van de dreigingen waarmee rekening wordt gehouden. De dreigingsanalyse, die door artikel 3 van de wet van 10 juli 2006 betreffende de dreigingsanalyse momenteel beperkt is tot dreigingen die ontstaan uit terrorisme en extremisme, werd reeds in de KI-wet voor de bescherming van kritieke infrastructuren uitgebreid tot elk type van dreiging die onder de bevoegdheid van de ondersteunende diensten valt zoals bedoeld in het artikel 2, 2°, van de wet van 10 juli 2006 betreffende de analyse van de dreiging, wanneer die door het OCAD pertinent worden geacht ten aanzien van de sector of deelsector. Hier wordt niets aan gewijzigd. Dat is enerzijds gerechtvaardigd door het feit dat terrorisme en extremisme slechts een klein deel uitmaken van de alle risico's benadering van de Richtlijn en anderzijds door de aanzienlijke weerslag die de verstoring van de werking of van de vernietiging van een kritieke entiteiten in het land zou hebben.

sur la base desquelles des évaluations des risques doivent déjà être effectuées.¹³

Article 8

L'OCAM effectue une analyse des menaces pour les (sous-)secteurs énumérés en annexe. Cette analyse de la menace trouve son origine dans la loi IC, mais s'inscrit dans le cadre de l'approche tous risques de la Directive. Dans la loi IC, cette analyse de la menace n'était demandée qu'après l'identification des infrastructures critiques. Ce point a été avancé dans le présent projet afin que les autorités sectorielles puissent inclure les informations de cette analyse de la menace dans leur évaluation des risques visée à l'article 7. L'analyse de la menace sera ensuite également partagée avec les entités critiques afin qu'elles puissent elles aussi inclure les informations pertinentes dans leur propre évaluation des risques.

Toute analyse de la menace est valable quatre ans. Cela signifie que les analyses effectuées avant l'entrée en vigueur de cette loi, et ne datant pas de plus de quatre ans, restent valables en vertu de ce projet jusqu'à l'expiration de cette période de quatre ans.

Toutes les analyses de la menace doivent être renouvelées chaque fois que nécessaire, ce qui est évalué en accord avec l'OCAM, par exemple lorsqu'un nouvel événement modifie cette analyse, qu'il s'agisse soit d'un nouveau type de menace, soit de renseignements qui modifient la probabilité ou l'impact d'un type de menace.

Le paragraphe 2 définit l'analyse de la menace au sens du Chapitre 4 du présent projet.

La nature de l'analyse est précisée: il s'agit d'une évaluation stratégique commune au sens de l'article 8, alinéa 1^{er}, 1° de la loi du 10 juillet 2006 relative à l'analyse de la menace avec néanmoins une différence quant à l'étendue du champ des menaces prises en considération. L'analyse de la menace, qui est actuellement limitée aux menaces liées au terrorisme et à l'extrémisme par l'article 3 de la loi du 10 juillet 2006 relative à l'analyse de la menace, a déjà été étendue dans la loi IC pour la protection des infrastructures critiques à tout type de menace relevant de la compétence des services d'appui visés à l'article 2, 2°, de la loi du 10 juillet 2006 relative à l'analyse de la menace, lorsque l'OCAM le juge pertinent par rapport au secteur ou au sous-secteur. Rien de cela n'a été modifié. Ceci est justifié, d'une part, par le fait que le terrorisme et l'extrémisme ne constituent qu'une petite partie de l'approche tous risques de la Directive et, d'autre part, par l'impact important que l'interruption du fonctionnement ou la destruction d'une entité critique aurait dans le pays.

¹³ Verordening (EU) 2019/947 van het Europees Parlement en de Raad, Verordening (EU) 2017/1938 van het Europees Parlement en de Raad, Richtlijn 2012/18/EU van het Europees Parlement en de Raad, en Richtlijn 2007/60/EG van het Europees Parlement en de Raad.

¹³ Règlement (UE) 2019/947 du Parlement européen et du Conseil, Règlement (UE) 2017/1938 du Parlement européen et du Conseil, Directive 2012/18/UE du Parlement européen et du Conseil, et Directive 2007/60/CE du Parlement européen et du Conseil.

De analyse van de dreiging wordt hier gedefinieerd verwijzend naar de taken van de ondersteunende diensten bedoeld bij artikel 2, 2 van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

Het gaat om:

- a) de inlichtingen- en veiligheidsdiensten, zoals bedoeld in artikel 2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, hierna de "wet houdende regeling van de inlichtingen- en veiligheidsdienst" genoemd;
- b) de politiediensten zoals bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus;
- c) de federale overheidsdienst Financiën, in het bijzonder de Administratie der Douane en Accijnzen;
- d) de federale overheidsdienst Mobiliteit en Vervoer;
- e) de federale overheidsdienst Binnenlandse Zaken, in het bijzonder de Dienst Vreemdelingenzaken;
- f) de federale overheidsdienst Buitenlandse Zaken;
- g) de federale overheidsdienst Binnenlandse Zaken, in het bijzonder het Nationaal Crisiscentrum;
- h) de federale overheidsdienst Justitie, in het bijzonder het Directoraat-generaal Penitentiaire inrichtingen;
- i) de federale overheidsdienst Justitie, in het bijzonder de dienst Erediensten en Vrijzinnigheid van het Directoraat-generaal Wetgeving, Fundamentele rechten en Vrijheden;
- j) de federale overheidsdienst Financiën, in het bijzonder de algemene administratie van de Thesaurie.

Wat betreft de inlichtingen- en veiligheidsdiensten, preciseert artikel 7, 1°, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst dat "De Veiligheid van de Staat (...) als opdracht heeft: 1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk en economisch potentieel, zoals gedefinieerd door het Ministerieel Comité, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité, bedreigt of zou kunnen bedreigen;" en artikel 11, § 1, 1° en 2°, dat "De Algemene Dienst inlichting en veiligheid heeft als opdracht:

1° het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen, het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie en die opgenomen zijn in een op voorstel van de minister van Justitie en de minister van Landsverdediging door het ministerieel Comité voor Inlichting en Veiligheid goedgekeurde lijst, de vervulling van de opdrachten van de strijdkrachten, of de veiligheid van de Belgische onderdanen in het buitenland of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité, bedreigt of zou kunnen bedreigen, en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies te verlenen bij de omschrijving van haar buitenlands defensiebeleid;

L'analyse de la menace est définie en faisant référence aux tâches des services d'appui visés à l'article 2, 2, de la loi du 10 juillet 2006 relative à l'analyse de la menace.

Il s'agit :

- a) les services de renseignement et de sécurité tels que visés à l'article 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, ci-après dénommée la "loi organique des services de renseignement et de sécurité" ;
- b) les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ;
- c) le service public fédéral Finances, en particulier l'Administration des Douane et Accises ;
- d) le service public fédéral Mobilité et Transport ;
- e) le service public fédéral Intérieur, en particulier l'Office des Etrangers ;
- f) le service public fédéral Affaires étrangères ;
- g) le service public fédéral Intérieur, en particulier le Centre de Crise National ;
- h) le service public fédéral Justice, en particulier la direction générale Etablissements pénitentiaires ;
- i) le service public fédéral Justice, en particulier le Service des Cultes et de la Laïcité de la Direction générale, Législation, libertés et droits fondamentaux ;
- j) le service public fédéral Finances, en particulier l'administration générale de la Trésorerie.

En ce qui concerne les services de renseignement et de sécurité, l'article 7, 1°, de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité précise que "La Sûreté de l'Etat (...) a pour mission : 1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'Etat et les relations internationales, le potentiel scientifique ou économique défini par le Comité ministériel, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel ; et l'article 11, § 1er, 1° et 2°, que "Le Service général du renseignement et de la sécurité a pour mission :

1° de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer l'intégrité du territoire national, les plans de défense militaires, le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Comité ministériel du renseignement et de la sécurité, sur proposition du ministre de la Justice et du ministre de la Défense, l'accomplissement des missions des forces armées ou la sécurité des ressortissants belges à l'étranger ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Comité ministériel, et d'en informer sans délai les ministres compétents ainsi que de donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique extérieure de défense ;

2° het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert, de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten;"

De dreigingen die vallen onder de bevoegdheden van deze diensten zijn dus divers. Het vloeit overigens voort uit de opdrachten van de politiediensten, gedefinieerd door de artikelen 14 en 15 van de wet op het politieambt, om namelijk misdrijven te voorkomen, de daders ervan op te sporen of nog personen en goederen te beschermen, zijnde opdrachten die gelijk welk type van dreiging dekken. Er wordt dus tegemoetgekomen aan het doel van de Richtlijn om een "alle risico's omvattende aanpak" te beogen.

Alle relevante informatie waarover het NCCN en de sectorale overheden beschikken, wordt gedeeld met het OCAD. Gelet op het feit dat de dreigingsanalyse in dit ontwerp plaatsvindt voor de officiële aanduiding van kritieke entiteiten, is het mogelijk dat de sectorale overheid over sectorspecifieke informatie beschikt die relevant kan zijn voor de uitvoering van de dreigingsanalyse. Dergelijke relevante informatie kan onder meer de incidentenmeldingen door kritieke entiteiten inhouden.

Artikel 9

Artikel 9 bevat de omzetting van artikel 6 van de CER-Richtlijn, en omschrijft het identificatieproces voor kritieke entiteiten. Er werden enkele stappen aan dit proces toegevoegd teneinde beter overeen te stemmen met de huidige procedures in de KI-wet.

Paragraaf 1 houdt de chronologische volgorde van de identificatieprocedure in.

Teneinde de kritieke entiteiten te identificeren, overlegt de sectorale overheid vooraf met het NCCN. Zij zal tevens de vertegenwoordigers van de betrokken sector en de potentiële kritieke entiteiten kunnen raadplegen. Een dergelijke raadpleging zal immers toelaten aan de sectorale overheid om te beschikken over een duidelijke visie op de sector en de betrokken activiteiten en zal eveneens een betere uitvoering van deze wetgeving door de entiteit moeten toelaten, die in eerste instantie zal betrokken zijn in het proces. Deze raadpleging zorgt er ook voor dat de kritieke entiteiten op de hoogte zijn van de identificatieprocedure en het feit dat zij potentieel aangeduid kunnen worden als kritieke entiteit. De entiteit kan zich dan beter voorbereiden en kan ook reeds van start gaan met de identificatie van de kritieke infrastructuur waar zij als kritieke entiteit van afhankelijk zijn.

2° de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires et, dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le Ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés ;"

Les menaces qui relèvent des compétences de ces services sont donc variées. Il découle par ailleurs des articles 14 et 15 de la loi sur la fonction de police que la prévention des délits, la recherche des auteurs ou la protection des personnes et des biens sont des missions des services de police qui couvrent tout type de menace. L'objectif de la Directive qui consiste en une "approche tous risques" est dès lors atteint.

Toutes les informations pertinentes à la disposition du NCCN et des autorités sectorielles sont communiquées à l'OCAM. Étant donné que l'analyse de la menace dans ce projet a lieu avant la désignation officielle des entités critiques, il est possible que l'autorité sectorielle dispose d'informations spécifiques au secteur qui pourraient être utiles pour effectuer l'analyse de la menace. Ces informations pertinentes peuvent comprendre des rapports d'incidents émis par des entités critiques.

Article 9

L'article 9 contient la transposition de l'article 6 de la Directive CER et définit le processus d'identification des entités critiques. Quelques étapes ont été ajoutées à ce processus pour qu'il corresponde davantage aux procédures actuelles prévues par la loi IC.

Le paragraphe 1^{er} porte sur l'ordre chronologique de la procédure d'identification.

Afin d'identifier les entités critiques, l'autorité sectorielle consulte préalablement le NCCN. Elle pourra également consulter les représentants du secteur concerné et des potentielles entités critiques. Cette consultation permettra en effet à l'autorité sectorielle de disposer d'une vision claire du secteur et des activités concernées, et devrait également améliorer la mise en œuvre de cette législation par l'entité qui sera impliquée en premier lieu dans le processus. Grâce à cette consultation, les entités critiques seront en outre au courant de la procédure d'identification et du fait qu'elles peuvent potentiellement être désignées comme entité critique. L'entité pourra ainsi mieux se préparer et entamer d'ores et déjà l'identification des infrastructures critiques dont elle dépend en tant qu'entité critique.

Eveneens zal de sectorale overheid de gefedereerde entiteiten kunnen raadplegen, indien de potentiële kritieke infrastructuur onder hun bevoegdheden vallen. Het standpunt van de Raad van State in zijn advies van 9 december 2010¹⁴ over de wet van 1 juli 2011 met betrekking tot de beveiliging en bescherming van kritieke infrastructuur, was dat aangezien de gefedereerde entiteiten bevoegdheden bezitten op het gebied van de betrokken sectoren uit die wet, bij uitvoering ervan een weerslag van sommige van de maatregelen voelbaar kan zijn in het beheer van de infrastructuur die tot de bevoegdheid van de gefedereerde entiteiten horen. Er werd aldus aanvaard dat zij wel betrokken kunnen worden in het proces, doch de autonomie van de federale overheid gerespecteerd wordt, aangezien een consultatie vrijwillig is en de aanneming van maatregelen door de federale overheid niet kan verhinderen.

Dit ontwerp behelst de verschillende aspecten van weerbaarheid van kritieke entiteiten waarbij de bescherming en beveiliging ervan één van de elementen is die al degelijk werden uitgewerkt in de KI-wet. Wat in het verleden werd opgebouwd blijft aldus behouden en wordt geïntegreerd, samen met het verhogen van de weerbaarheid ten aanzien van alle risico's die gevat worden in de CER-Richtlijn waarvan deze CER-wet de omzetting is.

Deze identificatieprocedure gebeurt met toepassing van de hierna gedefinieerde criteria.

In de tweede paragraaf wordt beschreven hoe de identificatie verloopt van de kritieke infrastructuur onder het beheer van de potentiële kritieke entiteiten. Het is de verantwoordelijkheid van de potentiële kritieke entiteit, die op grond van paragraaf 1 op de hoogte is van de lopende identificatieprocedure, om een lijst op te stellen van kritieke infrastructuren waarvan haar essentiële dienstverlening afhankelijk is.

De potentiële kritieke entiteit maakt de gemotiveerde lijst van kritieke infrastructuur binnen haar entiteit binnen zes maanden na de kennisgeving uit paragraaf 1 over aan de sectorale overheid. De sectorale overheid kan aan de potentiële kritieke entiteit bijsturingen opleggen in de voorgestelde lijst van kritieke infrastructuur, rekening houdend met de criteria die zij gebruikt tijdens de identificatieprocedure op grond van paragraaf 1, alsook met de coherentie in haar sector of deelsector voor wat betreft de identificatie van kritieke infrastructuur. De bevoegde sectorale overheid kan verduidelijking en toelichting vragen aan de potentiële kritieke entiteit en kan desgevallend voorgestelde kritieke infrastructuur weigeren dan wel andere infrastructuur binnen de kritieke entiteit aanduiden, mits opgave van redenen.

De kritieke entiteit is verantwoordelijk voor het actualiseren van deze lijst, en moet binnen een periode van 30 dagen na een wijziging van de lijst de bevoegde sectorale overheid op de hoogte stellen van deze wijzigingen. Dergelijke wijziging kan onder meer een adreswijziging, een toevoeging en een schrapping van een kritieke infrastructuur inhouden. De sectorale

L'autorité sectorielle pourra aussi consulter les entités fédérées, si les infrastructures critiques potentielles relèvent de leurs compétences. Dans son avis du 9 décembre 2010¹⁴ concernant la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, le point de vue du Conseil d'Etat était le suivant: dans la mesure où les entités fédérées disposent de compétences dans le domaine des secteurs concernés par cette loi, certaines mesures peuvent, au moment de leur mise en œuvre, avoir des répercussions sur la gestion de l'infrastructure qui relève de la compétence des entités fédérées. Il a dès lors été admis qu'elles peuvent être associées au processus, mais doivent respecter l'autonomie des autorités fédérales étant donné qu'une consultation est volontaire et ne peut empêcher la prise de mesures par les autorités fédérales.

Ce projet englobe les différents aspects de la résilience entière des entités critiques, leur protection et leur sécurité étant l'un des éléments déjà bien développés dans la loi IC. Ce qui a été construit dans le passé est ainsi préservé et intégré, tout en augmentant la résilience à tous les risques contenus dans la Directive CER, dont cette loi CER est la transposition.

Cette procédure d'identification s'effectue par l'application des critères définis ci-après.

Le deuxième paragraphe décrit la façon dont se déroule l'identification des infrastructures critiques gérées par les entités critiques potentielles. Il appartient à l'entité critique potentielle qui, conformément au paragraphe 1^{er}, est au courant de la procédure d'identification en cours, d'établir la liste des infrastructures critiques dont ses services essentiels dépendent.

L'entité critique potentielle transmet la liste motivée des infrastructures critiques de son entité à l'autorité sectorielle dans les six mois suivant la notification visée au paragraphe 1^{er}. L'autorité sectorielle peut imposer à l'entité critique potentielle des ajustements à la liste d'infrastructures critiques proposée, en tenant compte des critères qu'elle utilise durant la procédure d'identification en vertu du paragraphe 1^{er}, ainsi que de la cohérence dans son secteur ou sous-secteur en termes d'identification des infrastructures critiques. L'autorité sectorielle compétente peut demander des éclaircissements et des explications à l'entité critique potentielle et, le cas échéant, rejeter les infrastructures critiques proposées ou désigner d'autres infrastructures au sein de l'entité critique, en motivant sa décision.

L'entité critique est responsable de l'actualisation de cette liste et doit informer, dans une période de 30 jours après la modification de cette liste, l'autorité sectorielle compétente de cette modification. Une telle modification peut notamment concerner un changement d'adresse, un ajout et une suppression d'une infrastructure critique. L'autorité sectorielle transmet ces informations au NCCN dans les plus brefs délais.

¹⁴ RvS 9 décembre 2010, nr. 48.989/VR.

¹⁵ C.E., 9 décembre 2010, n° 48.989/VR.

overheid stuurt deze informatie onverwijld door naar het NCCN.

Een goede informatie-uitwisseling tussen de sectorale overheden en potentiële kritieke entiteiten is noodzakelijk om dit proces vlot en kwaliteitsvol te laten verlopen. Om deze informatiestroom te faciliteren, werd in het huidige ontwerp een delegatie aan de Koning voorzien voor het opstellen van modaliteiten betreffende de informatie-uitwisseling.

Het CCB wordt tijdens het hele identificatieproces, bij het door de sectorale overheden en het NCCN gevoerde overleg, betrokken, binnen de grenzen van hun respectievelijke bevoegdheden, voor wat betreft de kritieke entiteiten die betrekking hebben op de beveiliging van netwerk- en informatiesystemen, dit omdat, behoudens tegenbewijs, de kritieke entiteiten geacht worden afhankelijk te zijn van netwerk- en informatiesystemen, en een goede informatie-uitwisseling hieromtrent tussen de bevoegde autoriteiten noodzakelijk is.

Gelet op het feit dat kritieke entiteiten op grond van de NIS 2 richtlijn automatisch essentiële entiteiten zijn, wordt ook de nationale cyberbeveiligingsautoriteit bedoeld in artikel 16 van de wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, geïnformeerd van de aanduidingen van kritieke entiteiten.

Artikel 10

Artikel 10 houdt de omzetting in van artikel 6 van de CER-Richtlijn, waarin de drie basiscriteria vastgelegd worden waaraan een entiteit moet voldoen alvorens deze kan geïdentificeerd worden als kritieke entiteit.

Tijdens de identificatieprocedure moeten de sectorale overheden ten minste rekening houden met deze criteria aan de hand waarvan kan worden bepaald hoe ernstig het verstorend effect van een incident is of kan zijn, welke één van de drie basiscriteria is. Deze criteria worden omschreven in artikel 7, eerste lid van de CER-Richtlijn. Het komt aan de sectorale overheid toe om, in het kader van de identificatie van de kritieke entiteiten de niveaus van weerslag of de drempelwaarden van deze criteria te definiëren.

Deze criteria worden zo veel als mogelijk op kwantitatieve en (deel-)sectorspecifieke wijze bepaald en gemotiveerd. Een duidelijke en kwaliteitsvolle redenering is van essentieel belang voor het verdere verloop van het identificatieproces. Het NCCN kan, aan de hand van een gemotiveerd verzoek, alle relevante informatie hierover opvragen zodat onder meer het advies uit artikel 12 van dit ontwerp correct onderbouwd kan worden.

De sectorale overheid bepaalt de niveaus van weerslag of de drempelwaarden van deze criteria, in overleg met het NCCN, en in voorkomend geval, na raadpleging van de gefedereerde entiteiten voor zover het gaat om hun bevoegdheden. In dit verband wordt verwezen naar het commentaar betreffende artikel 9, §1.

Un échange efficace d'informations entre les autorités sectorielles et les entités critiques potentielles est nécessaire afin d'assurer un déroulement correct et qualitatif du processus. Pour faciliter ce flux d'informations, le présent projet prévoit une délégation au Roi afin d'établir les modalités de l'échange d'informations.

Tout au long du processus d'identification, le CCB est impliqué dans la concertation menée par les autorités sectorielles et le NCCN, dans les limites de leurs compétences respectives, pour ce qui concerne les entités critiques qui portent sur la sécurité des systèmes de réseau et d'information. La raison en est que, sauf preuve du contraire, les entités critiques sont supposées dépendre des systèmes de réseau et d'information, et qu'un bon échange d'informations à ce sujet est nécessaire entre les autorités compétentes.

Étant donné que les entités critiques sont automatiquement des entités essentielles en vertu de la directive NIS 2, l'autorité nationale de cybersécurité visée à l'article 16 de la loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique est également informée des désignations d'entités critiques.

Article 10

L'article 10 est une transposition de l'article 6 de la Directive CER, qui définit les trois critères de base qu'une entité doit satisfaire avant de pouvoir être identifiée comme entité critique.

Durant le processus d'identification, l'autorité sectorielle doit au moins tenir compte de ces critères qui permettent de déterminer le degré de gravité de l'impact perturbateur qu'a ou peut avoir un incident, ce qui constitue l'un des trois critères de base. Ces critères sont définis à l'article 7, premier alinéa, de la Directive CER. Il appartient à l'autorité sectorielle de définir, dans le cadre de l'identification des entités critiques, les niveaux d'impact ou les valeurs seuils de ces critères.

Dans la mesure du possible, ces critères sont déterminés et justifiés d'une manière quantitative et (sous-)sectorielle. Un raisonnement suffisamment clair et de qualité est essentiel pour la suite du processus d'identification. A tout moment, le NCCN peut, sur requête motivée, demander toutes les informations pertinentes à ce sujet afin de pouvoir correctement étayer, entre autres, l'avis prévu à l'article 12 du présent projet.

L'autorité sectorielle détermine les niveaux d'impact ou les valeurs seuils de ces critères en concertation avec le NCCN et, le cas échéant, après consultation des entités fédérées pour autant qu'il s'agisse de leurs compétences. Il est fait référence à cet égard au commentaire relatif à l'article 9, § 1^{er}.

Het overleg met het NCCN, wat betreft de criteria uit artikel 10 en 11 van dit ontwerp, is gerechtvaardigd door haar coördinerende rol op het vlak van de weerbaarheid van de kritieke entiteiten. Dat overleg moet een harmonisering van de benaderingswijze binnen de verschillende sectoren mogelijk maken.

Artikel 11

Artikel 11 regelt de bepaling van sectorale criteria, welke zijn oorsprong vindt in de KI-wet. Deze sectorale criteria kunnen bijkomend aan de criteria uit artikel 10 van dit ontwerp gebruikt worden, indien nodig. Er bestaat geen verplichting om bijkomende sectorale criteria op te stellen, doch wordt het gebruik ervan ten zeerste aangemoedigd, aangezien het op deze manier mogelijk is om met meer sectorspecifieke eigenschappen rekening te houden tijdens het identificatieproces.

Ze zullen in ieder geval vastgelegd en gedocumenteerd moeten worden in overleg met het NCCN, alsook, indien van toepassing, na raadpleging van de gefedereerde entiteiten voor de potentiële kritieke entiteiten die onder hun bevoegdheden vallen.

Artikel 12

Na de kritieke entiteiten te hebben geïdentificeerd, moet de sectorale overheid overgaan tot hun aanduiding.

Paragraaf 1 omschrijft het mechanisme voor de aanduiding van de kritieke entiteiten, namelijk de aanduiding na het advies van het NCCN. Het advies wordt gegeven nadat een gecoördineerd dossier werd bezorgd aan het NCCN, waarin alle nodige informatie staat dat nodig kan zijn om een grondig gemotiveerd advies te kunnen geven. Dat advies is gerechtvaardigd door de coördinerende rol van het NCCN, beschreven in het commentaar bij artikel 10. Dit advies is niet bindend voor de sectorale overheid, maar heeft wel een belangrijke adviserende waarde.

De gefedereerde entiteiten zullen eveneens kunnen worden geraadpleegd door de sectorale overheden vóór de aanduiding voor wat de kritieke entiteiten betreft van sectoren die onder hun bevoegdheden vallen.

Het NCCN zal voor elke substantiële wijziging in het geconsolideerde dossier opnieuw advies moeten geven over die wijziging. Met een substantiële wijziging wordt bedoeld een toevoeging of schrapping van kritieke infrastructuur, en niet de louter adreswijziging van bestaande kritieke infrastructuur. Dit advies heeft als doel de harmonisatie tussen de sectoren te waarborgen en verklaart tevens waarom de sectorale overheden tijdens de identificatieprocedure het NCCN moeten informeren.

Bij afwezigheid van aanduiding van een kritieke entiteit in haar welbepaalde (deel)sector, zet de bevoegde sectorale overheid hiervoor de redenen uiteen die geleid hebben tot deze afwezigheid. Deze motivatie kan bestaan uit de toetsing van de criteria uit artikel 10, §1 en §2.

La concertation avec le NCCN, en ce qui concerne les critères des articles 10 et 11 du présent projet, est justifiée par le rôle de coordination du NCCN en matière de résilience des entités critiques. Cette concertation doit permettre une harmonisation de l'approche au sein des différents secteurs.

Article 11

L'article 11 porte sur la définition des critères sectoriels, laquelle trouve son origine dans la loi IC. Ces critères sectoriels peuvent être utilisés en plus des critères prévus à l'article 10 du présent projet, si nécessaire. Il n'y a pas d'obligation d'établir des critères sectoriels supplémentaires, mais leur utilisation est fortement encouragée car elle permet de prendre en compte davantage de caractéristiques sectorielles spécifiques au cours du processus d'identification.

En tout état de cause, elles devront être enregistrées et documentées en consultation avec le NCCN, ainsi que, le cas échéant, après consultation des entités fédérées pour les entités critiques potentielles relevant de leur compétence.

Article 12

Après avoir identifié les entités critiques, l'autorité sectorielle doit procéder à leur désignation.

Le paragraphe 1^{er} définit le mécanisme de désignation des entités critiques, à savoir la désignation après l'avis du NCCN. L'avis est rendu après transmission d'un dossier coordonné au NCCN qui contient toutes les informations pouvant être nécessaires pour rendre un avis dûment motivé. Cet avis est justifié par le rôle de coordination du NCCN, tel que décrit au commentaire de l'article 10. Il n'est pas contraignant pour l'autorité sectorielle, mais il a une importante valeur consultative.

Les entités fédérées pourront également être consultées par les autorités sectorielles avant la désignation pour ce qui concerne les entités critiques de secteurs qui relèvent de leurs compétences.

Le NCCN devra rendre un nouvel avis pour chaque modification substantielle apportée au dossier consolidé au sujet de cette modification. Par modification substantielle, on entend un ajout ou une suppression de l'infrastructure critique et non pas un simple changement d'adresse. Cet avis vise à garantir l'harmonisation entre les secteurs et précise également pourquoi les autorités sectorielles doivent informer le NCCN au cours du processus d'identification.

En l'absence de désignation d'une entité critique dans son (sous-)secteur déterminé, l'autorité sectorielle compétente expose les motifs qui ont conduit à cette absence. Cette motivation peut consister en l'examen des critères repris à l'article 10, § 1^{er} et § 2.

Artikel 6.5. van de Richtlijn bepaalt dat het identificatie- en aanduiding proces ten minste elke vier jaar, en telkens wanneer nodig, hernieuwd wordt.

Artikel 13

Artikel 13 bepaalt de vormvoorschriften voor de aanduiding van de kritieke entiteit, namelijk de betekening van de gemotiveerde beslissing aan de kritieke entiteit met ontvangstbewijs.

Het is belangrijk dat men precies kan bepalen op welke datum de betekening van de aanduiding is gebeurd, omdat dat het startpunt is voor de termijn voor de verplichtingen van de kritieke entiteit, die zijn beschreven in het commentaar van de artikelen 16 t.e.m. 20 van deze wet.

In de KI-wet werd enkel de burgemeester van de gemeente op het grondgebied waarvan de kritieke entiteit zich bevindt, op de hoogte gebracht van deze aanduiding, in het kader van de externe bescherming. Op grond van de CER-Richtlijn moeten de weerbaarheidsplannen nu ook verplicht interne noodplannen bevatten, waardoor logischerwijze de gouverneurs mee in kennis gesteld moeten worden, zodat zij hun externe noodplannen hierop kunnen afstemmen.

Wanneer de aanduiding van een kritieke entiteit meerdere sectoren of deelsectoren aanbelangt, brengt het NCCN de bevoegde sectorale overheden samen voor overleg tussen de sectorale overheden zodat er voor de kritieke entiteiten geen dubbele verplichtingen bestaan. Tijdens het overleg kunnen bijvoorbeeld afspraken gemaakt worden met betrekking tot de inspecties en audits. Aangezien in verschillende sectoren de Minister aangeduid wordt als sectorale overheid, zal deze ook op de hoogte gesteld kunnen worden van de aanduidingen door de administraties die onder zijn of haar bevoegdheden vallen. De voorzitter van de NAMB wordt tevens ingelicht van aanduidingen in het Belgisch gedeelte van de Noordzee.

Afdeling 2

Kritieke entiteiten van Europees belang

Artikel 14

Dit artikel beschrijft de identificatieprocedure van kritieke entiteiten van bijzonder Europees belang, en zet Hoofdstuk IV van de CER-Richtlijn om. Ofschoon kritieke entiteiten over het algemeen binnen een steeds hechter dienstverlenings- en infrastructureel netwerk opereren en dikwijls in meer dan één lidstaat essentiële diensten verlenen, zijn een aantal van die kritieke entiteiten van bijzonder belang voor de Unie omdat zij essentiële diensten verlenen aan of in zes of meer lidstaten, en kunnen zij daarom specifieke ondersteuning op Unieniveau krijgen.

L'article 6.5. de la Directive stipule que le processus d'identification et de désignation est renouvelé au moins tous les quatre ans, et chaque fois que cela s'avère nécessaire.

Article 13

L'article 13 détermine les prescriptions de forme pour la désignation de l'entité critique, à savoir la notification de la décision motivée à l'entité critique avec accusé de réception.

Il est important de pouvoir déterminer avec précision la date de la notification de la désignation, car il s'agit du point de départ du délai pour les obligations de l'entité critique, qui sont décrites dans le commentaire des articles 16 à 20 de la présente loi.

En vertu de la loi IC, seul le bourgmestre de la commune sur le territoire de laquelle se trouve l'entité critique était notifié de cette désignation, dans le cadre de la protection externe. En vertu de la Directive CER, les plans de résilience doivent désormais également inclure des plans d'urgence internes, ce qui nécessite logiquement que les gouverneurs soient co-notifiés afin qu'ils puissent aligner leurs plans d'urgence externes en conséquence.

Lorsque la désignation d'une entité critique concerne plusieurs secteurs ou sous-secteurs, le NCCN réunit les autorités sectorielles compétentes pour une consultation entre les autorités sectorielles afin d'éviter la duplication des obligations des entités critiques. Au cours de cette concertation, des accords peuvent être conclus sur les inspections et les audits, par exemple. Etant donné que, dans plusieurs secteurs, le ministre est désigné comme autorité sectorielle, il pourra également être informé des désignations effectuées par les administrations relevant de sa compétence. Le président de la ANSM est également informé des désignations dans la partie belge de la mer du Nord

Section 2

Entités critiques revêtant une importante européenne particulière

Article 14

Cet article décrit la procédure d'identification des entités critiques revêtant une importance européenne particulière et transpose le Chapitre IV de la Directive CER. Bien que les entités critiques opèrent en général au sein d'un réseau toujours plus dense de services et d'infrastructures et fournissent souvent des services essentiels dans plus d'un Etat membre, un certain nombre d'entre elles revêtent une importance particulière pour l'Union parce qu'elles fournissent des services essentiels à ou dans six Etats membres ou plus, et peuvent par conséquent recevoir un soutien spécifique au niveau de l'Union.

De entiteit die werd aangeduid als kritieke entiteit op grond van artikel 12 van deze wet, is verantwoordelijk om de bevoegde sectorale overheid te informeren in het geval zij essentiële diensten verleent aan of in meer dan zes lidstaten. De kritieke entiteit vermeldt hierbij over welke essentiële diensten het gaat en in welke lidstaten deze worden verleend. Het NCCN stelt, in haar functie als Nationaal Centraal Contactpunt, in overleg met de bevoegde sectorale overheden, zonder onnodige vertraging de Europese Commissie in kennis van de identiteit van dergelijke kritieke entiteiten en van de informatie die zij verstrekken op basis van dit artikel.

De Commissie raadpleegt via het Nationaal Centraal Contactpunt de bevoegde sectorale overheid, die de kritieke entiteit als zodanig heeft aangeduid, de bevoegde autoriteit van andere betrokken lidstaten en de betrokken kritieke entiteit zelf. Deze raadpleging heeft als doel te onderzoeken of de geleverde diensten wel degelijk als essentiële diensten zijn aangeduid in de betrokken lidstaten. In het geval dat de Commissie oordeelt dat de betrokken kritieke entiteit essentiële diensten verleent aan of in meer dan zes lidstaten, stelt zij het NCCN ervan in kennis dat de entiteit als een kritieke entiteit van bijzonder Europees belang wordt beschouwd. Het NCCN stelt onverwijld de bevoegde sectorale overheid hiervan in kennis, dewelke op haar beurt de kritieke entiteit zonder onnodige vertraging de kennisgeving toezendt.

De bepalingen onder Hoofdstuk 5 van dit ontwerp zijn van toepassing vanaf de datum van ontvangst door de kritieke entiteit van de kennisgeving door de sectorale overheid dat zij als kritieke entiteit van Bijzonder Europees Belang beschouwd wordt.

In overleg met de lidstaat die de kritieke entiteit van bijzonder Europees belang heeft geïdentificeerd als een kritieke entiteit, moet de Commissie een adviesmissie kunnen organiseren om de door die entiteit genomen maatregelen te beoordelen.

Artikel 15

Het NCCN, in haar functie van Nationaal Centraal Contactpunt, vervult een verbindingfunctie met het oog op grensoverschrijdende samenwerking met de centrale contactpunten van de andere lidstaten. Artikel 15 beschrijft de mogelijkheid om bilaterale of multilaterale besprekingen te voeren met betrokken lidstaten van de Europese Unie in het geval dat een kritieke entiteit op Belgisch grondgebied banden heeft met die lidstaten, doordat er gebruik gemaakt wordt van kritieke infrastructuur die verbonden is tussen twee of meer lidstaten, doordat zij deel uitmaken van bedrijfsstructuren die verbonden zijn aan kritieke entiteiten in andere lidstaten of wanneer zij essentiële diensten verlenen aan of in andere lidstaten. Met name worden hier de kritieke entiteiten bedoeld die niet voldoen aan de voorwaarden om als kritieke entiteiten van Bijzonder Europees Belang aangeduid te worden, en dus geen essentiële diensten verlenen aan of in meer dan zes lidstaten.

Dit artikel komt tegemoet aan het wegvallen van de categorie 'Europese Kritieke Infrastructuur' uit de ECI-Richtlijn. De entiteiten die voorheen als zodanig werden geïdentificeerd, maar onder dit ontwerp niet voldoen aan

L'entité qui a été désignée comme entité critique en vertu de l'article 12 de la présente loi est chargée d'informer l'autorité sectorielle compétente dans le cas où elle fournit des services essentiels à ou dans six Etats membres ou plus. L'entité critique mentionne de quels services essentiels il s'agit et dans quels Etats membres ceux-ci sont fournis. Le NCCN, en sa qualité de Point de Contact Central National, en consultation avec les autorités sectorielles compétentes, notifie sans délai la Commission européenne de l'identité de ces entités critiques et des informations qu'elles fournissent sur la base du présent article.

La Commission consulte via le Point de Contact Central National l'autorité sectorielle compétente, qui a désigné l'entité critique comme telle, l'autorité compétente d'autres Etats membres concernés ainsi que l'entité critique concernée. Cette consultation vise à examiner si les services fournis ont bel et bien été désignés comme services essentiels dans les Etats membres concernés. Dans le cas où la Commission estime que l'entité critique concernée fournit des services essentiels à six Etats membres ou plus, elle communique au NCCN que l'entité est considérée comme une entité critique revêtant une importance européenne particulière. Le NCCN informe sans délai l'autorité sectorielle compétente qui envoie à son tour, sans délai, la notification à l'entité critique.

Les dispositions du Chapitre 5 du présent projet s'appliquent à partir de la date de réception, par l'entité critique, de la notification par l'autorité sectorielle selon laquelle elle est considérée comme une entité critique revêtant une importance européenne particulière.

En concertation avec l'Etat membre qui a identifié l'entité critique revêtant une importance européenne particulière comme entité critique, la Commission doit pouvoir organiser une mission consultative afin d'évaluer les mesures prises par cette entité.

Article 15

En sa qualité de Point de Contact Central National, le NCCN remplit une fonction de liaison en vue de la collaboration transfrontalière avec les points de contact centraux des autres Etats membres. L'article 15 décrit la possibilité de mener des discussions bilatérales ou multilatérales avec les Etats membres concernés de l'Union européenne au cas où une entité critique a, sur le territoire belge, des liens avec ces Etats membres parce qu'elle utilise des infrastructures critiques physiquement connectées entre deux Etats membres ou plus, qu'elles font partie de structures d'entreprise liées à des entités critiques dans d'autres Etats membres ou quand elles fournissent des services essentiels à ou dans d'autres Etats membres. Sont ici visées les entités critiques qui ne répondent pas aux conditions pour être désignées comme entités critiques revêtant une importance européenne particulière et qui ne fournissent donc pas de services essentiels à ou dans six Etats membres ou plus.

Cet article tient compte de la suppression de la catégorie des « Infrastructures Critiques Européennes » de la Directive ICE. Les entités précédemment identifiées comme telles, mais qui, selon ce projet, n'atteignent pas

de drempel van zes lidstaten, zullen voortaan geen bijzonder statuut meer bezitten. Dit artikel benadrukt voor deze gevallen de mogelijkheid tot bilaterale of multilaterale samenwerking.

HOOFDSTUK 5

Interne weerbaarheidsmaatregelen van kritieke entiteiten

Artikel 16

In dit Hoofdstuk worden de weerbaarheidsmaatregelen georganiseerd die de kritieke entiteit moet nemen, in functie van de risico's waaraan zij wordt blootgesteld.

Artikel 13.3 van de CER-Richtlijn legt de verplichting op aan de kritieke entiteit om een 'Contactpunt kritieke entiteit' aan te duiden, die een rol van contactpunt vervult met de bevoegde overheden. Dergelijke verplichting stond ook in de KI-wet, en houdt dus een verderzetting in van het beleid hieromtrent.

Omdat het doel hiervan het verzekeren van een permanent contactpunt is tussen de kritieke entiteit en de autoriteiten, werd gekozen voor een contactpunt dat 24u/24bereikbaar is voor de bevoegde autoriteiten, het NCCN, de burgemeester en de gouverneur. Het is aan de entiteit om toe te zien dat er permanentie verzekerd wordt door één of verschillende personen bevoegd om de veiligheidsvragen met betrekking tot de kritieke entiteiten te behandelen.

De kritieke entiteit dient dit contactpunt aan te duiden en de contactgegevens te communiceren binnen de zes maanden van zijn aanduiding als kritieke entiteit.

De tweede paragraaf beoogt de hypothese waarin een contactpunt van hetzelfde type reeds opgelegd zou zijn aan de kritieke entiteit krachtens andere nationale of internationale reglementeringen.

Dit is momenteel het geval voor wat betreft de havens, die op grond van de wet van 8 mei 2019 tot invoering van het Belgisch Scheepvaartswetboek, een maritieme beveiligingsfunctionaris moeten aanduiden, dewelke fungeert als lokaal contactpersoon voor alle aangelegenheden die verband houden met de maritieme beveiliging van de betrokken haven.

De derde paragraaf van dit artikel legt een beschikbaarheid op aan het contactpunt van 24u/24, aangezien een incident zich op elk ogenblik kan voordoen.

Artikel 17

Artikel 12.1 van de Richtlijn legt op dat de kritieke entiteiten alle relevante risico's beoordelen die de verlening van hun essentiële diensten kunnen verstoren. Kritieke entiteiten moeten een breed inzicht hebben in de risico's waaraan zij blootgesteld kunnen worden en zij moeten deze risico's afdoende analyseren. Daartoe moeten zij, telkens wanneer hun specifieke omstandigheden en de evolutie van die risico's daartoe

le seuil de six Etats membres, ne bénéficieront désormais plus d'un statut spécial. Dans de tels cas, cet article souligne la possibilité d'une coopération bilatérale ou multilatérale.

CHAPITRE 5

Mesures internes de la résilience des entités critiques

Article 16

Ce Chapitre régit les mesures de résilience que l'entité critique doit prendre, en fonction des risques auxquels elle est exposée.

L'article 13, point 3, de la Directive CER impose à l'entité critique l'obligation de désigner un « Point de Contact entité critique », qui joue le rôle de point de contact avec les autorités compétentes. Cette obligation figurait également dans la loi IC et représente donc une continuation de la politique en la matière.

Dans la mesure où l'objectif est d'assurer un point de contact permanent entre l'entité critique et les autorités, il a été décidé d'opter pour un point de contact disponible 24h/24 pour les autorités compétentes, le NCCN, le bourgmestre et le gouverneur. Il appartient à l'entité de veiller à ce qu'une permanence soit assurée par une ou plusieurs personnes compétentes pour traiter les questions de sécurité relatives aux entités critiques.

L'entité critique est tenue de désigner ce point de contact et de communiquer les coordonnées de contact endéans les six mois de sa désignation comme entité critique.

Le deuxième paragraphe vise l'hypothèse dans laquelle un point de contact du même type aurait déjà été imposé à l'entité critique en vertu d'autres réglementations nationales ou internationales.

Ceci est actuellement le cas en ce qui concerne les ports qui, conformément à la loi du 8 mai 2019 introduisant le Code belge de la Navigation, sont tenus de désigner un agent de sûreté maritime qui agit en tant que personne de contact locale pour toutes les questions liées à la sécurité maritime du port concerné.

Le troisième paragraphe de cet article impose au point de contact une disponibilité 24h/24 étant donné qu'un incident peut survenir à tout instant.

Article 17

L'article 12.1 de la Directive impose aux entités critiques d'évaluer tous les risques pertinents susceptibles de perturber la fourniture de leurs services essentiels. Les entités critiques doivent avoir une connaissance approfondie des risques auxquels elles peuvent être exposées et elles doivent les analyser de façon adéquate. A cette fin, elles doivent procéder à des évaluations des risques chaque fois que leurs circonstances particulières

nopen, en in ieder geval om de vier jaar, risicobeoordelingen uitvoeren. Hierbij moet tevens rekening gehouden worden met afhankelijkheden binnen en van andere in deze wet genoemde sectoren, en in voorkomend geval ook in naburige lidstaten en derde landen.

De sectorale overheid dient zijn sectorale risicobeoordeling, uitgevoerd op basis van artikel 7 van dit ontwerp, mee te delen aan de kritieke entiteit zodat deze de relevante informatie hieruit kan opnemen in zijn eigen risicobeoordeling. Hiernaast houdt de kritieke entiteit ook rekening met de dreigingsanalyse uitgevoerd op basis van artikel 8, en alle andere relevante informatie waarover zij beschikt.

Indien kritieke entiteiten risicobeoordelingen hebben uitgevoerd of documenten hebben opgesteld op grond van verplichtingen opgenomen in andere rechtshandelingen, die relevant zijn voor hun risicobeoordeling, kunnen zij die beoordelingen en documenten gebruiken om aan de voorschriften voor hun risicobeoordeling die zijn vastgesteld in deze wet, te voldoen.

Artikel 18

Dit artikel legt aan de kritieke entiteit de verplichting op om een weerbaarheidsplan van de kritieke entiteit (hieronder "W.P.E.") uit te werken die de technische, beveiligings- en organisatorische weerbaarheidsmaatregelen bevat, om incidenten te voorkomen, te beperken of te beheersen, en om bescherming te bieden of bestand te zijn tegen, te reageren op of zich aan te passen aan een incident of daarvan te herstellen. Deze weerbaarheidsmaatregelen moeten in verhouding en evenredig zijn met de verschillende risico's die elke kritieke entiteit bij haar risicobeoordeling heeft vastgesteld en de specifieke kenmerken van de betrokken entiteit.

Het W.P.E. moet weerbaarheidsmaatregelen bevatten die toegepast worden in functie van de risico's waaraan de entiteit kan worden blootgesteld, rekening houdend met de mogelijkheid tot wijzigende omstandigheden. Dit wil zeggen dat er naast de standaard maatregelen ook de mogelijkheid moet zijn om de maatregelen op te schalen wanneer de omstandigheden hiertoe noodzakelijk zijn. Een opschaling van maatregelen kan bijvoorbeeld nodig zijn in het geval van een concrete dreiging, noodweer of een gezondheids crisis. De kritieke entiteit is verantwoordelijk voor het bepalen welke maatregelen adequaat en noodzakelijk worden geacht om tegemoet te komen aan veranderende omstandigheden.

Voor het overige is de mogelijkheid gelaten aan de Koning om eventuele aanvullende informatie of maatregelen die het W.P.E. moet bevatten voor een bepaalde sector, of voor een deelsector, vast te leggen. De specificiteit van de ene of de andere sector kan immers verantwoorden dat de sectorale overheid gemeenschappelijke richtlijnen op het vlak van weerbaarheidsmaatregelen vastlegt. De wet bepaalt aldus de algemene verplichtingen waaraan bijzondere verplichtingen die eigen zijn aan elke sector kunnen worden toegevoegd.

et l'évolution de ces risques l'exigent et, en tout cas, tous les quatre ans. Il faut également tenir compte à cet égard des dépendances au sein de et émanant d'autres secteurs cités dans la présente loi et, le cas échéant, dans les Etats membres voisins et les pays tiers.

L'autorité sectorielle est tenue de communiquer à l'entité critique son évaluation sectorielle des risques, menée sur la base de l'article 7 du présent projet, afin de lui permettre d'intégrer les informations pertinentes dans sa propre évaluation des risques. En outre, l'entité critique tient également compte de l'analyse de la menace effectuée en vertu de l'article 8, et de toutes les autres informations pertinentes dont elle dispose.

Si les entités critiques ont effectué des évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour leurs évaluations des risques, elles peuvent utiliser ces évaluations et documents pour répondre aux prescriptions concernant leurs évaluations des risques contenues dans la présente loi.

Article 18

Cet article impose à l'entité critique l'obligation d'élaborer un plan de résilience de l'entité critique (ci-après dénommé "P.R.E.") qui contient les mesures techniques, sécuritaires et organisationnelles de résilience en vue de prévenir tout incident, de le limiter ou de le maîtriser, et de s'en protéger ou d'y résister, d'y réagir, de s'y adapter ou de s'en rétablir. Ces mesures de résilience doivent être appropriées et proportionnées aux différents risques que chaque entité critique a identifiés dans son évaluation des risques, ainsi qu'aux spécificités de l'entité concernée.

Le P.R.E. doit contenir des mesures de résilience qui s'appliquent en fonction des risques auxquels l'entité peut être exposée, compte tenu de la possibilité d'un changement de circonstances. Cela signifie qu'outre les mesures standard, il doit également être possible de renforcer les mesures quand les circonstances le nécessitent. Un renforcement des mesures peut s'avérer nécessaire, par exemple, en cas de menace concrète, de conditions météorologiques défavorables ou de crise sanitaire. L'entité critique est chargée de déterminer les mesures jugées adéquates et nécessaires pour faire face à l'évolution de la situation.

Pour le surplus, le Roi a la possibilité de prévoir des informations ou mesures complémentaires éventuelles que le P.R.E. doit contenir pour un secteur ou un sous-secteur déterminé. La spécificité d'un secteur ou d'un autre peut en effet justifier que l'autorité sectorielle définisse des orientations communes en ce qui concerne les mesures de résilience. La loi fixe dès lors les obligations générales auxquelles des obligations particulières, propres à chaque secteur, peuvent être ajoutées.

De derde paragraaf bevat de weerbaarheidsmaatregelen die het W.P.E. minstens moet bevatten, om te voldoen aan de verplichtingen uit de CER-Richtlijn.

Met het oog op effectiviteit en verantwoording moeten kritieke entiteiten, rekening houdend met de vastgestelde risico's, de maatregelen die zij nemen voldoende gedetailleerd beschrijven in het W.P.E., dan wel een of meer daarmee vergelijkbare documenten, teneinde dat plan in de praktijk toe te passen.

De weerbaarheidsmaatregelen voorgeschreven door het W.P.E. moeten geïmplementeerd worden binnen een termijn van 10 maanden vanaf de aanduiding als kritieke entiteit.

De kritieke entiteit, als eerste verantwoordelijke voor de weerbaarheid van zijn entiteit en bijhorende kritieke infrastructuur, draagt dus de verantwoordelijkheid voor het uitwerken van het W.P.E. en het implementeren van de hierin opgenomen weerbaarheidsmaatregelen.

Wanneer een kritieke entiteit reeds technische-, beveiligings- en organisatorische maatregelen heeft genomen en documenten heeft opgesteld op grond van andere rechtshandelingen die relevant zijn voor weerbaarheidsbevorderende maatregelen uit hoofde van deze wet, moet zij die maatregelen en documenten kunnen gebruiken om aan de voorschriften ten aanzien van de weerbaarheidsmaatregelen uit hoofde van de wet te voldoen. Om dubbel werk te voorkomen kunnen bestaande weerbaarheidsmaatregelen genomen door de kritieke entiteit, die geheel of ten dele voldoen aan de voorschriften van deze Richtlijn, gebruikt worden om te voldoen aan de voorwaarden uit artikel 18.

Wanneer een kritieke entiteit beschikt over een Business Impact Analysis (BIA) en/of een Business Continuity Plan (BCP), dan kan moet men deze kunnen gebruiken om te voldoen aan de voorwaarden uit artikel 18.

Krachtens paragraaf 6 moet de kritieke entiteit daarnaast oefeningen organiseren om het W.P.E. te testen en regelmatig te evalueren. De Koning kan de frequentie van de oefeningen en van de updates bepalen. De bepaalde termijn houdt aldus rekening met de realiteit van de sector of deelsector en van de frequentie die het meest geschikt is, en die per sector of deelsector anders kan zijn.

Delegatie wordt eveneens gegeven aan de Koning teneinde de nadere regels vast te stellen volgens dewelke alle bevoegde diensten, deelnemen aan de oefeningen georganiseerd door de kritieke entiteit.

De verplichtingen van de kritieke entiteit voor wat betreft de weerbaarheidsmaatregelen zijn in principe van toepassing op elke kritieke infrastructuur die zij geïdentificeerd hebben. Gelet op de uitvoerbaarheid van de oefeningen zoals bedoeld in deze paragraaf, volstaat het dat deze uitgevoerd worden op het niveau van kritieke entiteit. Deze oefeningen hebben betrekking op de type risico's waarmee de kritieke entiteit in aanraking kan komen, waarvoor het mogelijk is om oefeningen op te stellen.

Le troisième paragraphe contient les mesures de résilience que le P.R.E. doit au moins contenir afin de répondre aux obligations prévues par la Directive CER.

Dans un souci d'efficacité et de justification, compte tenu des risques identifiés, les entités critiques doivent décrire les mesures qu'elles prennent de façon suffisamment détaillée dans le P.R.E., ou dans un ou plusieurs documents similaires afin d'appliquer ce plan dans la pratique.

Les mesures de résilience prescrites par le P.R.E. doivent être mises en œuvre dans un délai de 10 mois à compter de la désignation en tant qu'entité critique.

En tant que première responsable de la résilience de son entité et de l'infrastructure critique correspondante, l'entité critique est ainsi responsable de l'élaboration du P.R.E. et de la mise en œuvre des mesures de résilience qui y sont reprises.

Lorsqu'une entité critique a déjà pris des mesures techniques, sécuritaires et organisationnelles et établi des documents en vertu d'autres actes juridiques qui sont pertinents pour les mesures de résilience prévues par la présente loi, elle doit pouvoir utiliser ces mesures et documents pour se conformer aux exigences relatives aux mesures de résilience prévues par la présente loi. Pour éviter tout double emploi, les mesures de résilience existantes prises par l'entité critique, qui sont conformes en tout ou en partie aux exigences de la présente Directive, peuvent être utilisées pour remplir les conditions énoncées à l'article 18.

Si une entité critique dispose d'une Business Impact Analysis (BIA) et/ou d'un Business Continuity Plan (BCP), elle devrait avoir la possibilité de les utiliser pour remplir les conditions de l'article 18.

En vertu du paragraphe 6, l'entité critique doit organiser en outre des exercices afin de tester le P.R.E. et l'évaluer régulièrement. Le Roi peut déterminer la fréquence des exercices et des mises à jour. Le délai fixé tient donc compte de la réalité du secteur ou sous-secteur et de la fréquence la plus appropriée, laquelle peut varier selon le secteur ou sous-secteur.

Délégation est également donnée au Roi pour définir les modalités selon lesquelles les services compétents chargés, en vertu de la présente loi, de la mise en œuvre des mesures de protection externes, participent aux exercices organisés par l'entité critique.

Les obligations de l'entité critique en matière de mesures de résilience sont en principe applicables à toute infrastructure critique qu'elle a identifiée. Compte tenu de la faisabilité des exercices visés au présent paragraphe, il suffit qu'ils soient organisés au niveau de l'entité critique. Ces exercices couvrent les types de risques auxquels l'entité critique peut être confrontée et pour lesquels il est possible de mettre en place des exercices.

Artikel 19

Het risico bestaat dat werknemers van kritieke entiteiten of hun contractanten bijvoorbeeld hun toegangsrechten misbruiken om binnen de organisatie van de kritieke entiteit schade te veroorzaken. In artikel 14 van de CER-Richtlijn wordt daarom in een antecedentenonderzoek voorzien. Deze mogelijkheid bestaat reeds in België op grond van artikel 22quiquies, § 2 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereuleerde dienst, welke bepaalt dat een administratieve overheid kan vragen aan zowel privaatrechtelijke als publiekrechtelijke rechtspersonen die deel uitmaken van een betrokken activiteitensector, om over te gaan tot het uitvoeren van een risicobeoordeling binnen de eigen rechtspersoon. Artikel 19 verduidelijkt dat voor de kritieke entiteiten die vallen onder het toepassingsgebied van deze wet, de sectorale overheid of op eigen initiatief van de kritieke entiteit, verzocht kan worden dat een antecedentenonderzoek uitgevoerd wordt in overeenstemming met bovenvermelde wet. Artikel 19 laat de toepassing van de wet van 11 december 1998 dus onverlet. Aan de hand daarvan kan worden nagegaan of er voor een kritieke entiteit overgegaan moet worden tot het uitvoeren van veiligheidsverificaties voor het betrokken personeel.

Dit artikel laat de sectorspecifieke regelingen die hierrond reeds bestaan onverlet.

Artikel 20

Krachtens dit artikel heeft de kritieke entiteit de verplichting om de incidenten die van aard zijn de verlening van essentiële diensten aanzienlijk te verstoren, te notifiëren, zodat de bevoegde overheden snel en adequaat kunnen reageren op incidenten en een volledig overzicht krijgen van de impact, aard, oorzaak en mogelijke gevolgen van incidenten waarmee kritieke entiteiten te maken hebben, en in voorkomend geval de meest geschikte externe beschermingsmaatregelen zouden kunnen nemen.

Deze verplichtingen doet geen afbreuk aan de informatie die verplicht gegeven moet worden aan andere autoriteiten of diensten in het raam van andere wettelijke of reglementaire bepalingen. Het is inderdaad mogelijk dat een bevoegde overheid op dat vlak van beveiliging in een bepaalde sector of deelsector wettelijk gezien verwittigd moet worden van een incident.

Het Nationaal Centraal Contactpunt moet overigens, indien een incident aanzienlijke gevolgen heeft of kan hebben voor kritieke entiteiten en voor de continuïteit van de verlening van essentiële diensten in één of meer lidstaten, het Nationaal Centraal Contactpunt van de betrokken lidstaten verwittigen.

HOOFDSTUK 6

Rapportage en informatie-uitwisseling

Article 19

Le risque existe que les collaborateurs des entités critiques ou leurs contractants abusent par exemple de leurs droits d'accès pour causer des dommages au sein de l'organisation de l'entité critique. L'article 14 de la Directive CER prévoit dès lors une vérification des antécédents. Cette possibilité existe déjà en Belgique sur la base de l'article 22quiquies, § 2, de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité, et au service public réglementé, qui détermine qu'à la demande de l'autorité administrative compétente, les personnes morales de droit public ou de droit privé qui font partie d'un secteur d'activité concerné effectuent une analyse de risques pour elles-mêmes. L'article 19 précise qu'à la demande de l'autorité sectorielle ou de leur propre initiative, les entités critiques qui relèvent du champ d'application de la présente loi peuvent demander une vérification des antécédents effectuée conformément à la loi précitée. L'article 19 s'applique par conséquent sans préjudice de l'application de la loi du 11 décembre 1998. Ceci permet d'examiner si, pour une entité critique, des vérifications de sécurité doivent être effectuées pour le personnel concerné.

Cet article est sans préjudice des réglementations sectorielles qui existent déjà à ce sujet.

Article 20

En vertu de cet article, l'entité critique a l'obligation de notifier les incidents qui sont de nature à perturber de manière importante la fourniture de services essentiels, pour que les autorités compétentes puissent réagir rapidement et adéquatement aux incidents et se faire une idée complète de l'impact, de la nature, de la cause et des conséquences possibles des incidents auxquels les entités critiques sont confrontées et, le cas échéant, prendre les mesures de protection externes les plus adéquates.

Ces obligations ne portent pas préjudice aux informations qui doivent être obligatoirement fournies aux autres autorités ou services dans le cadre d'autres dispositions légales ou réglementaires. Il est en effet possible qu'une autorité compétente doive être avertie d'un incident sur le plan de la sécurité dans un secteur ou sous-secteur déterminé.

Si un incident a ou peut avoir un effet perturbateur important pour les entités critiques ou pour la continuité de la fourniture des services essentiels dans un ou plusieurs Etats membres, le Point de Contact Central National doit par ailleurs en avertir le Point de Contact Central National des Etats membres concernés.

CHAPITRE 6

Rapportage et échange d'informations

Afdeling 1

De bevoegde autoriteiten

Artikel 21

De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit die de rol van deze nationale autoriteit moet vervullen, is het Nationaal Crisiscentrum. Het wordt niet rechtstreeks in de wet vermeld omdat, zoals de afdeling Wetgeving van de Raad van State al heeft opgemerkt, met name in advies 63.296/4, het rechtstreeks aanwijzen van de diensten van de uitvoerende macht die door de Koning zijn opgericht en door Hem aangewezen zijn, een inmenging van de wetgevende macht in de interne organisatie van de uitvoerende macht zou zijn.

Deze autoriteit wordt tevens aangeduid als het Nationaal Centraal Contactpunt voor de weerbaarheid van kritieke entiteiten, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de lidstaten van de Europese Unie. Het betreft de omzetting van artikel 9, tweede lid, van de Richtlijn.

Paragraaf drie geeft delegatie aan de Koning om de coördinerende rol van deze autoriteit verder uit te werken. Het kan gaan over de facilitering van informatie-uitwisseling tussen sectorale overheden onderling, gelet op de nadruk die de CER-Richtlijn legt op de intersectorale afhankelijkheden tussen kritieke entiteiten, alsook over de rol die deze autoriteit kan opnemen ter ondersteuning van de sectorale overheden.

De Koning wijst tevens de sectorale overheden aan die belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet, behalve wanneer de sectorale overheden zelf bij wet werden opgericht.

Artikel 22

Artikel 4 van de CER-Richtlijn legt aan elke lidstaat op om een strategie vast te stellen om de weerbaarheid van kritieke entiteiten te verbeteren, welke moet zorgen voor een integrale aanpak betreffende de weerbaarheid van kritieke entiteiten. De strategie moet de uit te voeren strategische doelstellingen en beleidsmaatregelen bevatten. In het belang van samenhang en efficiëntie moet de strategie zo worden ontworpen dat het bestaande beleid er naadloos in wordt geïntegreerd, en dat waar mogelijk wordt voortgebouwd op bestaande nationale en sectorale strategieën, plannen of soortgelijke documenten.

De Koning wijst de autoriteit aan die verantwoordelijk is voor het opstellen van deze nationale strategie.

Afdeling 2

Informatie-uitwisseling

Section 1^{ère}

Les autorités compétentes

Article 21

Le Roi désigne l'autorité qui, en tant qu'autorité nationale, est chargée de suivre et de coordonner l'application de la présente loi.

L'autorité envisagée pour remplir le rôle d'autorité nationale le Centre de Crise National. Il n'est pas directement cité dans la loi car, comme a déjà pu le préciser la section de législation du Conseil d'Etat, notamment dans l'avis 63.296/4, désigner directement des services du pouvoir exécutif créés par le Roi et qui dépendent de Lui serait une immixtion du pouvoir législatif dans l'organisation interne du pouvoir exécutif.

Cette autorité est également désignée comme Point de Contact Central National pour la résilience des entités critiques, pour tous les secteurs et sous-secteurs, pour la Belgique dans ses relations avec la Commission européenne et les Etats membres de l'Union européenne. Il s'agit de la transpositions de l'article 9, alinéa 2, de la Directive.

Le paragraphe trois donne délégation au Roi pour définir plus avant le rôle de coordination de cette autorité. Il peut s'agir de faciliter l'échange d'informations entre les autorités sectorielles, vu l'accent que la Directive CER met sur les dépendances intersectorielles entre les entités critiques, et de préciser le rôle que cette autorité peut jouer afin de soutenir les autorités sectorielles.

Le Roi désigne également les autorités sectorielles responsables du contrôle de l'application des dispositions de la présente loi, sauf lorsque les autorités sectorielles elles-mêmes ont été instituées par la loi.

Article 22

L'article 4 de la Directive CER impose à chaque Etat membre de définir une stratégie destinée à améliorer la résilience des entités critiques, qui doit garantir une approche intégrale en matière de résilience des entités critiques. La stratégie doit contenir les objectifs et les mesures stratégiques à mettre en œuvre. Dans un souci de cohérence et d'efficacité, la stratégie doit être conçue de façon à intégrer aisément la politique existante et se baser, dans la mesure du possible, sur les stratégies, plans ou documents similaires qui existent au niveau national et sectoriel.

Le Roi désigne l'autorité responsable de la rédaction de cette stratégie nationale.

Section 2

Echange d'informations

Artikel 23

Het NCCN, het OCAD en in voorkomend geval, het CCB, werken, elks vanuit hun eigen bevoegdheden, samen om de bescherming te verzekeren van de kritieke entiteiten op het Belgisch grondgebied.

Om deze opdracht te verwezenlijken moeten ze de nuttige informatie kunnen verzamelen om externe beschermingsmaatregelen te kunnen nemen.

Artikel 24

Dit artikel voorziet in een algemeen samenwerkingsprincipe tussen de kritieke entiteiten en de bevoegde overheden voor de bescherming van kritieke entiteiten teneinde de interne weerbaarheidsmaatregelen en de externe beschermingsmaatregelen op elkaar af te stemmen en op die manier de weerbaarheid van de entiteiten te optimaliseren. De samenwerking met de bevoegde overheden gebeurt op basis van hun eigen opdracht en bevoegdheden.

Deze samenwerking vloeit voort uit artikel 10 van de CER-Richtlijn, dat aanzet tot het faciliteren van de informatie-uitwisseling over aangelegenheden die onder deze Richtlijn vallen.

De verwijzing naar het contactpunt van de kritieke entiteit werd toegevoegd ter volledigheid.

Artikel 25

Artikel 25 verleent een delegatie aan de Koning om te bepalen, voor een bepaalde sector of deelsector, of de informatie in het W.P.E. nuttig kan zijn voor de opdrachten van de verschillende diensten belast met de externe bescherming van de kritieke entiteiten, te weten het NCCN en het OCAD en zo ja, om deze informatie te bepalen en de nadere regels te omschrijven volgens dewelke deze overheden ertoe toegang kunnen krijgen.

Omdat de inhoud van het W.P.E. en de gevoeligheidsgraad van de informatie die het bevat sector per sector verschilt, kan dat niet geval per geval in de wet worden geregeld, maar moet dat per sector gebeuren.

Artikel 26

Dit artikel voorziet de mogelijkheid dat het NCCN en de sectorale overheden de kritieke entiteit op de hoogte brengen van relevante informatie die een impact kan hebben op zijn weerbaarheid of op de externe beschermingsmaatregelen, indien blijkt dat die informatie nuttig zou kunnen zijn voor de aanpassing van de interne weerbaarheidsmaatregelen. Het NCCN dient de noodzaak van een dergelijke mededeling te beoordelen, wat geval per geval moet worden geëvalueerd, aangezien systematische communicatie niet kan worden overwogen gelet op de gevoeligheidsgraad die bepaalde informatie kan hebben. Het NCCN kan een kopie van deze informatie naar de betrokken sectorale overheid sturen teneinde deze op de hoogte te houden van eventuele dreigingen die wegen op haar sector.

Article 23

Le NCCN, l'OCAM et, le cas échéant, le CCB, coopèrent, chacun dans le cadre de ses compétences, en vue d'assurer la protection des entités critiques sur le territoire belge.

Afin de remplir cette mission, ils doivent pouvoir recueillir les informations utiles pour prendre des mesures de protection externes.

Article 24

Le présent article prévoit un principe général de coopération entre les entités critiques et les autorités compétentes pour la protection des entités critiques en vue d'harmoniser les mesures de résilience internes et les mesures de protection externes et d'optimiser ainsi la résilience des entités. La coopération avec les autorités compétentes se fait sur la base de leurs mandat et compétences respectifs.

Cette collaboration découle de l'article 10 de la Directive CER, qui incite à faciliter l'échange d'informations sur des questions qui relèvent de cette Directive.

La référence au point de contact de l'entité critique a été ajoutée par souci d'exhaustivité.

Article 25

L'article 25 donne délégation au Roi afin de déterminer, pour un secteur ou sous-secteur déterminé, si les informations contenues dans le P.R.E. peuvent être utiles pour les missions des différents services chargés de la protection externe des entités critiques, à savoir le NCCN et l'OCAM, et, si tel est le cas, de définir ces informations et les modalités selon lesquelles ces autorités peuvent y avoir accès.

Etant donné que le contenu du P.R.E. et le degré de sensibilité des informations qu'il contient diffèrent secteur par secteur, ceci ne peut pas être réglé au cas par cas dans la loi, mais doit l'être secteur par secteur.

Article 26

Cet article prévoit la possibilité pour le NCCN et les autorités sectorielles de notifier à l'entité critique des informations pertinentes susceptibles d'avoir un impact sur sa résilience ou sur les mesures de protection externes, s'il apparaît que ces informations pourraient être utiles pour l'adaptation des mesures de résilience internes. Le NCCN est tenu d'évaluer la nécessité d'une telle communication en procédant au cas par cas, étant donné qu'une communication systématique ne peut être envisagée au vu du degré de sensibilité de certaines informations. Le NCCN peut envoyer une copie de ces informations à l'autorité sectorielle concernée afin de la tenir informée des menaces éventuelles qui pèsent sur son secteur.

De communicatie van dit soort informatie ligt in de lijn van de coördinerende rol die het NCCN speelt inzake de weerbaarheid van kritieke entiteiten. Het gaat erom een mechanisme in te stellen voor de uitwisseling van informatie, waardoor coördinatie mogelijk moet zijn tussen de overheden en de kritieke entiteiten, en dat daardoor een zekere concordantie bestaat tussen de intern en extern genomen maatregelen.

Artikel 27

Dit artikel voorziet in een beperkte verspreiding van de informatie betreffende de criteria en de drempelwaarden of de niveaus van weerslag van de criteria vastgelegd door de sectorale overheid, omdat die criteria of drempels gevoelige informatie kunnen onthullen over een bepaalde entiteit of infrastructuur, wat haar beveiliging en bescherming kan schaden. Dezelfde beperkte verspreiding is van toepassing op de informatie in het W.P.E. die ter kennis gebracht wordt van de sectorale overheid, van de inspectiedienst, en van het OCAD krachtens dit artikel.

De mogelijkheid om te voorzien in de classificatie "BEPERKT" vindt zijn rechtsgrond in de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst,¹⁵ dat bepaalt: "Het niveau BEPERKT wordt toegekend wanneer de niet-geëigende aanwending nadelig kan zijn voor één van de belangen bedoeld in artikel 3, §1"

In het raam van dit ontwerp vormt het niveau 'BEPERKT' het beschermingsniveau dat minimaal moet worden toegekend aan de betrokken informatie, onverminderd de mogelijkheid voor de bevoegde overheid om deze te classificeren op een ander niveau overeenkomstig de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst.¹⁶ Artikel 3 van deze wet bepaalt inderdaad dat "In een classificatie kunnen worden ondergebracht: informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, waarvan de niet-geautoriseerde toegang of de niet-geëigende aanwending en verspreiding schade kan toebrengen aan een van de volgende belangen:

(...)

- c) de inwendige veiligheid van de Staat, (...);
- e) het wetenschappelijk en economisch potentieel van het land;
- f) elk ander fundamenteel belang van de Staat;

(...)"

Een dergelijke classificatie zal welteverstaan de noodzakelijkheid met zich meebrengen, voor de personen die kennis nodig hebben van deze informatie in de uitoefening van hun functies, houder te zijn van een veiligheidsmachtiging van een passend niveau, hetzij vertrouwelijk, geheim of zeer geheim volgens het

La communication de ce type d'informations s'inscrit dans le rôle de coordination que le NCCN remplit en matière de résilience des entités critiques. Il s'agit d'instaurer un mécanisme d'échange d'informations qui devrait permettre une coordination entre les autorités et les entités critiques, et ainsi de garantir une certaine concordance entre les mesures prises en interne et en externe.

Article 27

Cet article prévoit une diffusion limitée des informations relatives aux critères et aux valeurs seuils ou aux niveaux de répercussion des critères fixés par les autorités sectorielles, parce que ces critères ou seuils peuvent entraîner la divulgation d'informations sensibles concernant une entité ou infrastructure déterminée, ce qui peut nuire à sa sécurité et sa protection. Cette même diffusion limitée s'applique aux informations contenues dans le P.R.E. et qui sont portées à la connaissance des autorités sectorielles, du service d'inspection, et de l'OCAM en vertu du présent article.

La possibilité de prévoir la classification 'RESTREINT' trouve son fondement juridique dans la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité, et au service public réglementé,¹⁵ qui stipule : « le niveau RESTREINT est attribué lorsque l'utilisation inappropriée peut être défavorable à un des intérêts visés à l'article 3, § 1^{er} »

Dans le cadre du présent projet, le niveau 'RESTREINT' constitue le niveau de protection qui doit au moins être accordé aux informations concernées, sans préjudice de la possibilité pour l'autorité compétente de les classer à un autre niveau conformément à la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité, et au service public réglementé.¹⁶ L'article 3 de cette loi stipule en effet que "Peuvent faire l'objet d'une classification : les informations, documents ou données, le matériel, les matériaux ou matières, sous quelque forme que ce soit, dont l'accès non autorisé ou l'utilisation et la divulgation inappropriée peut porter atteinte à l'un des intérêts suivants:

(...)

- c) la sûreté intérieure de l'Etat, (...);
- e) le potentiel scientifique et économique du pays;
- f) tout autre intérêt fondamental de l'Etat;

(...)"

Une telle classification entraînera bien entendu la nécessité, pour les personnes qui ont besoin d'avoir connaissance de ces informations dans l'exercice de leurs fonctions, d'être détenteur d'une habilitation de sécurité d'un niveau approprié, soit confidentiel, secret ou très secret selon le niveau de classification. En vertu de

¹⁵ BS, 31 maart 2000.

¹⁶ BS, 7 mei 1999.

¹⁵ M.B., 31 mars 2000.

¹⁶ M.B., 7 mai 1999.

classificatieniveau. Volgens artikel 8 van de wet van 1998 hoeft een persoon evenwel geen houder te zijn van een veiligheidsmachtiging om toegang te hebben tot geclassificeerde informatie van het niveau BEPERKT.

Artikel 28

Dit artikel legt de kritieke entiteit de verplichting van het beroepsgeheim op voor alle informatie in het W.P.E., omdat daarin gevoelige informatie kan staan die, indien ze bekend zou worden, de weerbaarheid van de kritieke entiteit zou kunnen schaden.

Onverminderd artikel 25, dat voorziet in het recht voor de inspectiedienst en voor het OCAD om, binnen de door de Koning bepaalde grenzen, geheel of gedeeltelijk toegang te hebben tot het W.P.E., mag dergelijke informatie enkel maar worden overgemaakt aan personen die deze nodig hebben in de uitoefening van hun functies of opdracht. Het gaat dan met name om personen die gemachtigd zijn om veiligheidskwesties te behandelen in het raam van het contactpunt van de kritieke entiteit, alsook van de sectorale overheid.

Hetzelfde geheim is van toepassing op de informatie waarvan sprake is in Hoofdstuk 4 van het ontwerp van wet alsook op de informatie die aan de entiteit in kennis wordt gebracht met toepassing van Hoofdstuk 4, de artikelen 18, §6, 20, 24 en 26.

Dit beroepsgeheim overtreden is onderhevig aan de straffen voorzien bij artikel 458 van het Strafwetboek.

Artikel 29

Aangezien het gaat om een beperkte verspreiding of om een classificatie bedoeld door het artikel 27 van dit ontwerp, dient het doel van bescherming van belangen hiervoor uiteengezet logischerwijze te primeren op het principe van openbaarheid van bestuur.

Artikel 30

De sectorale overheid komt, in het kader van haar taak als bevoegde autoriteit voor de kritieke entiteiten, mogelijks in contact met geclassificeerde informatie. Hiernaast betreft alle informatie omtrent de weerbaarheid van kritieke entiteiten steeds gevoelige informatie. Teneinde een zo vlot mogelijke informatie doorstroom te faciliteren, werd er gekozen om de verplichting op te leggen voor het personeel dat toegang heeft tot informatie betreffende de weerbaarheid van kritieke entiteiten, om ervoor te zorgen dat minstens één iemand van dit personeel over een veiligheidsmachtiging van het niveau GEHEIM beschikt, als bedoeld in Hoofdstuk III van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsattesten, veiligheidsadviezen en de publiek gereguleerde dienst. De veiligheidsmachtiging betreft informatie uit België, de EU en NAVO. Op deze manier wordt er een veiligheidscultuur gecreëerd in de sectorale overheden, en is er zekerheid dat wanneer er geclassificeerde informatie gedeeld moet worden met een welbepaalde sectorale overheid, dit ook mogelijk is in de praktijk.

l'article 8 de la loi de 1998, il n'est pas nécessaire d'être titulaire d'une habilitation de sécurité pour avoir accès à des informations classifiées de niveau RESTREINT.

Article 28

Le présent article impose à l'entité critique l'obligation du secret professionnel pour toutes les informations contenues dans le P.R.E., étant donné que ce dernier peut contenir des informations sensibles qui, si elles venaient à être divulguées, pourraient porter préjudice à la résilience de l'entité critique.

Sans préjudice à l'article 25, qui prévoit le droit pour le service d'inspection et pour l'OCAM d'accéder en tout ou en partie au P.R.E., dans les limites fixées par le Roi, ces informations peuvent uniquement être transmises aux personnes qui en ont besoin dans l'exercice de leurs fonctions ou de leur mission. Il s'agit notamment de personnes qui sont autorisées à traiter les questions de sécurité dans le cadre du point de contact de l'entité critique, ainsi que de l'autorité sectorielle.

Le même secret s'applique aux informations dont il est question au Chapitre 4 du projet de loi, ainsi qu'aux informations qui sont portées à la connaissance de l'entité en application du Chapitre 4, des articles 18, § 6, 20, 24 et 26.

La violation de ce secret professionnel est punie des peines prévues à l'article 458 du Code pénal.

Article 29

Etant donné qu'il s'agit d'une diffusion limitée ou d'une classification prévue à l'article 27 du présent projet, l'objectif de protection des intérêts, tel qu'exposé ci-avant, doit en toute logique primer sur le principe de publicité de l'administration.

Article 30

L'autorité sectorielle, dans le cadre de son rôle d'autorité compétente pour les entités critiques, peut entrer en contact avec des informations classifiées. En outre, toutes les informations relatives à la résilience des entités critiques concernent toujours des informations sensibles. Afin de faciliter au maximum la circulation des informations, il a été décidé d'imposer au personnel ayant accès aux informations relatives à la résilience des entités critiques l'obligation de veiller à ce qu'au moins une personne de ce personnel dispose d'une habilitation de sécurité de niveau SECRET, telle que visée au chapitre III de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, attestations de sécurité, avis de sécurité, et au service public réglementé. L'habilitation de sécurité concerne les informations provenant de la Belgique, de l'UE et de l'OTAN. De cette manière, une culture de la sécurité est créée au sein des autorités sectorielles, et il est garanti que lorsque des informations classifiées doivent être partagées avec une autorité sectorielle spécifique, ce partage est également possible dans la pratique.

Delegatie wordt gegeven aan de Koning om het gehele of een deel van het W.P.E. te classificeren. Dit volgt uit het feit dat men in het W.P.E. alle relevante informatie in acht moet nemen, waaronder mogelijk geclassificeerde informatie. Het betreft geen verplichting hiertoe, aangezien dit ook administratieve gevolgen met zich meebrengt. De Koning waakt erover dat de bevoegde personen binnen de kritieke entiteit ten allen tijde toegang hebben tot hun volledige W.P.E. Dit houdt in dat, in het geval van classificatie, deze personen ook beschikken over een adequaat niveau van veiligheidsmachtiging.

HOOFDSTUK 7

Controle en sancties

Afdeling 1

Inspecties en audits

Artikel 31

Artikel 31 organiseert de controle op de naleving van zijn verplichtingen door de kritieke entiteit. Per sector moet door de Koning een inspectiedienst worden aangeduid die voor deze controle instaat, op initiatief van de Minister die bevoegd is voor de sector. In voorkomend geval, kan een inspectiedienst per deelsector worden aangewezen, naargelang zijn eigen bijzonderheden.

Er wordt delegatie gegeven aan de Koning om de nadere regels voor de controle te bepalen. Deze nadere regels moeten onder andere de opdrachten van de inspectiedienst, de frequentie van de controles, de minimale voorwaarden waaraan de inspectieleden moeten voldoen en de punten waarop de controle dient te gebeuren of de rapportering die aan de sectorale overheid moet worden gedaan, betreffen.

Artikel 32

Artikel 21.1, b) van de CER-Richtlijn legt de verplichting op dat de bevoegde autoriteiten over de bevoegdheden en middelen beschikken om audits uit te voeren of te gelasten met betrekking tot kritieke entiteiten. Er wordt delegatie gegeven aan de Koning om de nadere regels omtrent de audits vast te leggen, zodat rekening gehouden kan worden met de specificiteiten van elke sector.

Afdeling 2

Procedure van de sancties

Dit ontwerp biedt naast de mogelijkheid tot strafsancities, nu ook de mogelijkheid tot het opleggen van administratieve sancties. De KI-wet bevatte enkel strafsancities, maar in de praktijk bleek dat het eerder ging over formele inbreuken die niet leidden tot ernstige incidenten. Het doel van sancties te voorzien is om een drukingsmiddel ter beschikking te hebben wanneer nodig. De toevoeging van administratieve sancties zorgt

Une délégation est donnée au Roi pour classer tout ou partie du P.R.E. Ceci découle du fait que toutes les informations pertinentes dans le P.R.E. doivent être prises en compte, y compris les informations potentiellement classifiées. Il ne s'agit pas d'une obligation, car ceci a également des implications administratives. Le Roi veille à ce que les personnes autorisées au sein de l'entité critique aient à tout moment accès à l'intégralité de leur P.R.E. Cela implique qu'en cas de classification, ces personnes disposent également d'un niveau d'habilitation de sécurité adéquat.

CHAPITRE 7

Contrôle et sanctions

Section 1^{ère}

Inspections et audits

Article 31

L'article 31 organise le contrôle du respect de ses obligations par l'entité critique. Par secteur, le Roi désigne un service d'inspection qui se charge de ce contrôle, à l'initiative du ministre chargé du secteur. Le cas échéant, un service d'inspection peut être désigné par sous-secteur en fonction de ses particularités.

Une délégation est donnée au Roi pour déterminer les modalités du contrôle. Ces modalités doivent, entre autres, porter sur les missions du service d'inspection, la fréquence des inspections, les conditions minimales à remplir par les membres de l'inspection et les points à inspecter, ou les rapports à faire à l'autorité sectorielle.

Article 32

L'article 21.1, b) de la Directive CER impose aux autorités compétentes de disposer des compétences et des moyens pour effectuer des audits concernant les entités critiques. Une délégation est donnée au Roi pour fixer les modalités des audits afin de tenir compte des spécificités de chaque secteur.

Section 2

Procédure de sanctions

Outre la possibilité de sanctions pénales, ce projet prévoit désormais la possibilité de sanctions administratives. La loi IC ne prévoyait que des sanctions pénales, mais dans la pratique, il s'est avéré qu'il s'agissait davantage d'infractions formelles qui n'entraînaient pas d'incidents graves. L'objectif des sanctions est de disposer d'un moyen de pression en cas de besoin. L'ajout de sanctions administratives garantit que si le Procureur du Roi décide

ervoor dat, wanneer de Procureur des Konings beslist om geen strafrechtelijke vervolging in te stellen, de sectorale overheid alsnog een administratieve sanctie kan opleggen aan de overtreder. Verplichtingen hebben immers meer gewicht als de niet-naleving ervan kan leiden tot sancties.

De toevoeging van de mogelijkheid om administratieve sancties op te leggen zorgt tevens voor harmonisatie in de sanctionering van kritieke entiteiten tussen de verschillende sectoren en deelsectoren. Sommige sectoren of deelsectoren kunnen reeds op basis van sectorspecifieke wetgeving administratieve sancties opleggen, terwijl andere sectoren dergelijk kader missen en dit dus niet kunnen. Dit zorgt voor grote verschillen en een ongelijkheid van behandeling tussen de sectoren, zowel voor wat betreft de hoogte van de administratieve boetes als voor wat betreft de procedurele aspecten. Daarnaast zorgt de toevoeging ervan voor een duidelijkere samenhang met de NIS 2-Richtlijn. De entiteiten die als kritiek geïdentificeerd worden onder CER, zullen ook essentiële entiteiten zijn onder NIS 2. Het is niet onwaarschijnlijk dat een bepaalde inbreuk, zowel een inbreuk op de CER- als de NIS 2-regelgeving uitmaakt, waardoor het van belang is dat het sanctiemechanisme van beide kaders coherent is.

Het kader voor administratieve sancties in deze wet doet geen afbreuk aan de reeds bestaande regelgeving voor administratieve sancties in bepaalde sectoren of deelsectoren. Afdeling 4 is bedoeld voor sectoren of deelsectoren die niet kunnen terugvallen op sectorspecifieke regelgeving voor administratieve sancties.

Artikel 33

Het artikel beschrijft de procedure voor de vaststelling van inbreuken op de wet, de uitvoeringsbesluiten ervan of de hieraan verbonden individuele administratieve beslissingen.

Een eerste remediëringstermijn wordt bepaald door middel van een formele ingebrekestelling. Deze wordt voorafgegaan door een gemotiveerde mededeling aan de kritieke entiteit, die de mogelijkheid heeft om opmerkingen te formuleren en kan vragen om te worden gehoord. Vervolgens stuurt de inspectiedienst de overtreder de ingebrekestelling, met een termijn waarbinnen de kritieke entiteit zich in regel moet stellen.

Artikel 34

Bij een gebrek aan remediëring na een ingebrekestelling, wordt een proces-verbaal opgemaakt door de beëdigde personeelsleden van de inspectiedienst en wordt een kopie van het proces-verbaal overgemaakt aan de sectorale overheid. Het origineel van het proces-verbaal wordt overgemaakt aan de Procureur des Konings.

De wet kent bijzondere bewijskracht toe aan de materiële vaststellingen die het voorwerp uitmaken van dat proces-verbaal. Dit is gerechtvaardigd gezien de technische aard van deze vaststellingen, die het in de praktijk moeilijk maakt om sommige aspecten van de in de wet bedoelde inbreuken vast te stellen op een andere wijze dan door de

de ne pas engager de poursuites pénales, l'autorité sectorielle peut toujours imposer une sanction administrative à l'auteur de l'infraction. En effet, les obligations ont plus de poids si leur non-respect peut entraîner des sanctions.

L'ajout de la possibilité d'imposer des sanctions administratives garantit également l'harmonisation des sanctions à l'encontre des entités critiques dans les différents secteurs et sous-secteurs. Certains secteurs ou sous-secteurs peuvent déjà imposer des sanctions administratives sur la base d'une législation sectorielle, tandis que d'autres secteurs ne disposent pas d'un tel cadre et ne peuvent donc pas le faire. Ceci crée des différences significatives et une inégalité de traitement entre les secteurs, tant en ce qui concerne le niveau des amendes administratives que les aspects procéduraux. En outre, l'ajout de cette disposition renforce la cohérence avec la Directive NIS 2. Il n'est pas improbable qu'une infraction donnée constitue une infraction à la fois à la réglementation CER et à la réglementation NIS 2, d'où l'importance de la cohérence du mécanisme de sanction prévu par les deux cadres.

Le cadre des sanctions administratives dans cette loi est sans préjudice des réglementations déjà existantes pour les sanctions administratives dans certains secteurs ou sous-secteurs. La section 4 est destinée aux secteurs ou sous-secteurs qui ne peuvent pas s'appuyer sur des réglementations sectorielles spécifiques pour les sanctions administratives.

Article 33

L'article décrit la procédure de constatation des violations de la loi, de ses décrets d'application ou des décisions administratives individuelles y afférentes.

Une première période de recours est déterminée par une mise en demeure. Celle-ci est précédée d'une mise en demeure motivée adressée à l'entité critique, qui a la possibilité de présenter des observations et de demander à être entendue. Le service d'inspection envoie ensuite la mise en demeure au contrevenant, assortie d'un délai dans lequel l'entité critique doit se mettre en conformité.

Article 34

En cas de non-réparation après une mise en demeure, un procès-verbal est dressé par le personnel assermenté du service de contrôle et une copie du procès-verbal est remise à l'autorité sectorielle. L'original du procès-verbal est remis au Procureur du Roi.

La loi attribue une force probante particulière aux constatations matérielles qui font l'objet de ce procès-verbal. Cela se justifie par le caractère technique de ces constatations qui, en pratique, rendent difficile la constatation de certains aspects des infractions visées par la loi autrement que par des inspecteurs ou des experts assermentés. En outre, les droits de l'accusé ne sont pas

beëdigde inspecteurs of experten. Bovendien worden de rechten van de beklaagde niet beperkt aangezien het mogelijk blijft om het tegenbewijs aan te leveren met alle bewijsmiddelen die de rechter zal beoordelen.

Artikel 35

Het is niet mogelijk om zowel strafrechtelijke als administratieve sancties op te leggen aan een kritieke entiteit. Indien er een strafrechtelijke sanctie werd opgelegd, zal het opleggen van een administratieve sanctie niet meer mogelijk zijn.

Artikel 36

Volgens dit artikel beschikt de Procureur des Konings over een termijn van twee maanden te rekenen vanaf de ontvangst van het proces-verbaal om een strafrechtelijke vervolging in te stellen tegen de kritieke entiteit, die hierover binnen dezelfde termijn wordt ingelicht. De dag van ontvangst wordt geacht de derde dag te zijn die volgt op deze waarop het kopie van het proces-verbaal aan de postdiensten overhandigd werd, tenzij de geadresseerde het tegendeel bewijst.

Er mag geen administratieve geldboete worden opgelegd voor het verstrijken van deze termijn of voor de beslissing van de Procureur des Konings om niet te vervolgen.

Artikel 37

Voor wat betreft de deelsector vervoer over water zal een inbreuk op deze wetgeving vaak gelijklopen aan een inbreuk op het Belgisch Scheepvaartwetboek en de ISPS-Code. Hiervoor is een volledig eigen systeem van administratieve sancties voorzien overeenkomstig de wet van 25 december 2016 tot instelling van administratieve geldboetes van toepassing in geval van inbreuken op de scheepvaartwetten. Procedureel is het niet opportuun om een ander systeem van administratieve boetes in te stellen voor deze deelsector.

Afdeling 3

Strafrechtelijke sancties

Artikel 38

Dit artikel bepaalt de strafsancities die van toepassing zijn op de kritieke entiteit bij het niet in acht nemen van de verplichtingen die worden opgelegd bij dit ontwerp en bij de uitvoeringsbesluiten ervan, evenals in geval van belemmering van de controles uitgevoerd door de inspectiediensten.

Het strafstelsel is gebaseerd op wat bepaald werd in de wet KI, en dus reeds sinds 2011 in voege is. De afwezigheid van de weerbaarheidsmaatregelen, het niet uitvoeren ervan of het verzuim de overheden te informeren over elke gebeurtenis die de weerbaarheid van kritieke entiteiten kan treffen, kunnen gevolgen hebben voor de essentiële dienstverlening, hetgeen een zekere strengheid van bestraffing verantwoordt. Het gaat erom de

limités, puisqu'il reste possible de prouver le contraire à l'aide de tout élément de preuve que le tribunal appréciera.

Article 35

Il n'est pas possible d'imposer à la fois des sanctions pénales et administratives à une entité critique. Si une sanction pénale a été imposée, l'imposition d'une sanction administrative ne sera plus possible.

Article 36

Selon cet article, le Procureur du Roi dispose d'un délai de deux mois à compter de la réception du procès-verbal pour engager des poursuites pénales à l'encontre de l'entité critique, qui est notifiée dans le même délai. Le jour de réception est réputé être le troisième jour suivant celui où la copie du procès-verbal a été remise aux services postaux, sauf preuve contraire apportée par le destinataire.

Aucune amende administrative ne peut être imposée avant l'expiration de ce délai ou avant la décision du Procureur du Roi de ne pas poursuivre.

Article 37

En ce qui concerne le sous-secteur du transport par voie d'eau, une infraction à cette législation sera souvent équivalente à une infraction au Code maritime belge et au Code ISPS. Pour ce faire, un système de sanctions administratives totalement distinct est prévu conformément à la loi du 25 décembre 2016 établissant les amendes administratives applicables en cas d'infraction à la législation sur la navigation. D'un point de vue procédural, il n'est pas opportun d'établir un autre système d'amendes administratives pour ce sous-secteur.

Section 3

Les sanctions pénales

Article 38

Le présent article détermine les sanctions pénales qui s'appliquent à l'entité critique en cas de non-respect des obligations qui sont imposées par le présent projet et ses arrêtés d'exécution, ainsi qu'en cas d'obstacle aux contrôles effectués par les services d'inspection.

Le système pénal se base sur les dispositions de la loi IC et est donc déjà en vigueur depuis 2011. L'absence de mesures de résilience, leur non-exécution ou le fait de ne pas informer les autorités de chaque événement susceptible de nuire à la résilience des entités critiques, peut avoir des répercussions sur les services essentiels, ce qui justifie une certaine sévérité de la sanction. Il s'agit de responsabiliser l'entité critique quant à l'impact qu'elle-

kritieke entiteit te responsabiliseren voor de impact dat zijn entiteit, en bijhorende kritieke infrastructuur, kan hebben op de essentiële dienstverlening in het land.

Afdeling 4

Administratieve sancties

Artikel 39

Dit artikel vermeldt het principe en het bedrag van de administratieve sancties.

Artikel 40

Dit artikel regelt de principes voor het bepalen van het bedrag van de administratieve sanctie, de in aanmerking te nemen omstandigheden, de situaties van herhaling en de situaties van samenloop van inbreuken.

Met het oog op de eerbiediging van de rechten van verdediging is bepaald dat de overtreder kan worden gehoord of zijn verweermiddelen schriftelijk kan indienen binnen een termijn van vijftien dagen.

Artikel 41

Dit artikel bepaalt dat de beslissing ter kennis wordt gebracht van de overtreder.

Artikel 42

Dit artikel bepaalt de voorwaarden waarin de beslissing uitvoerbaar wordt.

Artikel 43

Uit dit artikel blijkt dat de verjaringstermijn voor administratieve geldboetes drie jaar bedraagt.

HOOFDSTUK 8

Sector overheid

Artikel 44

Het wetgevend kader betreffende de kritieke entiteiten, dat historisch gezien werd opgesteld voor, en enkel werd toegepast op, de privésector, is niet zo eenvoudig op volledig dezelfde manier toepasbaar op de sector overheid. De weerbaarheid van de overheidsinstellingen in België is uiteraard minstens even belangrijk als in de privésector, doch noodzaakt de specificiteit van deze sector eigenlijk een gespecialiseerd of aangepast kader.

In de eerste plaats bemoeilijkt dit de keuze voor een sectorale overheid aangezien de scheidingslijn met de kritieke entiteit in deze sector vervaagt. Het zou daarnaast ook niet werkbaar zijn om de ene overheidsdienst aan de andere normen en verplichtingen te laten opleggen en doen afdwingen, waardoor het onmogelijk is om een algemene sectorale overheid voor de gehele sector aan te duiden. Ten slotte is de situatie voor elke federale

même et son infrastructure critique peuvent avoir sur les services essentiels du pays.

Section 4

Les sanctions administratives

Article 39

Cet article énonce le principe et le montant des sanctions administratives.

Article 40

Cet article régit les principes de détermination du montant de la sanction administrative, les circonstances à prendre en compte, les situations de répétition et les situations de concours d'infractions.

Afin de respecter les droits de la défense, il est prévu que le contrevenant peut être entendu ou peut présenter sa défense par écrit dans un délai de quinze jours.

Article 41

Cet article précise que la décision sera notifiée à l'auteur de l'infraction.

Article 42

Cet article définit les conditions dans lesquelles la décision devient exécutoire.

Article 43

Cet article indique que le délai de prescription pour les amendes administratives est de trois ans.

CHAPITRE 8

Secteur des administrations publiques

Article 44

Le cadre législatif sur les entités critiques, historiquement rédigé et appliqué uniquement au secteur privé, n'est pas si facilement applicable de la même manière au secteur public. La résilience des institutions publiques en Belgique est évidemment au moins aussi importante que dans le secteur privé, mais la spécificité de ce secteur nécessite en fait un cadre spécialisé ou adapté.

En premier lieu, ceci complique le choix d'une autorité sectorielle, car la ligne de démarcation avec l'entité critique dans ce secteur est floue. En outre, il ne serait pas envisageable qu'une administration impose et fasse respecter des normes et des obligations à une autre, ce qui rendrait impossible la désignation d'une autorité sectorielle générale pour l'ensemble du secteur. Enfin, la situation étant différente pour chaque ministère fédéral, il

overheidsdienst verschillend, zodat het noodzakelijk is dat elke Minister zelf de invulling van de verplichtingen uit de wet kan vastleggen. Het wordt daarom niet opportuun geacht om alles in de wet zelf vast te leggen. Bijgevolg zal delegatie aan de Koning gegeven worden zodat dit sectoraal, en meer bepaald, per bevoegde minister, geregeld kan worden.

Omwille van de bovenstaande bijzondere eigenschappen van de sector overheid en de uitdagingen die deze met zich meebrengen wordt voor deze sector een bijzonder kader opgericht, gebaseerd op de verplichtingen uit de CER-Richtlijn en aangepast aan de specificiteiten van de sector. Voor deze sector zal volledig de *ratio legis* van de CER-Richtlijn gevolgd worden.

Op deze manier voldoet België aan zijn verplichting om de CER-Richtlijn tijdig om te zetten in nationale regelgeving, rekening houdend met de verschillen die bestaan tussen de private en publieke sector.

HOOFDSTUK 9

Diverse bepalingen

Artikelen 45 t.e.m. 73

Elke vermelding van het wetgevend kader uit de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur, alsook de verwijzing naar de term 'kritieke infrastructuur' wordt aangepast naar de nieuwe term 'kritieke entiteit' en het nieuwe wetgevend kader uit dit ontwerp.

De bepaling tot wijziging van de wet van 10 juli 2006 in artikel 54 strekt tot uitbreiding van de verplichting van de ondersteunende diensten om persoonsgegevens en informatie mee te delen waarover zij beschikken in het kader van hun wettelijke taken en die relevant zijn voor de doeleinden van de dreigingsanalyse bedoeld in artikel 8, tweede lid, van de wet betreffende de weerbaarheid van kritieke entiteiten.

Deze wijziging is noodzakelijk door de uitbreiding van de reikwijdte van de dreigingsanalyse in het kader van de weerbaarheid van kritieke entiteiten, die niet alleen terroristische en extremistische dreigingen omvat, maar elk type dreiging wanneer het OCAD dit relevant acht voor de sector of deelsector.

HOOFDSTUK 10

Slotbepalingen

Artikel 74

Omdat de Richtlijn slechts een minimumharmonisatie voorziet, en dat het daarnaast in de toekomst opportuun kan blijken om nieuwe sectoren aan te duiden of de draagwijdte van bepaalde sectoren uit te breiden, wordt aan de Koning machtiging gegeven om wetbepalingen op te heffen, aan te vullen, te wijzigen of te vervangen met het oog op het verzekeren van de omzetting van de

est nécessaire que chaque ministre puisse définir l'interprétation des obligations prévues par la loi. Il n'est donc pas jugé opportun de tout fixer dans la loi elle-même. C'est la raison pour laquelle délégation sera donnée au Roi afin que ceci puisse être réglé sectoriellement, et plus précisément, par ministre compétent.

En raison des caractéristiques particulières du secteur public et des défis qu'il pose, un cadre spécial sera établi pour ce secteur, basé sur les obligations de la Directive CER et adapté à ses spécificités. La *ratio legis* de la Directive CER sera intégralement respectée pour ce secteur.

De cette manière, la Belgique remplit son obligation de transposer la Directive CER dans la réglementation nationale en temps voulu, en tenant compte des différences qui existent entre le secteur privé et le secteur public.

CHAPITRE 9

Dispositions diverses

Articles 45 à 73

Toute référence au cadre législatif de la loi du 1^{er} juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, ainsi que la référence au terme "infrastructure critique" doivent être adaptées au nouveau terme "entité critique" et au nouveau cadre législatif du présent projet.

La disposition modificative de la loi du 10 juillet 2006 dans l'article 54 vise à étendre l'obligation des services d'appui de communiquer les données à caractère personnel et les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents en vue d'atteindre les finalités de l'analyse de la menace visée à l'article 8, § 2, de la loi relative à la résilience des entités critiques.

Cette modification est rendue nécessaire par le champ étendu de l'analyse de la menace dans le cadre de la résilience des entités critiques qui porte non pas uniquement sur les menaces terroristes et extrémistes mais bien sur tout type de menace lorsque l'OCAM le juge pertinent par rapport au secteur ou au sous-secteur.

CHAPITRE 10

Dispositions finales

Article 74

Etant donné que la Directive prévoit seulement une harmonisation minimale et qu'il peut s'avérer opportun, à l'avenir, de désigner de nouveaux secteurs ou d'étendre la portée de certains secteurs, le Roi est habilité à abroger, ajouter, modifier ou remplacer des dispositions légales en vue d'assurer la transposition des directives européennes en matière de résilience des entités critiques. Vu

Europese richtlijnen met betrekking tot de weerbaarheid van kritieke entiteiten. Gelet op de huidige geopolitieke situatie houdt de weerbaarheid van kritieke entiteiten immers een prioriteit in, zowel op Europees als nationaal niveau. Inderdaad, wanneer een toekomstige richtlijn nieuwe sectoren zal toevoegen, of de bestaande verplichtingen zal aanpassen, zal het gaan om het aanbrengen van technische aanpassingen aan de regelgeving, zonder dat een beweegruimte wordt gelaten aan de Lidstaten. Derhalve is het volkomen gerechtvaardigd een machtiging te geven aan de Koning om deze aanpassingen aan te brengen.

Daarnaast wordt dezelfde machtiging aan de Koning gegeven om de regels op vlak van de weerbaarheid van kritieke entiteiten uit te breiden naar andere sectoren voor dewelke in de toekomst de bescherming van hun weerbaarheid noodzakelijk zou blijken in het belang van de ene of de andere essentiële dienstverlening.

De maatregelen genomen door de Koning zullen het voorwerp uitmaken van een overleg in de Ministerraad.

Artikel 75

Gelet op het uitvoerige kader dat in deze wet vervat zit met betrekking tot de weerbaarheid van kritieke entiteiten, wordt de wet van 1 juli 2011 betreffende de bescherming en de beveiliging van kritieke infrastructuur opgeheven. Het huidige ontwerp bestendigt het wetgevend kader uit de KI-wet, en breidt het verder uit op basis van de verplichtingen uit de CER-Richtlijn.

Artikel 76

Volgens de termijnen vervat in deze wet moeten de kritieke entiteiten 10 maanden na de kennisgeving van aanduiding als kritieke entiteit de weerbaarheidsmaatregelen uit het W.P.E. implementeren. Deze aanduiding dient uiterlijk te gebeuren op 17 juli 2026. Teneinde rechtszekerheid en continuïteit te waarborgen met betrekking tot het statuut als exploitant van kritieke infrastructuur wordt in dit artikel een overgangsbepaling voorzien, waarin bepaald wordt dat alle exploitanten van kritieke infrastructuur die op grond van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuur als zodanig werden geïdentificeerd, vanaf 17 juli 2026 van rechtswege beschouwd worden als kritieke entiteiten.

Deze entiteiten zullen echter tot 17 mei 2027 gehouden worden aan de verplichtingen waaraan zij moesten voldoen op grond van de artikelen 13, 13/1, 13/2 en 14 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuur, zodat er geen leemte kan ontstaan tussen de opheffing van wet van 2011 en de inwerkingtreding van de verplichtingen voor kritieke entiteiten uit dit ontwerp, en zodat het huidige veiligheidsniveau kan worden behouden tijdens de overgangsperiode.

Artikel 77

Een dreigingsanalyse houdt rekening met de huidige, te verwachten en toekomstige dreiging. Er is dus geen reden waarom de analyse herhaald zou moeten worden als er

notamment la situation géopolitique actuelle, la résilience des entités critiques est en effet une priorité, tant au niveau européen que national. En effet, lorsqu'une future directive ajoutera de nouveaux secteurs ou adaptera les obligations existantes, il s'agira d'apporter des adaptations techniques à la réglementation sans laisser de marge de manœuvre aux Etats membres. Il est par conséquent totalement justifié d'habiliter le Roi à procéder à ces adaptations.

En outre, la même habilitation est donnée au Roi pour ce qui est d'étendre les règles de résilience des entités critiques à d'autres secteurs pour lesquels la protection de leur résilience s'avèrerait nécessaire à l'avenir, dans l'intérêt de l'un ou de l'autre service essentiel.

Les mesures prises par le Roi feront l'objet d'une délibération en Conseil des ministres.

Article 75

Vu le cadre détaillé prévu par la présente loi en ce qui concerne la résilience des entités critiques, la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est abrogée. Le projet actuel perpétue le cadre législatif de la loi IC et l'élargit sur base des obligations de la Directive CER.

Article 76

Selon les délais prévus dans la présente loi, les entités critiques doivent mettre en œuvre les mesures de résiliences du P.R.E. 10 mois après la notification de leur désignation en tant qu'entité critique. Cette désignation doit avoir lieu au plus tard le 17 juillet 2026. Afin d'assurer la sécurité juridique et la continuité du statut d'opérateur d'infrastructure critique, cet article prévoit une disposition transitoire, stipulant que tous les opérateurs d'infrastructures critiques identifiés comme tels en vertu de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques sont réputés être des entités critiques de plein droit à partir du 17 juillet 2026.

Toutefois, ces entités seront tenues aux obligations qu'elles devaient remplir en vertu des articles 13, 13/1, 13/2 et 14 de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques jusqu'au 17 mai 2027, de sorte qu'il ne peut y avoir de décalage entre l'abrogation de la loi de 2011 et l'entrée en vigueur des obligations pour les entités critiques en vertu du présent projet, et de manière à ce que puisse être maintenu le niveau de sécurité actuel pendant la période de transition.

Article 77

Une analyse de la menace tient compte de la menace actuelle, prévisible et à venir. Il n'y a, par conséquent, pas de raison que l'analyse soit renouvelée lors de l'entrée en

nieuwe wetgeving van kracht wordt. Analyses die minder dan 4 jaar geleden zijn uitgevoerd, blijven daarom geldig voor de rest van de tijd, tenzij er een nieuwe factor zou zijn die een nieuwe dreigingsanalyse vereist.

Dit is, Dames en Heren, de inhoud van het ontwerp van wet dat de Regering de eer heeft aan uw beraadslagingen voor te leggen.

De Minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing,

vigueur d'une nouvelle législation. Les analyses réalisés il y a moins de 4 ans restent donc valables et ce, pour le solde de temps restant, sauf en cas de nouvel élément nécessitant une nouvelle analyse de la menace.

Telle est, Mesdames, Messieurs, la teneur du projet de loi que le Gouvernement a l'honneur de soumettre à vos délibérations.

La Ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique,



Annelies Verlinden