DOC 54 **3340/003**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

12 maart 2019

WETSONTWERP

tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

VERSLAG

NAMENS DE COMMISSIE VOOR DE BINNENLANDSE ZAKEN, DE ALGEMENE ZAKEN EN HET OPENBAAR AMBT UITGEBRACHT DOOR DE HEREN **Franky DEMON** EN **Eric THIÉBAUT**

INHOUD Blz.

I. Inleidende uiteenzetting 3
II. Algemene bespreking.....8
III. Artikelsgewijze bespreking en stemmingen 22

Zie:

Doc 54 **3340/ (2018/2019):**
001: Wetsontwerp.
002: Amendementen.

Zie ook:
004: Tekst aangenomen door de commissie.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

12 mars 2019

PROJET DE LOI

établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

RAPPORT

FAIT AU NOM DE LA COMMISSION DE L'INTÉRIEUR, DES AFFAIRES GÉNÉRALES ET DE LA FONCTION PUBLIQUE PAR MM. **Franky DEMON** ET **Eric THIÉBAUT**

SOMMAIRE Pages

I. Exposé introductif 3
II. Discussion générale.....8
III. Discussion des articles et votes.....22

Voir:

Doc 54 **3340/ (2018/2019):**
001: Projet de loi.
002: Amendements.

Voir aussi:
004: Texte adopté par la commission.

Samenstelling van de commissie op de datum van indiening van het verslag/
Composition de la commission à la date de dépôt du rapport
Voorzitter/Président: Brecht Vermeulen

A. — Vaste leden / Titulaires:		**B. — Plaatsvervangers / Suppléants:**
N-VA	Christoph D'Haese, Koenraad Degroote, Koen Metsu, Brecht Vermeulen	Peter Buysrogge, Sarah Smeyers, Valerie Van Peel, Jan Vercammen, Bert Wollants
PS	Nawal Ben Hamou, Julie Fernandez Fernandez, Eric Thiébaut	Laurent Devin, André Frédéric, Emir Kir, Laurette Onkelinx
MR	Sybille de Coster-Bauchau, Philippe Pivin, Françoise Schepmans	Emmanuel Burton, Gautier Calomne, Caroline Cassart-Mailleux, Stéphanie Thoron
CD&V	Franky Demon, Veerle Heeren	Leen Dierick, Nahima Lanjri
Open Vld	Sandrine De Crom, Katja Gabriëls	Patrick Dewael, Vincent Van Quickenborne, Frank Wilrycx
sp.a	Monica De Coninck	Hans Bonte, Alain Top
Ecolo-Groen	Gilles Vanden Burre	Wouter De Vriendt, Stefaan Van Hecke
cdH	Vanessa Matz	Christian Brotcorne, Anne-Catherine Goffinet
ONAFH		Veli Yüksel

C. — Niet-stemgerechtigde leden / Membres sans voix délibérative:

VB	Filip Dewinter
DéFI	Olivier Maingain
PP	Aldo Carcaci

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
DéFI	:	*Démocrate Fédéraliste Indépendant*
PP	:	*Parti Populaire*
Vuye&Wouters	:	*Vuye&Wouters*

Afkortingen bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*	*DOC 54 0000/000:*	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Schriftelijke Vragen en Antwoorden*	*QRVA:*	*Questions et Réponses écrites*
CRIV:	*Voorlopige versie van het Integraal Verslag*	*CRIV:*	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Beknopt Verslag*	*CRABV:*	*Compte Rendu Analytique*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*	*CRIV:*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Plenum*	*PLEN:*	*Séance plénière*
COM:	*Commissievergadering*	*COM:*	*Réunion de commission*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT:*	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp besproken tijdens haar vergaderingen van 13 en 27 februari 2019.

I. — **INLEIDENDE UITEENZETTING**

De heer Pieter De Crem, minister van Veiligheid en Binnenlandse Zaken, geeft aan dat het wetsontwerp strekt tot omzetting van Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, de zogeheten "NIS-richtlijn".

Netwerk- en informatiesystemen spelen een cruciale rol in onze moderne samenleving. Een groot deel van de entiteiten verlenen essentiële diensten voor het behoud van kritieke maatschappelijke of economische activiteiten in België (bijvoorbeeld inzake transport, energievoorziening of gezondheidszorg) en zijn dus afhankelijk van de goede werking van hun netwerk- en informatiesystemen.

De omvang, de frequentie en de gevolgen van incidenten die de netwerk- en informatiesystemen aantasten, nemen almaar toe en vormen een grote bedreiging voor de goede werking van die essentiële diensten. De informatiesystemen kunnen met name een doelwit worden van opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbreken. Hetzelfde geldt voor bepaalde digitale diensten die de levering van diezelfde essentiële diensten kunnen verstoren.

De bescherming, de beveiliging en de betrouwbaarheid van de netwerken en van de informatiesystemen van aanbieders van essentiële diensten en van sommige digitale dienstverleners zijn voortaan van algemeen belang voor de bescherming van de bevolking, van de instellingen en van de ondernemingen van ons land. Bijgevolg zijn de beveiligingsvoorschriften inzake hun netwerk- en informatiesystemen zeer belangrijk voor de openbare veiligheid. Dit wetsontwerp wil een antwoord bieden op deze uitdagingen.

Dit wetsontwerp werd ingediend op 12 november 2018 en de Kamer keurde de behandeling ervan bij hoogdringendheid goed op 14 november 2018.

Het wetsontwerp heeft een dringend karakter enerzijds door de vertraging die werd opgelopen bij de omzetting van de richtlijn en anderzijds door het belang van dit thema voor de samenleving.

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de ses réunions des 13 et 27 février 2019.

I. — **EXPOSÉ INTRODUCTIF**

M. Pieter De Crem, ministre de la Sécurité et de l'Intérieur, explique que le projet de loi vise à transposer la Directive européenne 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'informations dans l'Union, dénommée la "Directive NIS".

Les réseaux et systèmes d'information jouent un rôle crucial dans nos sociétés modernes. Une grande partie des entités fournissent des services essentiels au maintien d'activités sociétales ou économiques critiques en Belgique (par exemple, dans le domaine du transport, de la distribution d'énergie ou des soins de santé) et sont donc tributaires du bon fonctionnement de leurs réseaux et systèmes d'information.

L'ampleur, la fréquence et l'impact des incidents affectant les réseaux et les systèmes d'information ne cessent de croître et représentent une menace considérable pour le bon fonctionnement de ces services essentiels. Les systèmes d'information peuvent notamment devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement. Il en va de même de certains services numériques qui sont susceptibles de perturber la fourniture de ces mêmes services essentiels.

La protection, la sécurisation et la fiabilité des réseaux et systèmes d'information des opérateurs fournissant des services essentiels et de certains fournisseurs de services numériques relèvent désormais de l'intérêt général lié à la protection de la population, des institutions et des entreprises de notre pays. Par conséquent, les règles de sécurité applicables à leurs réseaux et à leurs systèmes d'information sont importantes pour la sécurité publique. L'objectif du projet de loi à l'examen est de relever ces défis.

Le projet de loi à l'examen a été déposé le 12 novembre 2018 et la Chambre a accepté l'examen en urgence de celui-ci le 14 novembre 2018.

Le projet de loi revêt en effet un caractère urgent en raison, d'une part, du retard accusé dans la transposition de la directive, et, d'autre part, de l'importance de ce thème pour la société.

Het wetsontwerp hangt tevens samen met het wetsontwerp tot wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het federaal agentschap voor nucleaire controle betreffende de nucleaire cyberbeveiliging (DOC 54 3336/001).

De heer Miguel De Bruycker, managing director van het Centre for Cybersecurity Belgium (CCB), gaat nader in op een aantal technische aspecten van het wetsontwerp.

Wat de bevoegdheid betreft, behoort de omzetting van de bepalingen van de richtlijn in Belgisch recht tot de restbevoegdheid van de federale wetgever inzake bescherming van de openbare veiligheid.

De wet bepaalt echter dat de deelstaten zullen worden geraadpleegd tijdens de fase waarin de aanbieders van essentiële diensten (publieke of private personen) of de digitaledienstverleners worden aangeduid wanneer zij bij hun activiteiten onderworpen zijn aan gewestelijke of gemeenschapsregels.

De richtlijn beoogt te bewerkstelligen dat technische en organisatorische beveiligingsmaatregelen worden genomen om incidenten te voorkomen, dan wel de impact ervan te beperken, teneinde de goede werking van de essentiële diensten te waarborgen.

Tevens moet een verplichting worden ingevoerd voor het melden van incidenten die een aanzienlijke impact hebben op de netwerken en de informatiesystemen waarvan een aantal essentiële diensten afhankelijk zijn. Daartoe wil het wetsontwerp een aanpak voor het beheer van beveiligingsrisico's bevorderen die aansluit bij de bepalingen inzake de bescherming van persoonsgegevens, waaronder de Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (gewoonlijk "AVG" genoemd).

Artikel 5 preciseert dat de wet, onder voorbehoud van de afwijkingsbepalingen in titel 6 van het wetsontwerp, geen afbreuk doet aan de toepassing van de AVG, noch aan de wetten en reglementen die deze Verordening aanvullen of verduidelijken. Voorts wordt eraan herinnerd dat de bepalingen van het ter bespreking voorliggende wetsontwerp rekening houden met andere vigerende wettelijke bepalingen, meer bepaald:

— de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren in werking;

Le projet de loi à l'examen est par ailleurs lié au projet de loi portant 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 concernant la cybersécurité nucléaire (DOC 54 3336/001).

M. Miguel de Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB), approfondit certains aspects techniques du projet de loi.

En ce qui concerne la compétence, la transposition des dispositions de la directive en droit belge relève des compétences résiduelles du législateur fédéral en matière de protection de la sécurité publique.

La loi prévoit toutefois une consultation des entités fédérées au cours de la phase de désignation des opérateurs de services essentiels (personnes publiques ou privées) ou des fournisseurs de services numériques au cas où ils seraient soumis, pour leurs activités, à des règles régionales ou communautaires.

L'objectif de la directive est d'assurer la prise de mesures de sécurité techniques et organisationnelles pour prévenir les incidents ou en limiter l'impact, en vue d'assurer le bon fonctionnement des services essentiels.

Il y a lieu également d'instaurer une obligation de notification des incidents qui ont un impact considérable sur les réseaux et sur les systèmes d'information dont dépendent un certain nombre de services essentiels. À cette fin, le projet de loi à l'examen entend promouvoir une approche de la gestion des risques de sécurité qui soit en harmonie avec les dispositions en matière de protection des données à caractère personnel, dont le Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (communément appelé "RGPD").

L'article 5 précise que, sous réserve des dispositions dérogatoires reprises au titre 6 du projet, la loi ne porte pas préjudice à l'application du RGPD ainsi qu'aux lois et règlements qui le complètent ou le précisent. Il est aussi rappelé que les dispositions prévues dans le projet à l'examen tiennent compte d'autres dispositions légales en vigueur, notamment:

— la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques;

— de regels die van toepassing zijn op de verwerking van geclassificeerde informatie als bedoeld in de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

— de regels die van toepassing zijn op de nucleaire documenten als bedoeld in 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.

De identificatie van de aanbieders van essentiële diensten (AED) gebeurt door de sectorale overheid, in overleg met het Centrum voor Cybersecurity België en de Algemene Directie Crisiscentrum van de FOD Binnenlandse Zaken, binnen de grenzen van hun respectieve bevoegdheden (na raadpleging van de gewesten, de gemeenschappen en de sectorvertegenwoordigers).

Artikel 18 voorziet in de instelling van een vereenvoudigd systeem voor de aanwijzing van de exploitanten van infrastructuren die al als kritiek zijn aangewezen met toepassing van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

De operatoren die één of meer infrastructuren beheren die met toepassing van de wet van 1 juli 2011 als kritiek zijn aangewezen, zullen als AED worden aangewezen voor zover de geleverde dienst afhankelijk is van de netwerk- en informatiesystemen en de betrokken sector binnen het toepassingsgebied van de NIS-richtlijn valt.

Artikel 20 voorziet in de algemene verplichting voor de aanbieder van essentiële diensten om passende en evenredige technische en organisatorische maatregelen te nemen ter beveiliging van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Die maatregelen moeten een beveiligingsniveau waarborgen dat afgestemd is op de risico's, rekening houdend met de stand van de kennis ter zake, teneinde de continuïteit van de diensten te waarborgen.

Artikel 21 bepaalt dat de doelstellingen en maatregelen worden opgenomen in een document, genaamd "beveiligingsbeleid voor de netwerk- en informatiesystemen" (IBB).

De Koning kan de aanbieders van essentiële diensten van één of meer sectoren eventueel bepaalde beveiligingsmaatregelen opleggen.

— les règles applicables au traitement des informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité;

— les règles applicables aux documents 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 de Contrôle nucléaire.

L'identification des opérateurs de services essentiels (OSE) se fera par l'autorité sectorielle, en concertation avec le Centre pour la Cybersécurité Belgique et la Direction Générale Centre de crise du SPF Intérieur, dans les limites de leurs compétences respectives (après la consultation des Régions et des Communautés et des représentants du secteur).

L'article 18 instaure un système de désignation simplifié pour les exploitants d'infrastructures critiques déjà désignées comme telles en application de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Les opérateurs qui gèrent une ou plusieurs infrastructures désignée(s) comme infrastructures critiques, au sens de la loi du 1er juillet 2011, seront désignés comme OSE pour autant que le service fourni soit tributaire des réseaux et systèmes d'information et que le secteur concerné entre dans le champ d'application de la directive NIS.

L'article 20 prévoit l'obligation générale pour l'opérateur de services essentiels de prendre les mesures techniques et organisationnelles nécessaires et proportionnées de sécurité des réseaux et des systèmes d'information dont sont tributaires les services essentiels qu'il fournit. Ces mesures doivent garantir un niveau de sécurité adapté aux risques, compte tenu des connaissances en la matière, dans une perspective de continuité des services.

L'article 21 prévoit que les objectifs et les mesures soient repris sous forme d'un document dénommé politique de sécurité des systèmes et réseaux d'information (P.S.I.).

Le Roi peut éventuellement imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels d'un ou plusieurs secteurs.

De bedoeling is, in voorkomend geval, bepaalde minimale en specifieke beveiligingsmaatregelen op te leggen aan de aanbieders van essentiële diensten van verschillende sectoren.

De sectorale overheid kan, eveneens bij individuele administratieve beslissing, bijkomende beveiligingsmaatregelen opleggen aan een particuliere aanbieder.

Wanneer de aanbieder van essentiële diensten een beroep doet op een onderaannemer, moet hij zich ervan vergewissen dat deze de beveiligingsmaatregelen waartoe hij krachtens deze wet gehouden is, daadwerkelijk toepast.

Om de tenuitvoerlegging van de algemene beveiligingsverplichting te vergemakkelijken, bepaalt artikel 22 dat de aanbieders die erkende technische normen hanteren (bijvoorbeeld de internationale technische norm ISO/IEC 27001), het vermoeden genieten dat de inhoud van hun IBB conform is wanneer is voldaan aan de vereisten van deze norm, dan wel aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend.

Het vermoeden van conformiteit heeft louter betrekking op de inhoud van het IBB, met andere woorden op de doelstellingen inzake beveiligingsbeheer die dat document moet bevatten, niet op het afdoende karakter van de toegepaste beveiligingsmaatregelen.

De beveiligingsmaatregelen kunnen immers door de Koning of door de sectorale overheid worden aangevuld. Ze moeten worden gecontroleerd door een externe auditeur of door de inspectiedienst van de sectorale overheid.

Artikel 24, § 1, strekt tot verankering van de verplichting voor de aanbieders van essentiële diensten om incidenten met ingrijpende gevolgen te melden aan de bevoegde autoriteiten, met name het nationale CSIRT (CCB), de sectorale overheid of haar sectorale CSIRT, en aan de ADCC.

Of de gevolgen van een incident al dan niet ingrijpend zijn, moet worden beoordeeld in het licht van de beschikbaarheid, de vertrouwelijkheid, de integriteit of de authenticiteit van de informatiesystemen waarvan de door de aanbieder verleende essentiële diensten afhankelijk zijn.

De digitaledienstverleners (DDV) zullen worden verzocht soortgelijke maatregelen te nemen inzake de beveiliging en de melding van incidenten, met dien verstande dat deze maatregelen minder streng mogen zijn en dat ze op Europees niveau worden geharmoniseerd

L'objectif est de rendre obligatoire, le cas échéant, certaines mesures minimales et précises de sécurité pour les opérateurs de services essentiels de différents secteurs.

L'autorité sectorielle peut, également par décision administrative individuelle, imposer des mesures complémentaires de sécurité à un opérateur particulier.

Lorsqu'il fait appel à un sous-traitant, l'opérateur de services essentiels doit s'assurer que son sous-traitant applique de manière effective les mesures de sécurité imposées en vertu de la présente loi.

Afin de faciliter la mise en œuvre de l'obligation générale de sécurité, l'article 22 énonce que les opérateurs utilisant des normes standards techniques reconnues, comme la norme ISO/IEC 27001 (norme technique internationale), pourront bénéficier d'une présomption de conformité du contenu de leur P.S.I. lorsque celle-ci répond aux exigences de cette norme – ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi.

La présomption porte uniquement sur le contenu de la P.S.I., c'est-à-dire sur les objectifs de gestion de la sécurité qui doivent figurer dans ce document, et non sur le caractère suffisant des mesures de sécurité appliquées.

En effet, les mesures de sécurité peuvent être complétées par le Roi ou l'autorité sectorielle. Elles devront faire l'objet d'un contrôle par un auditeur externe ou par le service d'inspection de l'autorité sectorielle.

L'article 24, paragraphe 1er, consacre l'obligation pour les OSE de notifier les incidents ayant un impact significatif aux autorités compétentes CSIRT national (CCB), à l'autorité sectorielle ou son CSIRT sectoriel et à la DGCC.

Le caractère significatif de l'impact d'un incident sera évalué au regard de son effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires les services essentiels fournis par l'opérateur.

Des mesures de sécurité et de notification des incidents similaires seront demandées aux fournisseurs de service numérique (FSN), à la différence que les mesures peuvent être moins exigeantes et sont harmonisées au niveau européen, conformément à la directive

overeenkomstig de NIS-richtlijn en de uitvoeringsverordening van de Europese Commissie van 30 januari 2018 (EU) 2018/151.

Voor de controle van de aanbieders van essentiële diensten beoogt het wetsontwerp te voorzien in drie niveaus:

— de controle die te allen tijde door de sectorale inspectiediensten kan worden uitgevoerd;

— een interne audit (jaarlijks);

— een externe audit (om de drie jaar), uit te voeren door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door BELAC (de door de Koning aangewezen instelling voor de accreditatie van de instellingen voor de conformiteitsbeoordeling in België), dan wel door een door de sectorale overheid erkende organisatie.

De inschakeling van geaccrediteerde of door de sectorale overheid erkende externe auditinstellingen waarborgt een hoog gemeenschappelijk expertiseniveau in de verschillende sectoren bij de uitvoering van de regelmatige controles van de aanbieders. Deze regeling ondersteunt tevens de inspectiediensten bij de uitvoering van hun controleopdrachten en maakt het mogelijk de noodzakelijke budgettaire kosten voor de goede werking van voormelde diensten binnen de perken te houden (de externe audits vallen immers ten laste van de aanbieders).

Gezien de snelle evolutie van de informatie- en communicatietechnologie voorzien de bepalingen van dit wetsontwerp in de verplichting voor aanbieders van essentiële diensten om regelmatig audits uit te voeren. Daarnaast kunnen de inspectiediensten op elk ogenblik controles uitvoeren. De sectorale overheden kunnen inbreuken op de wetsbepalingen bestraffen met strafrechtelijke of administratieve sancties (die worden bepaald op grond van de ernst, de omstandigheden, de situaties van herhaling of van samenloop van inbreuken).

Tot op heden beschikte ons land niet over een volledig wetgevingsarsenaal inzake de beveiliging van netwerken informatiesystemen. Enkel de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren voorzag in een gedeeltelijke verplichting om beveiligingsmaatregelen te nemen voor zogenaamde “kritieke infrastructuren”, waaronder de netwerk- en informatiesystemen. Bijgevolg heeft dit wetsontwerp tot doel deze leemte op te vullen, in een domein dat steeds strategischer en gevoeliger wordt voor onze openbare veiligheid.

NIS et au règlement d’exécution de la Commission européenne du 30 janvier 2018 (UE) 2018/151.

Le projet de loi prévoit trois niveaux de contrôle des OSE:

— le contrôle à tout moment par des services d’inspection sectoriels;

— un audit interne (chaque année);

— un audit externe (tous les 3 ans) par un organisme d’évaluation de la conformité accrédité par BELAC (qui est l’organisme d’accréditation désigné par le Roi pour accréditer en Belgique des organismes d’évaluation de la conformité) ou une organisation agréée par l’autorité sectorielle.

Le recours à des organismes d’audit externe accrédités ou agréés par l’autorité sectorielle assure un niveau commun et élevé d’expertise entre les différents secteurs pour réaliser les contrôles réguliers des opérateurs. Ce mécanisme permettra également d’aider les services d’inspection dans leur mission de contrôle et de maîtriser les coûts budgétaires nécessaires (les audits externes étant à charge des opérateurs) au bon fonctionnement des services précités.

Vu l’évolution rapide des technologies de l’information et de la communication, les dispositions du projet de loi à l’examen obligent les opérateurs de services essentiels à procéder régulièrement à des audits. Par ailleurs, les services d’inspection peuvent effectuer des contrôles à tout moment. Les autorités sectorielles peuvent sanctionner les infractions aux dispositions légales par le biais de sanctions pénales ou administratives (déterminées en fonction de la gravité, des circonstances et des éventuels cas de récidive ou de concours d’infractions).

Notre pays ne s’était jusqu’à présent pas doté d’un arsenal législatif complet sur la sécurité des réseaux et des systèmes d’information. Seule la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques prévoyait une obligation partielle de prendre des mesures de sécurité pour les infrastructures dites “critiques”, dont les réseaux et les systèmes d’information. Le projet de loi à l’examen vise donc à combler cette lacune, dans un domaine qui devient sans cesse plus stratégique et plus critique pour notre sécurité publique.

Tot slot verduidelijkt het wetsontwerp ook de bevoegdheden en de opdrachten van de bevoegde administratieve autoriteiten inzake de beveiliging van de netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Deze zullen door de Koning worden aangewezen (nationale autoriteit, nationaal CSIRT, sectorale overheden, sectorale CSIRT's, inspectiediensten, enzovoort).

II. — **ALGEMENE BESPREKING**

A. **Vragen en opmerkingen van de leden**

De heer Brecht Vermeulen (N-VA) stipt aan dat het thema van de cyberveiligheid hem nauw aan het hart ligt. Over de omzetting van de NIS-richtlijn heeft hij de eerste minister eerder meermaals bevraagd. Een eerste mondelinge vraag hierover werd beantwoord op 4 oktober 2016 (CRIV 54 COM 500, blz. 33). Dat is drie maanden nadat de Europese richtlijn over de netwerk- en informatieveiligheid werd aangenomen. De laatste vraag van zijn hand aan de eerste minister dateert van de bespreking van de beleidsbrief voor 2019. In het antwoord werd de nakende bespreking van het wetsontwerp in verband met de omzetting aangekondigd (DOC 54 3294/011, blz. 25).

In het antwoord van oktober 2016 meldde de eerste minister dat "de NIS-richtlijn voorziet in een vrij lange omzettingstermijn van 22 maanden, tot 10 mei 2018, en een bijkomende termijn van zes maanden voor de identificatie van aanbieders van essentiële diensten" (CRIV 54 COM 500, blz. 34). Ondanks het feit dat de eerste minister toen van mening was dat de omzettingstermijn vrij lang was, moet de spreker thans vaststellen dat België – samen met Luxemburg – het enige Europese land is dat niet op tijd klaar is met deze omzetting. Alle andere landen hebben voor de uiterste datum van de omzetting de wetgeving wel uitgevoerd. Inmiddels werd België door de Europese Commissie in gebreke gesteld voor de niet-tijdige omzetting van de NIS-richtlijn. Kan verklaard worden waarom de omzetting zo laat gebeurde?

In de algemene toelichting staat te lezen dat de deelstaten geraadpleegd zullen worden als AED's of digitale dienstverleners voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsmaatregelen. Deze raadpleging is facultatief en gebeurt op een zodanige wijze dat, indien de deelgebieden verzuimen om mee te werken, dit niet verhindert dat de federale overheid de voorgenomen maatregelen kan nemen.

Enfin, le projet de loi précise les compétences et les missions des autorités administratives compétentes en ce qui concerne la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Ces autorités seront désignées par le Roi (autorité nationale, CSIRT national, CSIRT sectoriels, services d'inspection, etc.).

II. — **DISCUSSION GÉNÉRALE**

A. **Questions et observations des membres**

M. Brecht Vermeulen (N-VA) souligne que la cybersécurité est un thème qui lui tient à cœur et qu'il a déjà interrogé le premier ministre à plusieurs reprises à propos de la transposition de la directive NIS. Il a notamment répondu à une première question orale le 4 octobre 2016 (*cf.* CRIV 54 COM 500, p. 33), soit trois mois après l'adoption de la directive européenne sur la sécurité des réseaux et des systèmes d'information. La dernière question à ce sujet adressée par l'intervenant au premier ministre date de la discussion portant sur la note de politique générale pour l'année 2019. Dans sa réponse, le premier ministre avait évoqué l'imminence de l'examen du projet de loi relatif à la transposition de la directive (DOC 54 3294/011, p. 25).

Dans la réponse qu'il a communiquée en octobre 2016, le premier ministre a indiqué que la directive NIS prévoyait un délai de transposition relativement long de 22 mois, expirant le 10 mai 2018, et un délai supplémentaire de six mois pour l'identification de fournisseurs de services essentiels (CRIV 54 COM 500, p. 34). Bien que le premier ministre ait estimé à l'époque que le délai de transposition était assez long, l'orateur doit maintenant constater que la Belgique – avec le Luxembourg – est le seul pays européen qui n'a pas achevé cette transposition à temps. Tous les autres pays ont mis en œuvre la législation avant la date limite de transposition. Dans l'intervalle, la Belgique a été mise en demeure par la Commission européenne pour n'avoir pas transposé la directive NIS à temps. Peut-on expliquer pourquoi la transposition a été si tardive?

L'exposé général indique qu'il est prévu de consulter, de manière facultative et en manière telle que leur éventuelle abstention de collaborer n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale, les entités fédérées lorsque certains opérateurs de services essentiels ou fournisseurs de services numériques seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires.

Is er voorafgaand aan het wetsontwerp contact geweest met de gewesten en gemeenschappen over de voorliggende tekst? Zo ja, wanneer en via welke weg is dat gebeurd? Hebben zij een advies kunnen verlenen?

De bijlagen 1 en 2 van het wetsontwerp bevatten tabellen over enerzijds de sectoren en soorten entiteiten van AED's en anderzijds de soorten digitale dienstverleners (DOC 54 3340/001, blz. 194 en 200). De eerste minister stelde in zijn antwoord op 4 oktober 2016 dat de uitdrukkelijk beoogde sectoren energie, transport, financiën en telecommunicatie zijn" (CRIV 54 COM 500, blz. 34). Uiteindelijk werden zes sectoren opgenomen in de tabel die de AED definieert, met name energie, vervoer, financiën, gezondheidszorg, drinkwater en de digitale infrastructuren.

In vergelijking met het antwoord van de eerste minister blijkt dat de telecommunicatiesector niet mee opgenomen is in de definitieve lijst. Kan dit verschil verklaard worden? Valt de sector van de telecommunicatie geheel of ten dele onder de digitale infrastructuren? Indien het gedeeltelijk is, wat valt er dan niet onder? Hoe is de lijst van AED's tot stand gekomen? Welke actoren zijn hiervoor geraadpleegd?

Het komt de sectorale overheden toe om de AED's te identificeren. Ze moeten minstens rekening houden met de gegevens die in de bijlage 1 zijn beschreven. Hoe zal gewaakt worden over de uniformiteit in de keuzes van deze sectorale overheden? Zijn hiervoor gemeenschappelijke criteria of richtsnoeren opgesteld? Hoeveel potentiële AED's zijn momenteel reeds geïdentificeerd en in welke sectoren zijn deze actief? Wensen sommige bedrijven te weerleggen dat ze een AED zijn? Zijn bij de potentiële AED's ook entiteiten die niet geïdentificeerd zijn in tabel 1?

Zal deze wetgeving tevens een impact hebben op de toeleveranciers van bedrijven die als AED worden geïdentificeerd? Zullen hierover afspraken worden gemaakt met de (potentiële) AED's?

In de toelichting bij artikel 6 staat te lezen dat wordt overwogen om een nationaal comité voor de beveiliging van netwerk- en informatiesystemen voor de levering en distributie van drinkwater op te richten (DOC 54 3340/001, blz. 12). Dit zou zijn samengesteld uit vertegenwoordigers van de Federale Staat en de drie gewesten. Welke elementen zullen doorslaggevend zijn bij de beslissing of dit nationaal comité wordt opgericht? Zijn er, naast drinkwater, nog andere sectoren of subsectoren waarvoor een dergelijk overlegplatform nuttig zou zijn?

Le texte à l'examen a-t-il donné lieu à des contacts avec les Régions et les Communautés préalablement au projet de loi? Dans l'affirmative, quand ont-ils eu lieu et par quel biais? Les Régions et Communautés ont-elles pu rendre un avis?

Les annexes 1 et 2 du projet de loi contiennent des tableaux représentant, d'une part, les secteurs et les types d'entités des OSE et, d'autre part, les types de services numériques (DOC 54 3340/001, p. 197 et 200). Dans sa réponse du 4 octobre 2016, le premier ministre a cité comme secteurs clés l'énergie, les transports, les finances et les télécommunications (CRIV 54 COM 500, p. 34). Au final, six secteurs ont été retenus dans le tableau qui définit les OSE, à savoir l'énergie, les transports, les finances, la santé, l'eau potable et les infrastructures numériques.

Par rapport à la réponse du premier ministre, le secteur des télécommunications ne figure manifestement pas dans la liste finale. Cette différence peut-elle s'expliquer? Le secteur des télécommunications relève-t-il totalement ou partiellement des infrastructures numériques? Si c'est partiellement, qu'est-ce qui en est exclu? Comment est née la liste des OSE? Quels acteurs ont été consultés à cette fin?

Il appartient aux autorités sectorielles d'identifier les OSE. Elles doivent au moins tenir compte des données reprises à l'annexe 1. Comment l'uniformité dans les choix de ces autorités sectorielles sera-t-elle assurée? Des critères ou lignes directrices communs ont-ils été élaborés à cette fin? Combien de OSE potentiels ont-ils déjà été identifiés et dans quels secteurs sont-ils actifs? Certaines entreprises souhaitent-elles réfuter le fait qu'elles sont des OSE? Parmi les OSE potentiels, y a-t-il aussi des entités qui ne sont pas identifiées dans le tableau 1?

Cette législation aura-t-elle également un impact sur les fournisseurs des entreprises identifiées comme OSE? Des accords seront-ils conclus à ce sujet avec les OSE (potentiels)?

Le commentaire de l'article 6 indique qu'il est envisagé de créer un comité national pour la sécurité des réseaux et des systèmes d'information pour l'approvisionnement et la distribution d'eau potable (DOC 54 3340/001, p. 12). Celui-ci serait composé de représentants de l'État fédéral et des trois régions. Quels éléments seront déterminants pour décider de la mise en place de ce comité national? Outre l'eau potable, existe-t-il d'autres secteurs ou sous-secteurs pour lesquels une telle plate-forme de concertation serait utile?

Artikel 29 van het wetsontwerp stelt dat de nationale CSIRT incidenten moeten melden aan de andere lidstaten van de Europese Unie wanneer die aanzienlijke gevolgen hebben voor de continuïteit van essentiële diensten in die lidstaten. Vermits de andere Europese landen hun omzetting 9 maanden geleden voltooid hebben, informeert de heer Vermeulen of het CCB al weet heeft van incidenten in andere lidstaten. Zo ja, zijn deze incidenten rechtstreeks gemeld aan het CCB of via het "CSIRTS network" van ENISA (*EU agency for network and information security*)? Over hoeveel meldingen gaat het, uit welke lidstaten waren deze afkomstig en uit welke sectoren kwamen deze meldingen?

Voorts vraagt de spreker hoeveel Belgische bedrijven digitale dienstverleners zijn? In welke sectoren zijn deze bedrijven actief? Op welke wijze worden de betrokken bedrijven geïnformeerd over hun nieuwe verplichtingen? Zijn er maatregelen getroffen om deze bedrijven bij te staan voor deze (bijkomende) verplichtingen? Hoe wordt bepaald welke veiligheidsincidenten een voldoende "grote impact" hebben, waardoor deze aan het CCB, de sectorale overheid of haar sectorale CSIRT (*Computer Security Incident Response Team*) en het Crisiscentrum moeten worden meegedeeld?

De heer Eric Thiébaut (PS) merkt op dat artikel 21 van het wetsontwerp de Koning machtigt bepaalde beveiligingsmaatregelen op te leggen aan de aanbieders van essentiële diensten van verschillende sectoren. Bedoeling is, in voorkomend geval, bepaalde minimale en specifieke beveiligingsmaatregelen verplicht te maken voor de aanbieders van essentiële diensten van verschillende sectoren (cf. DOC 54 3340/001, blz. 21). Kan de minister verduidelijken welke maatregelen aldus zullen kunnen worden opgelegd en welke maatregelen facultatief zullen blijven?

Mevrouw Sybille de Coster-Bauchau (MR) benadrukt het belang van het wetsontwerp, dat een gemeenschappelijke aanpak beoogt inzake de beveiligingsmaatregelen die de verschillende aanbieders zullen toepassen.

De omzetting van de NIS-richtlijn komt inderdaad laat, maar gezien de hoge inzet voor de aanbieders, die nieuwe beveiligingsverplichtingen opgelegd krijgen, was het belangrijk de nodige tijd te nemen, om aldus te waarborgen dat de tekst zo adequaat mogelijk is.

Gezien de technische aard van het wetsontwerp beperkt de spreekster zich tot enkele algemene vragen.

L'article 29 du projet de loi stipule que le CSIRT national doit signaler les incidents aux autres États membres de l'Union européenne lorsque ces incidents ont un impact significatif sur la continuité des services essentiels dans ces États membres. Les autres pays européens ayant achevé leur transposition il y a neuf mois, M. Vermeulen a demandé si le CCB était déjà au courant d'incidents dans d'autres États membres. Dans l'affirmative, ces incidents ont-ils été signalés directement au CCB ou via le réseau CSIRTS de l'ENISA (Agence européenne pour la sécurité des réseaux et de l'information)? Combien de rapports sont concernés, de quels États membres et de quels secteurs proviennent-ils?

L'orateur demande également combien d'entreprises belges sont des fournisseurs de services numériques? Dans quels secteurs ces entreprises sont-elles actives? Comment les entreprises concernées sont-elles informées de leurs nouvelles obligations? Des mesures ont-elles été prises pour aider ces entreprises à remplir ces obligations (supplémentaires)? Comment détermine-t-on quels incidents de sécurité ont un "impact suffisamment important" pour être communiqués au CCB, à l'autorité sectorielle ou à son CSIRT (*Computer Security Incident Response Team*) sectoriel et au Centre de crise?

M. Eric Thiébaut (PS) constate que l'article 21 du projet de loi habilite le Roi à imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels de plusieurs secteurs. L'objectif est de rendre obligatoires, le cas échéant, certaines mesures minimales et précises de sécurité pour les opérateurs de services essentiels de plusieurs secteurs (cf. DOC 54 3340/1, p. 21). Le ministre peut-il préciser quelles mesures pourront de la sorte être rendues obligatoires et quelles sont celles qui resteront facultatives?

Mme Sybille de Coster-Bauchau (MR) souligne l'importance du projet de loi qui tend à mettre en œuvre une approche commune des mesures de sécurité qui seront appliquées par les différents opérateurs.

Il est exact que la transposition de la directive NIS intervient tardivement mais compte tenu des enjeux pour les opérateurs auxquels on impose de nouvelles obligations de sécurité, il était important de prendre le temps nécessaire pour garantir que le texte soit les plus adéquat possible.

Vu la technicité du projet de loi, l'intervenante se limitera à quelques questions générales.

De eerste vraag betreft de begrippen “aanbieders van essentiële diensten” en “kritieke infrastructuren”. Wat zijn de verschillen tussen die twee begrippen? Kan een aanbieder van essentiële diensten tegelijkertijd een kritieke infrastructuur zijn en omgekeerd?

Zal na de goedkeuring van dit wetsontwerp een nieuwe nationale strategie worden aangenomen?

Hoe zullen de digitaledienstverleners worden aangewezen?

De spreekster wenst ook te worden geïnformeerd over de maatregelen die met betrekking tot de nucleaire sector zullen worden genomen.

Wat is de rol van de deelstaten bij deze omzetting?

Welke koninklijke besluiten zullen tot slot moeten worden uitgevaardigd na de inwerkingtreding van de wet?

De heer Franky Demon (CD&V) geeft aan dat de minister terecht heeft gewezen op de stijgende gevoeligheid van informatienetwerken in de intergeconnecteerde wereld. De daaraan verbonden veiligheidsrisico’s nemen steeds verder toe. Dat is in het bijzonder zo voor gevoelige sectoren waarvan de werking cruciaal is voor het algemeen belang of waarbij de verstoring van de werking bijzondere risico’s kunnen inhouden.

Een voorbeeld daarvan is de gezondheidssector. De gevolgen van *hacking* van het informatiesysteem van die sector, waarbij allerlei data worden gewijzigd, kunnen vreselijke gevolgen hebben voor patiënten van wie levensbelangrijke data zou worden gewijzigd door hackers (bijvoorbeeld de wijziging van de bloedgroep of van bepaalde toe te dienen medicatie).

Het voorliggende wetsontwerp wil een wettelijk kader aanbieden inzake het voorkomen van incidenten en het beperken van de impact ervan, om de continuïteit van deze essentiële diensten te waarborgen. Tevens zou worden voorzien in een meldingsplicht bij incidenten.

Voor welke sectoren gelden de verplichtingen? Naast de sectoren die zijn vervat in de bijlage van het wetsontwerp, zouden ook subsectoren kunnen worden aangeduid. Bestaat daarover reeds meer duidelijkheid?

Voor de driejaarlijkse externe audit moeten de aanbieders van essentiële diensten voor de conformiteitsbeoordeling een beroep doen op een instelling die geaccrediteerd is door de nationale accreditatieautoriteit, dan wel door een instelling die de erkenningsakkoorden van de “*European Cooperation for Accreditation*” mee

La première concerne les notions d’opérateurs de services essentiels et d’infrastructures critiques. Quelles sont les différences entre ces deux notions? Un opérateur de services essentiels peut-il être simultanément une infrastructure critique, et vice versa?

Une nouvelle stratégie nationale va-t-elle être adoptée après l’adoption de ce projet de loi?

Comment les fournisseurs de services numériques seront-ils désignés?

L’intervenante souhaite par ailleurs être informée des mesures qui seront prises en ce qui concerne le secteur nucléaire.

Quel est le rôle des entités fédérées dans le cadre de cette transposition?

Enfin, quels arrêtés royaux devront-être pris une fois que la loi sera en vigueur?

M. Franky Demon (CD&V) indique que le ministre a épinglé à juste titre la sensibilité croissante des réseaux d’information dans un monde interconnecté. Les risques qui en découlent en termes de sécurité ne cessent de s’accroître. C’est particulièrement vrai pour des secteurs sensibles dont le fonctionnement est crucial pour l’intérêt général et dont l’interruption du fonctionnement peut engendrer des risques particuliers.

On peut citer comme exemple le secteur des soins de santé. Dans ce secteur, le piratage des systèmes d’information, en modifiant toutes sortes de données, peut avoir des conséquences funestes pour les patients dont les données vitales seraient ainsi modifiées (par exemple une modification du groupe sanguin ou de certains médicaments à administrer).

Le projet à l’examen veut offrir un cadre légal, de manière à éviter les incidents et à limiter leur impact, et ce, afin de garantir la continuité de ces services essentiels. Il prévoirait également une obligation de signalement en cas d’incidents.

Quels sont les secteurs couverts par les obligations? Outre les secteurs prévus dans l’annexe au projet, des sous-secteurs pourraient également être identifiés. Y a-t-il déjà plus de clarté à ce sujet?

Pour l’audit externe triennal, les opérateurs de services essentiels doivent faire appel à un organisme d’évaluation de la conformité accrédité par l’autorité nationale d’accréditation ou par un organisme cosignataire des accords d’accréditation de la “*European Cooperation for Accreditation*”. Des organismes ont-ils

ondertekend heeft. Werden reeds instellingen aangeduid in dit verband? Zo niet, wanneer zal dat gebeuren? Welke kosten zijn daaraan verbonden voor de betrokken dienstenaanbieders?

In welke maatregelen is voorzien om op Europees vlak samen te werken, bijvoorbeeld rond de melding van dreigingen? Het betreft immers de omzetting van een Europese richtlijn, en bedreigingen hebben vaak een *cross-border*-karakter.

Mevrouw Katja Gabriëls (Open Vld) stipt aan dat België tot nog toe niet beschikte over wetgeving met betrekking tot de beveiliging van netwerken en informatiesystemen. De omzetting van de NIS-richtlijn is dus van aanzienlijk belang. Daarom is het jammer dat de deadline voor de omzetting niet is gehaald. Dat is des te meer het geval omdat de AVG-regelgeving inmiddels een jaar van kracht is. Een afstemming van de beide wetgeving zou zeer welkom zijn geweest, net als de zorg voor het inrichten van een uniek meldpunt voor zowel AVG- als NIS-incidenten.

Zullen bedrijven die leveren aan of klant zijn van een operator van een essentiële dienst of van een digitale dienstverlener in de praktijk toch op een indirecte manier met bepaalde beveiligingsverplichtingen rekening moeten houden, en dus de gevolgen ondervinden van het wetsontwerp?

Wanneer zullen de koninklijke besluiten klaar zijn? Wat is de stand van zaken daarvan? De uitvoeringsbesluiten zijn immers van bijzonder belang, want zij bieden rechtszekerheid aan de ondernemingen waarop het wetsontwerp van toepassing is.

B. **Antwoorden**

1. ***Antwoorden van de minister***

De minister overloopt de verschillende vragen die werden gesteld.

— Omzetting van de richtlijn

De richtlijn moest uiterlijk op 9 mei 2018 zijn omgezet.

De Europese Commissie heeft de uitvoeringshandeling van de richtlijn echter met enkele maanden vertraging genomen: deze moest uiterlijk op 9 augustus 2017 worden aangenomen, maar dat gebeurde uiteindelijk pas op 30 januari 2018. Bovendien werden de richtsnoeren van de Europese samenwerkingsgroep NIS pas in februari 2018 aangenomen en gepubliceerd. Sommige Europese landen beschikten in hun nationaal recht al over uitgebreide wetgeving die verplichtingen

déjà été désignés dans ce contexte? Sinon, quand cela interviendra-t-il? Quels sont les coûts supportés par les prestataires de services concernés?

Quelles mesures ont-elles été prévues pour favoriser la collaboration au niveau européen, par exemple en ce qui concerne le signalement des menaces? Il s'agit en effet de la transposition d'une directive européenne, et les menaces ont souvent un caractère transfrontalier.

Mme Katja Gabriëls (Open Vld) indique que, jusqu'à présent, la Belgique ne disposait pas encore d'une législation relative à la sécurité des réseaux et des systèmes d'information. La transposition de la directive NIS est donc particulièrement importante. Il est dès lors regrettable que le délai de transposition n'ait pas été respecté, d'autant que la réglementation RGPD est entre-temps en vigueur depuis un an. Une harmonisation des deux législations aurait vraiment été la bienvenue, de même que la création d'un point de contact unique pour les incidents RGPD, et NIS.

Dans la pratique, les entreprises qui sont fournisseurs ou clients d'un opérateur de services essentiels ou d'un fournisseur de services numériques devront-elles tout de même tenir compte, de manière indirecte, de certaines obligations de sécurité, et donc subir les effets du projet de loi?

Quand les arrêtés royaux seront-ils prêts? Quel est leur état d'avancement? Les arrêtés d'exécution sont en effet particulièrement importants, car ils garantissent la sécurité juridique aux entreprises concernées par le projet de loi.

B. **Réponses**

1. ***Réponses du ministre***

Le ministre passe en revue les différentes questions posées.

— Transposition de la directive

La directive devait être transposée pour le 9 mai 2018.

Cependant, l'acte d'exécution de la directive a été pris par la Commission européenne avec plusieurs mois de retard: celui devait être adopté pour le 9 août 2017 mais n'a finalement été adopté que le 30 janvier 2018. De même, les lignes directrices du Groupe de coopération européen NIS n'ont été adoptés et publiés qu'au mois de février 2018. Il faut préciser que certains États européens disposaient déjà dans leur droit national d'une législation complète imposant des obligations

inzake beveiliging van informatiesystemen oplegt aan de aanbieders van essentieel belang en die bepalingen bevat die in overeenstemming zijn met de richtlijn; in België was dat niet het geval.

Tot dusver beschikte ons land niet over een volledig wetgevingsarsenaal inzake de beveiliging van de netwerk- en informatiesystemen. Dit wetsontwerp heeft ook tot doel deze leemte op te vullen, in een domein waarvan het strategische belang almaar toeneemt. De regering heeft de tijd genomen om samen met de verschillende Belgische betrokken partijen (de verschillende bevoegde besturen) een specifiek wetsontwerp op te stellen, rekening houdend met de adviezen van de Raad van State en van de Gegevensbeschermingsautoriteit (die op dat moment volledig werd hervormd), tot omzetting van de uit de richtlijn voortvloeiende verplichtingen.

In november 2018 hadden acht landen vertraging opgelopen bij de omzetting van de NIS-richtlijn: Nederland, Luxemburg, Oostenrijk, Bulgarije, Griekenland, Letland, Roemenië en België. Thans moeten alleen nog België en Luxemburg hun omzettingsverklaring aan de Europese Commissie voorleggen.

— Deelstaten

In verband met de contacten met de gewesten en gemeenschappen deelt de minister mee dat de verplichtingen van de NIS-richtlijn betrekking hebben op het beveiligingsniveau van de netwerk- en informatiesystemen van entiteiten die diensten van algemeen belang verlenen voor de bevolking en het bedrijfsleven, of die van cruciaal belang zijn voor het economisch potentieel van het land.

In het Belgisch recht behoort de omzetting van de bepalingen ervan tot de restbevoegdheid van de federale wetgever met betrekking tot de bescherming op het gebied van de openbare veiligheid.

Naar analogie van de bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren bepaalt de wet niettemin dat de deelgebieden worden geraadpleegd bij het identificatieproces en het nemen van beveiligingsmaatregelen wanneer sommige aanbieders van essentiële diensten (publiekrechtelijke of privaatrechtelijke personen) of digitale dienstverleners voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsregels. Het wetsontwerp bepaalt dat de sectorale overheid de betrokken gewesten of gemeenten formeel zal raadplegen bij de identificatie van de aanbieders van essentiële diensten en het nemen van de verplichte beveiligingsmaatregelen.

en matière de sécurité des systèmes d'information aux opérateurs d'importance vitales et disposant de dispositions conformes à la directive, ce qui n'était pas le cas de la Belgique.

Notre pays ne s'était jusqu'à présent pas doté d'un arsenal législatif complet sur la sécurité des réseaux et des systèmes d'information. Le projet de loi vise aussi à combler cette lacune, dans un domaine qui devient de plus en plus stratégique. Le gouvernement a pris le temps d'élaborer un projet spécifique de loi avec les différents intervenants belges concernés (les différentes administrations compétentes), de prenant en compte les avis du Conseil d'État et de l'Autorité de protection des données (qui était en pleine transformation à la même période) qui transpose les obligations découlant de la directive.

Au mois de novembre 2018, il y avait 8 pays en retard de transposition de la directive NIS: les Pays-Bas, le Luxembourg, l'Autriche, la Bulgarie, la Grèce, la Lettonie, la Roumanie et la Belgique. Actuellement, il ne reste que la Belgique et le Luxembourg qui doivent encore faire leur déclaration de transposition à la Commission européenne.

— Entités fédérées

En ce qui concerne les contacts avec les Régions et Communautés, le ministre indique que les obligations de la directive NIS portent sur le niveau de sécurité des réseaux et des systèmes d'information des entités fournissant des services d'intérêt général pour la population et les entreprises, ou des services critiques pour le potentiel économique du pays.

Dans le droit belge, la transposition de ces dispositions ressortit à la compétence résiduelle du législateur fédéral en ce qui concerne la protection dans le domaine de la sécurité publique.

À l'instar des dispositions de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, la loi prévoit néanmoins de consulter les entités fédérées lors du processus d'identification et de la prise de mesures de sécurité lorsque certains opérateurs de services essentiels (personnes publiques ou privées) ou fournisseurs de services numériques seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires. Le projet de loi prévoit que, lors de l'identification des opérateurs de services essentiels et de l'adoption des mesures de sécurité obligatoires, l'autorité sectorielle consultera formellement les Régions ou les Communautés concernées.

In het kader van het wetsontwerp worden de gewesten en/of de gemeenschappen bij de gang van zaken betrokken op het vlak van:

— de identificatie van de aanbieders van essentiële diensten;

— de sectorale en/of intersectorale criteria, weerslagniveaus of drempelwaarden;

— de lijst van aanbieders van essentiële diensten;

— de sectoren beveiligingsmaatregelen en bijkomende beveiligingsmaatregelen,

— en de weerslagniveaus en/of de drempelwaarden voor de melding van incidenten.

Op initiatief van het CCB en het Crisiscentrum werden de vertegenwoordigers van de gewestelijke besturen in de loop van 2018 uitgenodigd op verschillende werkvergaderingen over het NIS-wetsontwerp. De verschillende versies van het wetsontwerp werden aldus overgezonden aan de betrokken gewestelijke diensten. Het CCB en het Crisiscentrum hebben de vragen van de gewestelijke besturen beantwoord. Het wetsontwerp voorziet tenslotte ook in de mogelijkheid om sectorale overheden op te richten, bestaande uit vertegenwoordigers van de Federale Staat, de gemeenschappen en de gewesten.

— Drinkwater

Er wordt overwogen om de Koning een Nationaal Comité voor de beveiliging van levering en distributie van drinkwater te laten oprichten, dat zou zijn samengesteld uit vertegenwoordigers van de Federale Staat, het Vlaams Gewest, het Brussels Hoofdstedelijk Gewest en het Waals Gewest.

Voor de sector van de distributie van drinkwater achtte de federale regering het wenselijk om, naast het mechanisme van de voorafgaande raadpleging van de gewesten, een sectorale overheid op te richten bestaande uit vertegenwoordigers van de Federale Staat en van de gewesten. De gewestelijke besturen zijn immers vertrouwd met de betrokken aanbieders dankzij hun algemene bevoegdheid inzake water, om hun rol van sectorale overheid te vervullen. Voor de andere sectoren zijn er federale overheden die al instaan voor de coördinatie met de deelgebieden voor de kritieke infrastructuren en die voldoende kennis hebben van de activiteiten van de aanbieders en van de kritieke infrastructuren, zonder dat een nieuwe sectorale overheid moet worden opgericht.

Dans le cadre du projet de loi, les Régions et/ou les Communautés sont associées au processus opératoire en ce qui concerne:

— l'identification des opérateurs de services essentiels;

— les critères sectoriels et/ou intersectoriels, les niveaux d'incidence ou les seuils;

— la liste des opérateurs de services essentiels;

— les mesures de sécurité sectorielles et les mesures complémentaires de sécurité;

— et les niveaux d'incidence et/ou les seuils pour la notification d'incidents.

À l'initiative du CCB et du Centre de crise, les représentants des administrations régionales ont été invités, au cours de l'année 2018, à différentes réunions de travail sur le projet de loi NIS. Les différentes versions du projet de loi ont ainsi été transmises aux services régionaux concernés. Le CCB et le Centre de crise ont répondu aux questions reçues des administrations régionales. Le projet de loi prévoit aussi la possibilité de créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions.

— Eau potable

Il est envisagé la création par le Roi d'un Comité national de sécurité de la fourniture et de la distribution d'eau potable, lequel serait composé de représentants de l'État fédéral, de la Région wallonne, de la Région de Bruxelles-Capitale et de la Région flamande.

Pour le secteur de la distribution de l'eau potable, le gouvernement a jugé opportun, outre le mécanisme de consultation préalable des Régions, de créer une autorité sectorielle composée de représentants de l'État fédéral et des Régions. De par leur compétence générale en matière d'eau, les administrations régionales peuvent en effet compter sur leur bonne connaissance des opérateurs concernés pour remplir leur rôle d'autorité sectorielle. Pour les autres secteurs, il existe des autorités fédérales qui assurent déjà la coordination avec les entités fédérées pour les infrastructures critiques et qui disposent d'une connaissance suffisante des activités des opérateurs et des infrastructures critiques, sans qu'il soit nécessaire de créer une nouvelle autorité sectorielle.

— Maatregelen betreffende de nucleaire sector

Er wordt verduidelijkt dat de elementen van een voor de industriële productie van elektriciteit bestemde nucleaire installatie die dienen voor de transmissie van elektriciteit, volgens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren zijn onderworpen aan de bepalingen van de wet.

Ook moet worden aangestipt dat de regering een wetsontwerp betreffende de nucleaire cyberbeveiliging heeft ingediend, dat betrekking heeft op alle nucleaire operatoren en dat momenteel eveneens wordt besproken in de commissie voor de Binnenlandse Zaken (DOC 54 3336/001). Wat de voor de tenuitvoerlegging van het wetsontwerp vereiste uitvoeringsmaatregelen betreft, legt de regering in een werkgroep de laatste hand aan een koninklijk besluit dat tot doel heeft de bevoegde nationale overheden aan te wijzen, de nadere regels voor de melding en de rapportering van incidenten te bepalen (met inbegrip van de oprichting van een gemeenschappelijk en beveiligd platform voor de melding van incidenten), alsook de algemene accreditatievoorwaarden voor de conformiteitsbeoordelingsinstellingen (externe auditeurs) vast te stellen.

De regering werkt ook aan een ander ontwerp van koninklijk besluit betreffende de oprichting en de werking van een sectorale overheid die bevoegd is voor de drinkwatersector.

2. ***Antwoorden van het Centre for Cybersecurity Belgium (CCB)***

— De gevatte (deel)sectoren

De heer Miguel De Bruycker, managing director van het Centre for Cybersecurity Belgium (CCB), geeft aan dat de sectoren en deelsectoren van de aanbieders van essentiële diensten zijn opgenomen in bijlage I van het wetsontwerp. Het gaat om:

1. energie (elektriciteit, aardolie en gas);

2. vervoer (luchtvervoer, spoorvervoer, vervoer over water en vervoer over de weg);

3. financiën (financiële instellingen, financiële handelsplatformen);

4. gezondheidszorg (zorginstellingen, waaronder ziekenhuizen en privéklinieken);

5. drinkwater (leveranciers en distributeurs van drinkwater);

— Mesures pour le secteur nucléaire

Comme le prévoit la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, il est précisé que les éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité sont soumis aux dispositions de la loi.

Il faut noter également que le gouvernement a déposé le projet de loi relatif à la cybersécurité nucléaire qui vise tous les opérateurs nucléaires et qui est également en discussion en Commission de l'Intérieur (DOC 54 3336/001). Concernant les mesures d'exécution nécessaires à la mise en œuvre du projet de loi, il peut être précisé que le gouvernement finalise en groupe de travail un arrêté royal qui visera à désigner les autorités nationales compétentes, les modalités de notification et de rapportage des incidents, en ce compris la création d'une plate-forme commune et sécurisée de notification des incidents, les conditions générales d'accréditation des organismes de contrôle de la conformité (auditeurs externes).

Le gouvernement travaille également à un autre projet d'arrêté royal portant création et fonctionnement d'une autorité sectorielle compétente pour le secteur de l'eau potable.

2. ***Réponses du Centre pour la Cybersécurité Belgique (CCB),***

— Les (sous-)secteurs couverts

M. Miguel De Bruycker, managing director du Centre pour la Cybersécurité Belgique (CCB), indique que les secteurs et sous-secteurs des opérateurs de services essentiels sont repris à l'annexe I du projet de loi. Il s'agit:

1. de l'énergie (électricité, pétrole et gaz);

2. des transports (aérien, ferroviaire, par voie d'eau et routier);

3. des finances (établissements financiers, plates-formes de négociation financière);

4. de la santé (établissements de soins de santé, y compris les hôpitaux et les cliniques privées);

5. de l'eau potable (fournisseurs et distributeurs d'eau potable);

6. de digitale infrastructuren: IXP (internetknooppunten), leveranciers van DNS-diensten en registers van topleveldomeinnamen.

De NIS-richtlijn sluit activiteiten op het gebied van telecommunicatie en elektronische communicatie uit van zijn toepassingsgebied. Bijgevolg is de telecommunicatiesector niet opgenomen in de bijlage van het wetsontwerp. Activiteiten op het gebied van telecommunicatie en elektronische communicatie zijn immers al onderworpen aan Europese en nationale sectorale regelgeving.

Artikel 19 van het wetsontwerp bepaalt evenwel uitdrukkelijk dat de Koning, bij een in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders kan toevoegen aan bijlage I van deze wet. Bijgevolg kan de Koning de wet uitbreiden naar andere sectoren of naar andere soorten aanbieders binnen een sector.

Binnen de sector kan de sectorale overheid tijdens haar identificatieproces ook andere soorten aanbieders in aanmerking nemen dan die welke expliciet zijn vermeld in bijlage I.

Het gebruikte identificatieproces is vergelijkbaar met dat voor de kritieke infrastructuren: de sectorale overheden (aan te wijzen door de Koning) zullen, in overleg met de ADCC (het Crisiscentrum), het CCB en eventuele betrokken gewestelijke of gemeenschapsoverheden, de aanbieders in kennis stellen van een administratieve identificatiebeslissing.

Het CCB en de ADCC zullen deelnemen aan het voorafgaand overleg over de identificatie en een niet-bindend advies uitbrengen over de aanwijzingsvoorstellen. Deze manier van werken zal het mogelijk maken om eventuele problemen bij de toepassing van de identificatiecriteria in een vroeg stadium te identificeren.

De sectorale overheden hebben, in samenwerking met de ADCC en het CCB, al voorbereidende besprekingen aangevat met toekomstige aanbieders van essentiële diensten.

De formele identificatie kan evenwel slechts plaatsvinden na de inwerkingtreding van de wet. Dit proces zal voor het eerst worden uitgevoerd uiterlijk zes maanden na de inwerkingtreding van de wet. De sectorale overheden zullen daarna regelmatig de lijst van aanbieders en hun essentiële diensten moeten bijwerken, en dit ten minste om de twee jaar.

Wanneer de aanbieder van essentiële diensten een beroep doet op een onderaannemer, moet hij zich ervan

6. des infrastructures numériques: IXP (points d'échange internet), fournisseurs de services DNS et registres de noms de domaines de haut niveau.

La directive NIS exclut de son champ d'application les activités de télécommunication et de communications électroniques. Par conséquent, le secteur des télécommunications ne figure pas dans l'annexe du projet de loi à l'examen. En effet, les activités de télécommunication et de communications électroniques sont déjà soumises à des réglementations sectorielles européennes et nationales.

L'article 19 du projet de loi à l'examen prévoit cependant explicitement que le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs ou types d'opérateurs à l'annexe I de la loi. Le Roi pourra dès lors étendre la loi à d'autres secteurs ou à d'autres types d'opérateurs au sein d'un secteur.

Lors de son processus d'identification, l'autorité sectorielle de chaque secteur figurant dans l'annexe I pourra également prendre en compte d'autres types d'opérateurs que ceux figurant explicitement dans ladite annexe.

Le processus d'identification utilisé sera comparable à celui des infrastructures critiques: les autorités sectorielles (que le Roi désignera) notifieront, en concertation avec la DGCC (le Centre de crise), le CCB et les éventuelles autorités régionales ou communautaires concernées, une décision administrative d'identification aux opérateurs.

Le CCB et la DGCC participeront aux consultations préalables relatives à l'identification et émettront un avis non contraignant sur les propositions de désignation. Cette méthode de travail permettra d'identifier, à un stade précoce, les éventuelles difficultés rencontrées lors de l'application des critères d'identification.

Les autorités sectorielles ont déjà entamé des discussions préparatoires avec de futurs opérateurs de services essentiels, en collaboration avec la DGCC et le CCB.

L'identification formelle ne pourra toutefois intervenir qu'après l'entrée en vigueur de la loi. Cette identification sera effectuée pour la première fois au plus tard dans les six mois suivant l'entrée en vigueur de la loi. Les autorités sectorielles devront ensuite régulièrement mettre à jour la liste des opérateurs et de leurs services essentiels, et ce, au moins tous les deux ans.

Lorsqu'il fait appel à un sous-traitant, l'opérateur de services essentiels doit s'assurer que son sous-traitant

vergewissen dat deze de krachtens deze wet opgelegde beveiligingsmaatregelen werkelijk toepast.

— Eventuele incidenten

De heer Valéry Vander Geeten, juridisch verantwoordelijke van het Centre for Cybersecurity Belgium, geeft aan dat het CCB tot dusver nog geen meldingen heeft ontvangen over een bij een AED in een andere EU-lidstaat voorgevallen incident met een mogelijke weerslag in België.

Dat kan evenwel worden verklaard door het feit dat veel landen de richtlijn pas eind 2018 hebben omgezet en dat de in de richtlijn bepaalde termijn voor het identificeren van de AED's 9 november 2018 was.

— Belgische digitaledienstverleners

De digitaledienstverleners (*cloud-computing*-diensten, onlinemarktplaatsen en onlinezoekmotoren) moeten niet formeel door de bevoegde sectorale overheid worden aangewezen. Zodra de dienstverlener beantwoordt aan de in de wet (art. 6, 27°, 28° en 29°) opgenomen definitie, moet hij voldoen aan de beveiligings- en meldingsvereisten die worden opgelegd door de wet en door Uitvoeringsverordening (EU) 2018/151 van de Europese Commissie van 30 januari 2018 tot vaststelling van de toepassingsbepalingen van Richtlijn (EU) 2016/1148.

De digitaledienstverleners worden opgevolgd door de FOD Economie, die zal optreden als hun (door de Koning aangewezen) sectorale overheid. De digitaledienstverleners moeten de FOD Economie een contactpunt voor de computerbeveiliging bezorgen en moeten de gegevens ervan meedelen aan de sectorale overheid, ook na elke update.

Momenteel bestaan er nog geen cijfergegevens over de digitaledienstverleners in België.

— Impact van de te melden veiligheidsincidenten

De heer Miguel De Bruycker geeft aan dat om te bepalen of een incident aanzienlijke gevolgen heeft, de volgende parameters in aanmerking genomen worden, zoals voorzien in de NIS richtlijn:

a. het aantal gebruikers dat door de verstoring van de essentiële dienst wordt getroffen;

b. de duur van het incident;

applique effectivement les mesures de sécurité imposées par la loi.

— Incidents éventuels

Monsieur Valéry Vander Geeten, responsable juridique du Centre pour la Cybersécurité Belgique, indique que jusqu'à ce jour, le CCB n'a pas encore reçu de notifications d'un incident survenu auprès d'un OSE d'un autre pays membre de l'Union européenne et qui aurait un impact potentiel en Belgique.

Cela s'explique toutefois par le fait que de nombreux pays n'ont transposé la directive que fin de l'année 2018 et que le délai prévu par la directive pour identifier les OSE était le 9 novembre 2018.

— Fournisseurs de service numérique belges

Les fournisseurs de service numérique (service informatique en nuage, place de marché en ligne et moteur de recherche en ligne) ne doivent pas être formellement désignés par l'autorité sectorielle compétente. Dès le moment où le fournisseur répond à la définition donnée par la loi (art. 6, 27°, 28° et 29°), il devra veiller à se conformer aux exigences de sécurité et de notification imposés par la loi et l'acte de la Commission européenne du 30 janvier 2018 (n°2018/151) portant exécution de la directive.

Les fournisseurs de service numérique seront accompagnés par le SPF Économie qui sera leur autorité sectorielle (désignée par le Roi). Les fournisseurs devront transmettre au SPF Économie un point de contact pour la sécurité informatique et en communiquent les données à l'autorité sectorielle, ainsi qu'après chaque mise à jour.

À l'heure actuelle, il n'existe pas encore de données chiffrées sur les fournisseurs de service numérique en Belgique.

— Impact des incidents de sécurité à signaler

M. Miguel De Bruycker indique que pour déterminer si l'impact d'un incident est significatif, il est tenu compte des paramètres suivants, conformément à la directive NIS:

a. le nombre d'utilisateurs touchés par la perturbation du service essentiel;

b. la durée de l'incident;

c. de omvang van het geografische gebied dat door het incident is getroffen.

De Koning kan, per sector of deelsector, weerslagniveaus en/of drempelwaarden bepalen vanaf dewelke een incident aanzienlijke gevolgen heeft.

Bij gebrek aan dergelijke vastgestelde niveaus wordt de AED verzocht om alle gebeurtenissen met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen te melden; dit wil zeggen alle incidenten met reële gevolgen voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen die verband houden met de verlening van een essentiële dienst.

De beschikbaarheid is het vermogen van een informatiesysteem om toegankelijk en bruikbaar te zijn op verzoek van een gemachtigde entiteit. Het gaat erom de normale werking van een informatiesysteem te waarborgen.

De vertrouwelijkheid is het vermogen van een informatiesysteem om toegang tot zijn gegevens door niet-gemachtigde entiteiten te voorkomen. Het gaat erom te vermijden dat de informatie in verkeerde handen valt of openbaar wordt gemaakt zonder toestemming van de verantwoordelijke van het informatiesysteem.

De integriteit is het vermogen van een informatiesysteem om niet te worden gewijzigd door niet-gemachtigde entiteiten. Het gaat erom zich te beschermen tegen een onwettige en schadelijke wijziging van het informatiesysteem.

De authenticiteit is het vermogen van een informatiesysteem om te bevestigen dat het is wat het beweert te zijn. Het gaat erom zeker te zijn dat de gegevens afkomstig zijn van een welbepaald informatiesysteem.

— Verplichte of facultatieve beveiligingsmaatregelen

De heer Valéry Vander Geeten benadrukt dat de AED krachtens de artikelen 20 en 21 van het wetsontwerp een beveiligingsbeleid voor zijn netwerk- en informatiesystemen (IBB) moet uitwerken, dat minstens concrete beveiligingsdoelstellingen en praktische beveiligingsmaatregelen omvat; daartoe voert hij eerst een risicoanalyse van zijn informatiesystemen uit.

Hij heeft de algemene plicht passende en evenredige technische en organisatorische maatregelen te nemen om een niveau van fysieke en logische beveiliging te waarborgen dat is afgestemd op de bestaande risico's, rekening houdend met de stand van de techniek. Hij

c. la portée géographique eu égard à la zone touchée par l'incident.

Le Roi peut établir, par secteur ou sous-secteur, des niveaux d'incidence et/ou des seuils à partir desquels un incident est considéré comme ayant un impact significatif.

En l'absence de tels niveaux déterminés, l'OSE sera invité à notifier tous les événements ayant un impact négatif réel sur la sécurité des systèmes de réseaux et d'information, c'est-à-dire un effet réel sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information liés à la fourniture d'un service essentiel.

La disponibilité est l'aptitude d'un système d'information à être accessible et utilisable à la demande d'une entité autorisée. Il s'agit de garantir le fonctionnement normal d'un système d'information.

La confidentialité est l'aptitude d'un système d'information à ne pas permettre l'accès à ses données à des entités non autorisées. Il s'agit d'éviter que les informations tombent entre des mains malveillantes ou soient rendues publiques sans le consentement du responsable du système d'information.

L'intégrité est l'aptitude d'un système d'information à ne pas être altéré par des entités non autorisées. Il s'agit de se prémunir contre une modification illégitime et nuisible du système d'information.

L'authenticité est l'aptitude d'un système d'information à confirmer qu'il est ce qu'il prétend être. Il s'agit d'être certain que les données proviennent bien d'un système d'information déterminé.

— Mesures de sécurité obligatoires ou facultatives

Monsieur Valéry Vander Geeten souligne qu'en vertu des articles 20 et 21 du projet de loi, l'OSE est tenu d'adopter une politique de sécurité pour ses systèmes d'information et ses réseaux (PSI), en définissant au moins les objectifs et les mesures pratiques de sécurité (après la réalisation d'une analyse de risques de ses systèmes d'information).

Il a l'obligation générale de prendre les mesures techniques et organisationnelles nécessaires et proportionnées pour assurer un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances. Il doit également prendre les

moet ook passende maatregelen nemen om incidenten te voorkomen of de gevolgen ervan te beperken, teneinde de continuïteit van de essentiële diensten te waarborgen.

De beveiligingsmaatregelen en de risiconiveaus variëren naargelang van de soorten netwerk- en informatiesystemen die door de verschillende aanbieders van essentiële diensten worden gebruikt. Bijgevolg heeft het geen zin alle aanbieders van essentiële diensten dezelfde beveiligingsmaatregelen op te leggen. De aanbieder van essentiële diensten zal niettemin moeten aantonen dat hij concreet een beveiligingsmanagementbeleid voor zijn netwerk- en informatiesystemen uitvoert (met name in het licht van de internationale norm ISO 27001, als vermeld in artikel 22).

Bij koninklijk besluit of bij administratieve beslissing van de sectorale overheid kunnen evenwel specifieke beveiligingsmaatregelen worden opgelegd aan de aanbieders van essentiële diensten in een sector of deelsector (zie art. 21, §§ 3 en 4).

Bijvoorbeeld: netwerken waarvan de verleende essentiële diensten afhankelijk zijn, afscheiden van de overige netwerken van de aanbieder.

— Begrippen "aanbieder van essentiële diensten" en "kritieke infrastructuren"

Dit zijn twee verschillende begrippen die elkaar echter aanvullen."Kritieke infrastructuur" verwijst naar een specifieke uitrusting of locatie in België, terwijl een "aanbieder van essentiële diensten" verwijst naar een juridische entiteit die een dienst levert in België, ongeacht de locatie van zijn uitrusting (eventueel in het buitenland). Een aanbieder van essentiële diensten kan eventueel meerdere kritieke infrastructuren beheren.

Een aanbieder van essentiële diensten hangt noodzakelijkerwijs af van de goede werking van netwerk- en informatiesystemen om zijn diensten te verlenen, wat niet noodzakelijk het geval is voor een kritieke infrastructuur.

Bijvoorbeeld: een beheerder van een elektriciteitsdistributienet wordt aangewezen als AED, terwijl sommige van zijn (meest kritieke) sites als kritieke infrastructuren worden aangemerkt.

In de praktijk zal een exploitant van een kritieke infrastructuur in België bijna altijd worden aangewezen als aanbieder van essentiële diensten. Omgekeerd exploiteert een aangewezen aanbieder van essentiële diensten niet automatisch een kritieke infrastructuur (dit hangt af van de locatie van zijn uitrusting en van de

mesures appropriées pour prévenir ou limiter l'impact des incidents, afin d'assurer la continuité des services essentiels.

Les mesures de sécurité et les niveaux de risque encourus sont variables en fonction des types de systèmes et de réseaux informatiques utilisés par les différents opérateurs de services essentiels. Il n'est dès lors pas pertinent d'imposer de manière obligatoire les mêmes mesures de sécurité à tous les opérateurs de services essentiels. Il incombera néanmoins à l'opérateur de démontrer qu'il met en œuvre concrètement une politique de management de la sécurité de ses réseaux et systèmes d'information (au regard notamment de la norme internationale ISO 27001 reprise à l'article 22).

Au sein d'un même secteur ou sous-secteur, un arrêté royal ou une décision administrative de l'autorité sectorielle peut toutefois imposer l'application de certaines mesures de sécurité spécifiques aux opérateurs de services essentiels (voir l'art. 21, §§ 3 et 4).

Par exemple, l'isolement des réseaux dont sont tributaires les services essentiels fournis des autres réseaux de l'opérateur.

— Notions d'opérateurs de services essentiels et d'infrastructures critiques

Il s'agit de deux notions différentes mais complémentaires. L'infrastructure critique vise un équipement ou un lieu précis en Belgique alors que l'opérateur de services essentiels vise une entité juridique qui fournit un service en Belgique, indépendamment des lieux où sont situés ses équipements (éventuellement à l'étranger). Un opérateur de services essentiels peut gérer éventuellement plusieurs infrastructures critiques.

L'opérateur de services essentiels doit nécessairement être tributaire du bon fonctionnement de réseaux et des systèmes d'information pour fournir ses services, ce qui n'est pas nécessairement le cas d'une infrastructure critique.

Par exemple, un gestionnaire de réseau dans le domaine de l'énergie est désigné comme un OSE et certains de ses sites (les plus critiques) sont identifiés comme infrastructures critiques.

Dans les faits, l'exploitant d'une infrastructure critique en Belgique sera désigné, dans la presque totalité des cas, comme un opérateur de services essentiels. A l'inverse, l'opérateur de services essentiels désigné n'exploitera pas automatiquement une infrastructure critique (cela dépendra de la localisation de ses

vraag of hij al dan niet afhankelijk is van netwerk- en informatiesystemen).

Bijvoorbeeld: de beheerder van een elektriciteitsdistributienet die reeds is aangemerkt als exploitant van een kritieke infrastructuur, zal bijna automatisch worden aangewezen als AED.

— Strategie (artikel 10)

Het *Centre for Cybersecurity Belgium* werkt momenteel aan een nieuwe versie van de nationale cyberstrategie (actualisering van de door de regering in 2012 uitgewerkte strategie), die na de inwerkingtreding van de wet aan de regering zal worden voorgelegd. Deze nieuwe versie zal concreter en nauwkeuriger zijn, en komt er in overleg met de verschillende departementen die bij de cyberveiligheid betrokken zijn.

Zoals bepaald bij artikel 10 van het wetsontwerp, zal deze strategie de elementen bevatten die krachtens de NIS-richtlijn zijn vereist om een nationale strategie uit te werken. Ze zal trouwens volledig aansluiten bij het nationaal investeringsplan van de regering.

— Externe audit

De heer Miguel De Bruycker duidt aan dat de inwerkingtreding van de wet en van het koninklijk uitvoeringsbesluit moet worden afgewacht om te beschikken over instellingen voor de conformiteitsbeoordeling die geaccrediteerd zijn door BELAC of een andere accreditatie-instelling van een lidstaat van de Europese Unie, of die erkend zijn door de sectorale overheid.

Vanaf deze inwerkingtreding kunnen alle instellingen die beschikken over een accreditatie voor de ISO 27000-norm uitgegeven door BELAC of door een andere accreditatie-instelling van een lidstaat van de Europese Unie door de aanbieders van essentiële diensten gevraagd worden om de conformiteitsbeoordeling uit te voeren.

De termijn van drie jaar is een redelijk compromis tussen de kostprijs van een externe audit voor de aanbieder en de constante evolutie van de technologie.

De kostprijs van een externe audit hangt af van de omvang van de aanbieder, het aantal betrokken systemen en de ervaring van de auditeurs.

— Europese samenwerking

De beveiligingsmaatregelen van digitale diensten moeten voldoen aan de uitvoeringsverordeningen van de Europese Commissie.

équipements et de sa dépendance ou non à des réseaux et systèmes d'information).

Par exemple, le gestionnaire dans le domaine de l'énergie qui est déjà identifié comme exploitant d'une infrastructure critique sera presque automatiquement désigné comme un OSE.

— Stratégie (article 10)

Le Centre pour la Cybersécurité Belgique travaille actuellement à une nouvelle version de la stratégie nationale cyber (actualisant celle élaborée par le gouvernement en 2012), laquelle sera soumise au gouvernement après l'entrée en vigueur de la loi. Cette nouvelle version sera plus concrète, précise et intégrée avec les différents départements impliqués dans la Cybersécurité.

Comme le prévoit l'article 10 du projet de loi, cette stratégie reprendra les éléments requis par la directive NIS pour l'adoption d'une stratégie nationale. Celle-ci s'inscrira d'ailleurs pleinement dans le plan national d'investissements adopté par le gouvernement.

— Audit externe

M. Miguel De Bruycker précise qu'il faut attendre l'entrée en vigueur de la loi et de l'arrêté royal d'exécution pour qu'il puisse y avoir des organismes d'évaluation de la conformité accrédités par BELAC ou un autre organisme d'accréditation d'un État membre de l'Union européenne ou agréés par l'autorité sectorielle

À partir de cette entrée en vigueur, tous les organismes qui disposent d'une accréditation pour la norme ISO 27000 délivrée par BELAC ou par un autre organisme d'accréditation d'un État membre de l'Union européenne pourront être invités, par les opérateurs de services essentiels, à procéder à une évaluation de la conformité.

Le délai de trois ans est un compromis raisonnable entre le coût pour l'opérateur de faire réaliser un audit externe et l'évolution constante des technologies.

Le coût d'un audit externe dépend de la taille de l'opérateur, du nombre de systèmes concernés et de l'expérience des auditeurs.

— Coopération européenne

Les mesures de sécurité des services numériques devront être conformes aux règlements d'exécution de la Commission européenne.

Het CCB neemt deel aan de Europese Samenwerkingsgroep en aan het CSIRT-netwerk, opgericht om de strategische samenwerking en de informatie-uitwisseling te bevorderen.

Het CSIRT-netwerk speelt niet alleen een operationele rol, maar komt ook regelmatig samen en heeft een aantal opdrachten op basis van artikel 12 (3), van de richtlijn.

Volgens artikel 29 van de wet moeten nationale CSIRT's incidenten melden aan de andere lidstaten van de Europese Unie wanneer die aanzienlijke gevolgen hebben voor de continuïteit van essentiële diensten in die lidstaten.

— Afstemming van de AVG- en NIS-regelgeving

De heer Valéry Vander Geeten geeft aan dat artikel 31, § 1, de Koning gelast de nadere regels te bepalen inzake de melding en de rapportering van incidenten, met inbegrip van de oprichting van een beveiligd meldingsplatform.

Via dit platform zullen de aanbieders van essentiële diensten tevens inbreuken in verband met persoonsgegevens kunnen melden aan de toezichthoudende autoriteiten, zoals bepaald bij artikel 33, eerste lid, van Verordening (EU) 2016/679.

Wanneer een aanbieder van essentiële diensten een onderaannemer inschakelt, moet hij zich ervan vergewissen dat die de bij deze wet opgelegde beveiligingsmaatregelen daadwerkelijk toepast.

Het is niet ondenkbaar dat eenzelfde aanbieder voor bepaalde van zijn activiteiten wordt aangewezen als aanbieder van essentiële diensten, en voor andere activiteiten wordt aangemerkt als een digitaledienstverlener (die onderworpen is aan regels die rechtstreeks door de Europese Unie worden bepaald).

Bijvoorbeeld: een telecomaanbieder kan voor sommige van zijn activiteiten onderworpen zijn aan de verplichtingen van een aanbieder van essentiële diensten (bijvoorbeeld een leverancier van DNS-diensten), en voor andere aan de verplichtingen van een digitaledienstverlener (*cloud-computing*-dienst).

Naargelang van de betrokken activiteit zal hij ofwel moeten voldoen aan zijn verplichtingen als aanbieder van essentiële diensten, ofwel aan zijn verplichtingen als digitaledienstverlener (of zal hij eventueel voor al zijn systemen de strengste regels van beide moeten toepassen).

Le CCB participe au Groupe de coopération européen et au réseau des CSIRT, créés pour promouvoir la coopération stratégique et l'échange d'informations.

Le réseau des CSIRT ne joue pas uniquement un rôle opérationnel mais se réunit aussi régulièrement et remplit une série de missions sur la base de l'article 12 (3) de la directive.

L'article 29 de la loi charge le CSIRT national (CCB) de signaler aux autres États membres de l'Union européenne les incidents ayant un impact significatif sur la continuité des services essentiels dans ces États membres.

— Harmonisation des législations GDPR et NIS

Monsieur Valéry Vander Geeten explique que l'article 31, § 1er, charge le Roi de déterminer les modalités de notification et de rapportage des incidents, en ce compris de créer une plate-forme sécurisée de notification.

Cette plate-forme pourra permettre également aux opérateurs de services essentiels de notifier aux autorités de contrôle les violations de données à caractère personnel, comme imposé par l'article 33, alinéa 1er, du règlement UE 2016/679.

Lorsqu'il fait appel à un sous-traitant, l'opérateur de services essentiels doit s'assurer que son sous-traitant applique effectivement les mesures de sécurité imposées en vertu de la présente loi.

Il est tout à fait possible qu'un même opérateur soit, pour certaines de ses activités, désigné comme un opérateur de services essentiels et, pour d'autres activités, comme un fournisseur de service numérique (lequel est soumis à des règles directement prévues au niveau de l'Union européenne).

Par exemple, un opérateur télécom pourrait ainsi être soumis pour certaines de ses activités aux obligations d'un opérateur de services essentiels (p. ex. un fournisseur de services DNS) et pour d'autres aux obligations d'un fournisseur de service numérique (service d'informatique en nuage).

En fonction de l'activité concernée, il devra se conformer soit à ses obligations en qualité d'OSE, soit à ses obligations de FSN (ou éventuellement appliquer pour tous ses systèmes les règles les plus strictes des deux).

III. — **ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN**

TITEL 1

Definities en algemene bepalingen

HOOFDSTUK 1

Onderwerp en toepassingsgebied

Afdeling 1

Onderwerp

Artikelen 1 en 2

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

Afdeling 2

Toepassingsgebied

Art. 3 tot 5

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Definities

Art. 6

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 3

Bevoegde autoriteiten en samenwerking op nationaal niveau

Afdeling 1

Bevoegde autoriteiten

Art. 7

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

III. — **DISCUSSION DES ARTICLES ET VOTES**

TITRE 1ER

Définitions et dispositions générales

CHAPITRE 1ER

Objet et champ d'application

Section 1re

Objet

Articles 1 et 2

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

Section 2

Champ d'application

Art. 3 à 5

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

CHAPITRE 2

Définitions

Art. 6

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

CHAPITRE 3

Autorités compétentes et coopération au niveau national

Section 1re

Autorités compétentes

Art. 7

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

Afdeling 2

Samenwerking op nationaal niveau

Art. 8

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 4

Informatie-uitwisseling

Art. 9

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 5

Nationale strategie voor de beveiliging van netwerk- en informatiesystemen

Art. 10

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

TITEL 2

Netwerk- en informatiesystemen van de aanbieders van essentiële diensten

HOOFDSTUK 1

Identificatie van de aanbieders van essentiële diensten

Art. 11 tot 19

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Beveiligingsmaatregelen

Artikel 20 tot 23

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

Section 2

Coopération au niveau national

Art. 8

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

CHAPITRE 4

Échange d'informations

Art. 9

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

CHAPITRE 5

Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 10

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

TITRE 2

Réseaux et systèmes d'information des opérateurs de services essentiels

CHAPITRE 1ER

Identification des opérateurs de services essentiels

Art. 11 à 19

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

CHAPITRE 2

Mesures de sécurité

Articles 20 à 23

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

HOOFDSTUK 3

Melding van incidenten

Art. 24 tot 31

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

TITEL 3

Netwerk- en informatiesystemen van digitaledienstverleners

Art. 32

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 1

De beveiligingseisen

Art. 33 en 34

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Melding van incidenten

Art. 35 tot 37

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

CHAPITRE 3

Notification d'incidents

Art. 24 à 31

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

TITRE 3

Réseaux et systèmes d'information des fournisseurs de service numérique

Art. 32

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

CHAPITRE 1ER

Les exigences de sécurité

Art. 33 et 34

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

CHAPITRE 2

Notification d'incidents

Art. 35 à 37

Ces articles, qui ne donnent lieu à aucune observation, sont successivement adoptés à l'unanimité.

TITEL 4

Toezicht en sancties

HOOFDSTUK 1

Toezicht op de aanbieders van essentiële diensten

Afdeling 1

Audits

Art. 38 tot 41

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

Afdeling 2

Inspectiedienst

Art. 42 en 43

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

Art. 44

Dit artikel bevat de nadere regels betreffende de legitimatiekaart en de bevoegdheden van de leden van de inspectiedienst.

Mevrouw Françoise Schepmans c.s. dient *amendement nr. 1* (DOC 54 3340/002) in tot wijziging van het artikel. De hoofdindiener licht toe dat het amendement aansluiting zoekt bij de recente rechtspraak van het Grondwettelijk Hof. Zij verwijst voor het overige naar de verantwoording bij het amendement.

Amendement nr. 1 en het aldus geamendeerde artikel 44 worden achtereenvolgens eenparig aangenomen.

Art. 45 en 46

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

TITRE 4

Contrôle et sanctions

CHAPITRE IER

Les contrôles des opérateurs de services essentiels

Section 1re

Audits

Art. 38 à 41

Ces articles, qui ne donnent lieu à aucune observation, sont adoptés successivement à l'unanimité.

Section 2

Service d'inspection

Art. 42 et 43

Ces articles, qui ne donnent lieu à aucune observation, sont adoptés successivement à l'unanimité.

Art. 44

Cet article fixe les modalités concernant la carte de légitimation et les compétences des membres du service d'inspection.

Mme Françoise Schepmans et consorts présentent l'*amendement n° 1* (DOC 54 3340/002) tendant à modifier l'article. L'auteure principale explique que l'amendement tend à conformer l'article à la jurisprudence récente de la Cour constitutionnelle. Pour le surplus, elle renvoie à la justification de l'amendement.

L'amendement n° 1 et l'article 44, tel qu'il a été amendé, sont adoptés successivement à l'unanimité.

Art. 45 et 46

Ces articles, qui ne font l'objet d'aucune observation, sont adoptés successivement à l'unanimité.

HOOFDSTUK 2

Toezicht op de digitaledienstverleners

Art. 47

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 3

De sancties

Afdeling 1

Procedure

Art. 48 tot 50

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

Afdeling 2

Strafrechtelijke sancties

Art. 51

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

Afdeling 3

Administratieve sancties

Art. 52 tot 59

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

CHAPITRE 2

Contrôle des fournisseurs de service numérique

Art. 47

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

CHAPITRE 3

Les sanctions

Section 1re

Procédure

Art. 48 à 50

Ces articles, qui ne donnent lieu à aucune observation, sont adoptés successivement à l'unanimité.

Section 2

Sanctions pénales

Art. 51

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

Section 3

Sanctions administratives

Art. 52 à 59

Ces articles, qui ne donnent lieu à aucune observation, sont adoptés successivement à l'unanimité.

TITEL 5

CSIRT

HOOFDSTUK 1

Het nationale CSIRT

Afdeling 1

Taken van het nationale CSIRT

Art. 60

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

Afdeling 2

Voorschriften voor het nationale CSIRT

Art. 61 en 62

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Het sectoraal CSIRT

Afdeling 1

Taken van het sectoraal CSIRT

Art. 63

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

Afdeling 2

Voorschriften voor een sectoraal CSIRT

Art. 64

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

TITRE 5

CSIRT

CHAPITRE 1ER

Le CSIRT national

Section 1re

Tâches du CSIRT national

Art. 60

Cet article, qui ne donne lieu à aucune observation, est adopté à l'unanimité.

Section 2

Obligations du CSIRT national

Art. 61 et 62

Ces articles, qui ne donnent lieu à aucune observation, sont adoptés successivement à l'unanimité.

CHAPITRE 2

Le CSIRT sectoriel

Section 1re

Tâches du CSIRT sectoriel

Art. 63

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

Section 2

Obligations d'un CSIRT sectoriel

Art. 64

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

TITEL 6

Verwerking van persoonsgegevens

HOOFDSTUK 1

Beginselen inzake verwerking, wettelijke basis en doeleinden

Art. 65 tot 68

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Bewaartermijn

Art. 69

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 3

Functionaris voor gegevensbescherming

Art. 70

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

HOOFDSTUK 4

Beperking van de rechten van de betrokken personen

Art. 71 en 72

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

TITRE 6

Traitement des données à caractère personnel

CHAPITRE 1ER

Principes relatifs au traitement, bases légales et finalités

Art. 65 à 68

Ces articles ne donnent lieu à aucune observation et sont successivement adoptés à l'unanimité.

CHAPITRE 2

Durée de conservation

Art. 69

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

CHAPITRE 3

Délégué à la protection des données

Art. 70

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

CHAPITRE 4

Limitations des droits des personnes concernées

Art. 71 et 72

Ces articles ne donnent lieu à aucune observation et sont successivement adoptés à l'unanimité.

HOOFDSTUK 5

Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens

Art. 73

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

TITEL 7

Slotbepalingen

HOOFDSTUK 1

Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren

Art. 74

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

Art. 75

Dit artikel strekt tot wijziging van artikel 3 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

Mevrouw Françoise Schepmans c.s. dient *amendement nr. 2* (DOC 54 3340/002) in tot wijziging van het artikel. De hoofdindiener licht toe dat het amendement het artikel in overeenstemming brengt met de andere bepalingen van het wetsontwerp en met bijlage I, alsook met het advies van de Raad van State. Zij verwijst voor het overige naar de verantwoording bij het amendement.

Amendement nr. 2 en het aldus geamendeerde artikel 75 worden achtereenvolgens eenparig aangenomen.

Art. 76

Dit artikel strekt tot wijziging van artikel 4 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

Mevrouw Françoise Schepmans c.s. dient *amendement nr. 3* (DOC 54 3340/002) in tot vervanging van het artikel. De hoofdindiener licht toe dat het amendement het artikel eveneens in overeenstemming brengt met de

CHAPITRE 5

Limitations aux obligations de notification des violations de données à caractère personnel

Art. 73

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

TITRE 7

Dispositions finales

CHAPITRE 1ER

Modifications de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques

Art. 74

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

Art. 75

Cet article vise à modifier l'article 3 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Mme Françoise Schepmans et consorts présentent *l'amendement n° 2* (DOC 54 3340/002) tendant à modifier cet article. L'auteure principale explique que cet amendement tend à mettre cet article en conformité avec les autres dispositions du projet de loi à l'examen et avec l'annexe I, ainsi qu'avec l'avis du Conseil d'État. Pour le surplus, elle renvoie à la justification de l'amendement.

L'amendement n° 2 et l'article 75, ainsi modifié, sont successivement adoptés à l'unanimité.

Art. 76

Cet article vise à modifier l'article 4 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Mme Françoise Schepmans et consorts présentent *l'amendement n° 3* (DOC 54 3340/002) tendant à remplacer cet article. L'auteure principale explique que cet amendement tend également à mettre cet article

andere bepalingen van het wetsontwerp en met bijlage I, in het bijzonder voor wat betreft de sector financiën en de sector drinkwater.

Amendement nr. 3 tot vervanging van het artikel wordt eenparig aangenomen.

Art. 77 tot 84

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Wijzigingen 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. 85 en 86

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 3

Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector

Art. 87 tot 89

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

en conformité avec les autres dispositions du projet de loi à l'examen et avec l'annexe I, en particulier en ce qui concerne le secteur des finances et le secteur de l'eau potable.

L'amendement n° 3 tendant à remplacer cet article est adopté à l'unanimité.

Art. 77 à 84

Ces articles ne donnent lieu à aucune observation et sont successivement adoptés à l'unanimité.

CHAPITRE 2

Modifications 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. 85 et 86

Ces articles ne donnent lieu à aucune observation et sont successivement adoptés à l'unanimité.

CHAPITRE 3

Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 87 à 89

Ces articles ne donnent lieu à aucune observation. Ils sont successivement adoptés à l'unanimité.

HOOFDSTUK 4

Wijzigingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

De voorzitter merkt op dat het hoofdstuk 4 ertoe strekt om twee verschillende wetten te wijzigen.

Om de samenhang van het wetsontwerp te waarborgen wordt er voorgesteld om dit hoofdstuk te splitsen in twee aparte hoofdstukken, het ene met de wijzigingsbepalingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU en het andere met de wijzigingsbepalingen van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten

Art. 90

De voorzitter stelt vast dat het ontworpen artikel 90 strekt tot wijziging van de artikelen 71 en 79 van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

Vanuit wetgevingstechnisch oogpunt is het aangewezen het artikel te splitsen in twee wijzigende bepalingen, enerzijds van artikel 71 en anderzijds van artikel 79.

De commissie gaat akkoord met deze opmerking.

Het artikel, zoals verbeterd, wordt eenparig aangenomen.

Art. 91

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

CHAPITRE 4

Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

Le président observe que le chapitre 4 tend à modifier deux lois distinctes.

Pour garantir la cohérence du projet de loi, il est proposé de scinder ce chapitre en deux chapitres distincts, l'un contenant les dispositions modificatives de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE et l'autre contenant les dispositions de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

Art. 90

Le président remarque que l'article 90 en projet tend à modifier les articles 71 et 79 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.

D'un point de vue légistique, il serait indiqué de scinder l'article 90 en deux dispositions modificatives, d'une part de l'article 71 et d'autre part de l'article 79.

La commission marque son accord sur cette observation.

L'article, tel que corrigé, est adopté à l'unanimité.

Art. 91

Cet article ne donne lieu à aucune observation et est adopté à l'unanimité.

HOOFDSTUK 5

Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 92 tot 94

Deze artikelen, waarover geen opmerkingen worden gemaakt, worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 6

Inwerkingtreding

Art. 95

Dit artikel, waarover geen opmerkingen worden gemaakt, wordt eenparig aangenomen.

BIJLAGEN

Bijlage I en bijlage II worden achtereenvolgens eenparig aangenomen.

*
* *

Het gehele, aldus geamendeerde en verbeterde wetsontwerp wordt met inbegrip van de bijlagen eenparig aangenomen.

De rapporteurs, *De voorzitters,*

Franky DEMON
Eric THIÉBAUT

Brecht VERMEULEN
Koenraad DEGROOTE *a.i.*

Artikelen die een uitvoeringsbepaling vereisen (art. 78.2 Rgt.): niet meegedeeld.

CHAPITRE 5

Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 92 à 94

Ces articles ne donnent lieu à aucune observation. Ils sont successivement adoptés à l'unanimité.

CHAPITRE 6

Entrée en vigueur

Art. 95

Cet article ne donne lieu à aucune observation. Il est adopté à l'unanimité.

ANNEXES

Les annexes I et II sont successivement adoptées à l'unanimité.

*
* *

L'ensemble du projet de loi, tel qu'il a été amendé et corrigé, y compris les annexes, est adopté à l'unanimité.

Les rapporteurs, *Les présidents,*

Franky DEMON
Eric THIÉBAUT

Brecht VERMEULEN
Koenraad DEGROOTE *a.i.*

Articles nécessitant une mesure d'exécution (art. 78.2 du Règlement): non communiqué.

Centrale drukkerij – Imprimerie centrale