DOC 54 **3336/003**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

12 maart 2019

WETSONTWERP

houdende wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle betreffende de nucleaire cyberbeveiliging

VERSLAG

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

INHOUD Blz.

Zie:

Doc 54 **3336/ (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

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

RAPPORT

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

SOMMAIRE Pages

Voir:

Doc 54 **3336/ (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 7 november 2018 en 27 februari 2019.

I. — **INLEIDENDE UITEENZETTING**

Tijdens de vergadering van 7 november 2018 licht *de heer Jan Jambon, vice-eersteminister en minister van Veiligheid en Binnenlandse Zaken, belast met de Regie der gebouwen*, licht toe dat het wetsontwerp ertoe strekt de bestaande wetgeving inzake de nucleaire beveiliging te vervolledigen op het vlak van de cyberbeveiliging.

Door de toenemende cyberaanvallen tegen de overheid en de industrie wordt cyberbeveiliging op internationaal en nationaal vlak meer dan ooit een prioriteit. De bedreigingen ter zake nopen alle regeringen en beveiligingsoverheden tot bezorgdheid.

A. **De wettelijke regeling voor cyberbeveiliging in België**

De Belgische aanpak van de nucleaire cyberbeveiliging maakt deel uit van het specifieke stelsel voor de fysieke beveiliging van de nucleaire installaties en voor de bescherming van de zogenaamde gecategoriseerde informatie, met andere woorden de gegevens die betrekking hebben op de fysieke beveiligingsmaatregelen voor nucleaire installaties. Die aanpak vloeit voort uit de toepassing door ons land van het Verdrag inzake de fysieke beveiliging van kernmateriaal en nucleaire installaties. Na de *Nuclear Security Summit* van 2016 te Washington is het amendement op dat Verdrag in werking getreden.

Het geamendeerde Verdrag beoogt overal ter wereld een doeltreffende fysieke beveiliging van het kernmateriaal en de nucleaire installaties tot stand te brengen en in stand te houden; het betreft eveneens de bescherming van de gevoelige informatie. Daarom zijn de kernexploitanten op grond van de in België vigerende wetgeving ertoe verplicht om elke vorm van als "nucleair document" omschreven informatie te beschermen, ook wanneer die elektronisch of digitaal beschikbaar is.

Hoewel de termen "cyberbeveiliging" en "cyberaanval" niet letterlijk in de thans vigerende wetgeving staan, heeft elke nucleaire installatie bijgevolg nu al de verplichting om maatregelen te nemen om die nucleaire documenten te beschermen.

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de ses réunions des 7 novembre 2018 et 27 février 2019.

I. — **EXPOSÉ INTRODUCTIF**

Lors de la réunion du 7 novembre 2018, *M. Jan Jambon, vice-premier ministre et ministre de la Sécurité et de l'Intérieur, chargé de la Régie des Bâtiments*, explique que le projet de loi tend à compléter la législation relative à la sécurité nucléaire pour ce qui concerne la cybersécurité.

Suite à la multiplication des cyber-attaques contre des gouvernements et des industries, la cybersécurité est plus que jamais une priorité tant au niveau international que national. Les menaces en la matière constitue une préoccupation de tous les gouvernements et des autorités de sécurité.

A. **Le régime légal de la cybersécurité en Belgique**

L'approche de la cybersécurité nucléaire par la Belgique s'est inscrite dans le cadre du régime spécifique de la protection physique des installations nucléaires et de la protection des informations dites catégorisées, ce qui veut dire les informations qui portent sur les mesures de protection physique des installations nucléaires. Une telle approche découle de la mise en œuvre par la Belgique de la Convention sur la protection physique des matières et des installations nucléaires. L'amendement à cette Convention est entré en vigueur après le *Nuclear Security Summit* de 2016 à Washington.

La Convention amendée, qui a pour objectif d'instaurer et de maintenir dans le monde entier une protection physique efficace des matières et des installations nucléaires, porte également sur la protection de l'information sensible. C'est la raison pour laquelle la législation en vigueur en Belgique oblige les exploitants nucléaires à protéger tout type d'information définie, selon la législation, comme étant un "document nucléaire", y compris celle qui est disponible sur un support informatique et sous forme digitale.

En conséquence, et bien que les termes "cybersécurité" et "cyberattaque" ne figurent pas littéralement dans la législation pour l'instant en vigueur, toute installation nucléaire a d'ores et déjà l'obligation de prendre des mesures afin de protéger ces documents nucléaires.

Sinds jaren waren de inspanningen van de regering inzake nucleaire beveiliging vooral gericht op de versterking van de fysieke beveiligingssystemen van de nucleaire installaties. Het was vooral zaak om elke niet-toegestane toegang tot de nucleaire sites te verhinderen, teneinde elke kwaadwillige handeling te voorkomen waarbij kernmateriaal betrokken is. Door de toenemende cyberaanvallen op regeringen, instellingen en de industrie is de cyberbeveiliging evenwel een prioriteit geworden.

In deze context hebben de Belgische bevoegde autoriteiten een project opgestart om de mogelijke kenmerken van eventuele cyberaanvallen tegen de nucleaire sector te achterhalen. Dankzij deze aanpak konden de bijzonderheden van een dreiging en de specifieke risico's inzake de nucleaire installaties op ons grondgebied in kaart worden gebracht. Algemeen zijn de Belgische nucleaire beveiligingsautoriteiten er zich terdege van bewust dat de kerninstallaties, net als de inrichtingen waar ioniserende straling wordt gebruikt trouwens, een mogelijk doelwit voor cyberaanvallen vormen.

Het bewijs hiervan is het feit dat België, op eigen initiatief, het toepassingsgebied van de weerstandstests van 2011 heeft uitgebreid tot het risico op cyberaanvallen: na de kernramp in de kerncentrale van Fukushima-Daiichi in 2011 werden de Belgische nucleaire installaties van klasse I in het kader van gezamenlijke Europese initiatieven onderworpen aan weerstandstests (de zogenaamde "*stress tests*").

In ons land bleven deze weerstandstests niet beperkt tot de weerstand tegen de extreme natuurverschijnselen, maar werden zij verruimd tot de mogelijke bedreigingen die het gevolg zijn van menselijke handelingen, waaronder een cyberaanval. De exploitanten hebben de kwetsbaarheid van de installaties voor cyberaanvallen geanalyseerd; vervolgens werd de betrouwbaarheid van deze analyses geëvalueerd door het FANC en door Bel V.

Volgens de analyses van de exploitanten is het verlies van de veiligheidsfuncties van de kerncentrales ten gevolge van een cyberaanval weinig waarschijnlijk, met name omdat maatregelen (onder meer fysieke beveiliging) werden genomen ter bescherming van de informaticasystemen die de veiligheidsfuncties ondersteunen.

Hoewel de evaluatie van het FANC en van Bel V deze conclusies grotendeels bevestigde, werd verzocht de cyberbeveiligingsrisico's nauwgezet op te volgen en werd op meerdere aandachtspunten gewezen. Eerst en vooral nemen de kwetsbaarheid en het risico toe naarmate de informaticatechnologie van de installaties wordt gemoderniseerd. Voorts worden de industriële

Depuis des années, les efforts du gouvernement en matière de sécurité nucléaire avaient donc surtout porté sur le renforcement des systèmes de protection physique des installations nucléaires. Il s'agissait d'empêcher tout accès non autorisé aux sites nucléaires afin de prévenir tout acte malveillant impliquant des matières nucléaires. Cependant, suite à la multiplication des cyber-attaques contre des gouvernements, des institutions ou des industries, la cybersécurité est devenue une priorité.

C'est dans ce contexte que les autorités belges compétentes avaient initié un processus visant à identifier les possibles caractéristiques des éventuelles cyber-attaques portant sur le secteur nucléaire. Cette démarche a permis d'identifier les particularités des menaces et les risques propres aux installations nucléaires présentes sur notre territoire. De manière générale, les autorités de sécurité belges sont tout à fait conscientes du fait que les installations nucléaires, de même d'ailleurs que les établissements où des rayonnements ionisants sont utilisés, constituent une cible potentielle de cyber-attaques.

Témoigne de cette conviction le fait que la Belgique avait, d'initiative, élargi la portée des tests de résistance de 2011 au risque de cyber-attaques: au lendemain de l'accident nucléaire de Fukushima-Daiichi en 2011, les installations nucléaires belges ont été soumises à des tests de résistance, baptisés "*stress tests*", dans le cadre d'initiatives prises conjointement au niveau européen.

Dans notre pays, la portée de ces tests de résistance ne s'était pas limitée aux phénomènes naturels extrêmes, mais elle avait été élargie aux menaces potentielles liées aux activités humaines telles qu'une cyber-attaque. La vulnérabilité des installations aux cyber-attaques a fait l'objet d'une analyse des exploitants, dont la fiabilité avait ensuite été évaluée par l'AFCN et Bel V.

Selon l'analyse des exploitants, la perte des fonctions de sûreté des centrales nucléaires résultant d'une attaque informatique était difficilement concevable, considérant notamment les dispositions en place (incluant la protection physique) pour protéger les systèmes informatisés qui soutiennent des fonctions de sûreté.

Si l'évaluation de l'AFCN et de Bel V avait confirmé ces conclusions dans une large mesure, elle demandait un suivi minutieux des risques de cybersécurité et identifiait plusieurs points d'attention. Tout d'abord, la vulnérabilité et le risque augmentent de plus en plus au fur et à mesure de la modernisation de la technologie informatique des installations. Par ailleurs, la vulnérabilité

systemen van het type SCADA (*Supervisory Control and Data Acquisition*) kwetsbaarder doordat nieuwe malware opduikt die wordt ontwikkeld om deze systemen aan te vallen.

B. **Doelstelling**

Rekening houdend met de dreiging en de hierboven uiteengezette beschouwingen, dient het wettelijk stelsel hoofdzakelijk in twee opzichten verder te worden aangevuld en uitgewerkt. Enerzijds mag het niet worden beperkt tot de nucleaire installaties, maar moet het worden uitgebreid tot alle inrichtingen waar ioniserende straling wordt gebruikt. Anderzijds mogen de maatregelen die door de operatoren moeten worden genomen niet alleen gericht zijn op de bescherming van de informatie, maar tevens van de industriële en technische operaties, gelet op de kwetsbaarheid van de systemen van het type SCADA.

Het wetsontwerp strekt niet tot de omzetting van de zogenaamde "NIS"-Richtlijn (d.w.z. de Europese Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie) op een manier die aan de nucleaire sector aangepast zou zijn. Het sluit veeleer aan op de internationale verdragen met betrekking tot de nucleaire beveiliging en wil beantwoorden aan de vereisten van een sector die een intrinsiek beveiligingsrisico inhoudt, maar niet noodzakelijk een risico op de onderbreking van een essentiële dienst. Dit laatste is de doelstelling van het wetsontwerp tot omzetting van de NIS-richtlijn, meer bepaald het wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid", dat eerstdaags ter bespreking aan het Parlement zal worden voorgelegd.

Het is immers niet de dienstverlening – bijvoorbeeld de elektriciteitsproductie – maar de nucleaire beveiliging die de absolute prioriteit moet krijgen. Ondanks het fundamentele verschil in perspectief, zal het wetsontwerp een gelijkaardig stelsel invoeren zoals voorzien in het wetsontwerp over NIS. Om voor een zo groot mogelijke coherentie te zorgen, zullen de overheden die betrokken zijn bij de NIS-regelgeving, en in elk geval het Crisiscentrum en het Centrum voor *Cybersecurity*, ook betrokken worden bij de uitwerking en opvolging van de nucleaire cyberbeveiliging.

Een specifieke en aparte aanpak dringt zich niet alleen op omwille van het huidig kader van de nucleaire cyberbeveiliging en van de genese van het voorliggende wetsontwerp, maar tevens omwille van de specifieke

des systèmes industriels de type SCADA (*Supervisory Control and Data Acquisition*) augmente en raison de l'apparition de nouveaux malwares développés pour s'attaquer à ces systèmes.

B. **Objectifs**

Compte tenu de la menace et des considérations développées ci-dessus, il convient d'entreprendre de compléter et d'approfondir le régime légal, essentiellement à deux titres. D'une part, le régime ne doit pas être limité aux seules installations nucléaires mais doit être étendu à tous les établissements où des rayonnements ionisants sont utilisés. D'autre part, les mesures à adopter par les opérateurs devront viser à la protection non seulement des informations mais aussi des opérations industrielles ou techniques, dès lors que la vulnérabilité des systèmes de type SCADA a été identifiée.

Le projet de loi ne vise pas la transposition, adaptée au secteur nucléaire, de la Directive dite "NIS" (c'est-à-dire la Directive européenne (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union). Elle se situe plutôt dans la perspective des conventions internationales relatives à la sécurité nucléaire et veut répondre aux nécessités d'un secteur qui présente un risque de sécurité intrinsèque, mais ne présente pas nécessairement un risque d'interruption d'un service essentiel. Ceci est l'objectif du projet de loi transposant la directive dite NIS, à savoir le projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, qui sera soumis au parlement dans les prochains jours.

Ce n'est en effet pas au service – par exemple la production d'électricité, mais à la sécurité nucléaire qu'il convient d'accorder la priorité absolue. En dépit de la différence fondamentale de perspective, le projet de loi introduira un régime proche de celui prévu dans le projet de loi NIS. Afin de veiller à une cohérence maximale, les autorités associées à la réglementation NIS, et en tout cas le Centre de crise et le Centre pour la cybersécurité, seront également associés à l'élaboration et au suivi de la cybersécurité nucléaire.

Une telle approche spécifique et distincte s'impose non seulement en raison du cadre actuel de la cybersécurité nucléaire ainsi que de la genèse du projet de loi à l'examen, mais également en raison des singularités

kenmerken van de nucleaire cyberbeveiliging. Het gaat daarbij in het bijzonder om de link met de “categorisering” (classificatie) van de informatie, met de nationale beveiliging, en met het feit dat de cyberbeveiligingsmaatregelen die moeten worden getroffen desgevallend in sommige opzichten zouden moeten samengaan, zonder exact overeen te komen, met de meer “fysieke” beveiligingsmaatregelen, zoals reeds voorzien in de nucleaire wetgeving.

Het “NIS”-wetsontwerp heeft evenwel betrekking op het “niet-nucleaire” gedeelte van een nucleaire krachtcentrale, “vanaf de turbine” zou men kunnen stellen. Voor dit gedeelte heeft het FANC ook een controlerende rol. De NIS-wet kadert in het perspectief om de onderbreking van een essentiële dienst te voorkomen (de levering van elektriciteit), terwijl het wetsontwerp met betrekking tot de nucleaire cyberbeveiliging zich situeert in het kader van de nucleaire beveiliging (bv. de radiologische uitstoot voorkomen).

Het wetsontwerp bevat wel verwijzingen naar bepaalde artikelen van het wetsontwerp tot omzetting van de NIS-richtlijn. Deze verwijzingen zijn gebaseerd op het voorontwerp van de betreffende wet. Bij de stemming en de publicatie zal dus moeten worden nagegaan of zij nog steeds juridisch-technische correct en coherent zijn.

C. **Krachtlijnen**

De belangrijkste bepalingen van het wetsontwerp bestaan in de machtiging van de Koning om maatregelen inzake nucleaire cyberbeveiliging te bepalen die aan de betrokken operatoren zullen worden opgelegd. Het wetsontwerp voorziet daarenboven dat het FANC verantwoordelijk zal zijn voor de inspecties en controles met betrekking tot de nucleaire cyberbeveiligingsmaatregelen.

Deze maatregelen zullen zo veel mogelijk uitgewerkt worden in samenwerking met de andere betrokken overheden, en in ieder geval in samenwerking met het Crisiscentrum en het Centrum voor *Cybersecurity* België.

1. ***Inrichtingen***

De nucleaire cyberbeveiliging wordt gedefinieerd als de beveiliging van de netwerk- en informatiesystemen:

1. van de nucleaire installaties;

de la cybersécurité nucléaire. Il s’agit à cet égard spécialement de ses liens avec la “catégorisation” (classification) de l’information, avec la sécurité nationale, et le fait que les mesures de cybersécurité qui devront être prises devraient, le cas échéant, sous certains aspects, voisiner, sans exactement coïncider, avec les “mesures de protection physique”, ainsi que le prévoit déjà la législation dans le domaine nucléaire.

Le projet de loi relatif à la sécurité des réseaux et des systèmes d’information porte toutefois sur la partie “non nucléaire” des centrales nucléaires, c’est-à-dire sur la partie située “à partir de la turbine”, en quelque sorte. L’AFCN exerce également un contrôle sur cette partie. La loi relative à la sécurité des réseaux et des systèmes d’information s’inscrit dans la perspective de la prévention de l’interruption d’un service essentiel (fourniture d’électricité), tandis que le projet de loi relatif à la cybersécurité nucléaire s’inscrit dans le cadre de la sécurité nucléaire (prévention d’émissions radiologiques, par exemple).

Le projet de loi à l’examen renvoie cependant à certains articles du projet de loi transposant la directive relative à la sécurité des réseaux et des systèmes d’information. Ces renvois sont toutefois basés sur l’avant-projet de la loi concerné. Lors du vote et de la publication, il conviendra dès lors de vérifier s’ils sont encore corrects et cohérents sur le plan légistique.

C. **Lignes de force**

Les dispositions essentielles du projet de loi à l’examen résident dans l’habilitation permettant au Roi de prendre des mesures de cybersécurité nucléaire qui s’imposeront aux opérateurs concernés. Le projet de loi à l’examen prévoit en outre que l’AFCN sera responsable des inspections et contrôles des mesures de cybersécurité nucléaire.

Dans la mesure du possible, ces mesures seront élaborées en collaboration avec les autres autorités concernées, en tout cas avec le Centre de crise et le Centre pour la Cybersécurité Belgique.

1. ***Établissements***

La cybersécurité nucléaire est définie comme étant la sécurité des réseaux et des systèmes d’information:

1. des installations nucléaires;

2. van de inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, en

3. van de inrichtingen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is (X-stralen).

2. ***Netwerken en systemen***

De bedoelde netwerk- en informatiesystemen van de betrokken installaties en inrichtingen omvatten hoofdzakelijk de netwerk- en informatiesystemen in verband met:

1. de fysieke beveiliging, de beveiliging van radioactieve stoffen, de beveiliging van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is;

2. de nucleaire en radiologische veiligheid, en

3. de stralingsbescherming.

Ze zijn evenwel niet noodzakelijk beperkt tot deze opsomming. Het spreekt bijvoorbeeld voor zich dat een printer op zich niets te zien heeft met deze punten, maar dat deze (afhankelijk van de locatie) onrechtstreeks wel gebruikt zou kunnen worden voor een cyberaanval. Het is de Koning die zal bepalen welke netwerken en systemen van de installatie of de inrichting in aanmerking moeten worden genomen.

3. ***Samenwerking van het FANC met andere autoriteiten***

Het wetsontwerp machtigt de Koning om autoriteiten aan te duiden, hoofdzakelijk om advies te verstekken, om informatie uit te wisselen of om meldingen van cyberincidenten te ontvangen. Het betreft het Centrum voor *Cybersecurity* België (CCB), met inbegrip van zijn dienst het *Computer Emergency Response Team* (CERT.be), het Crisiscentrum, of nog andere bestaande, of nog op te richten instellingen.

Het is uiteraard de bedoeling om het mogelijk te maken dat de bevoegde nationale autoriteiten op het gebied van de cyberbeveiliging, de kritieke infrastructuren, of het crisisbeheer ook hun medewerking, hun advies en ervaring ter beschikking kunnen stellen van de nucleaire cyberbeveiliging.

4. ***Machtigingen aan de Koning***

Het wetsontwerp voorziet in meerdere machtigingen aan de Koning.

2. des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, et

3. des établissements où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives (rayons X)

2. ***Réseaux et systèmes***

Les réseaux et systèmes d'information considérés dans les installations et établissements visés incluent principalement les réseaux et systèmes d'information en rapport avec:

1. la protection physique, la sécurité pour les substances radioactives, la sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

2. la sûreté nucléaire et radiologique, et

3. la radioprotection.

Ils ne se limitent toutefois pas nécessairement à cette énumération. Il va sans dire, par exemple, qu'une imprimante ne sert pas intrinsèquement à exercer ces activités, ce qui n'empêche toutefois pas qu'elle puisse (en fonction de son emplacement) être utilisée indirectement dans le cadre d'une cyber-attaque. Il reviendra au Roi de déterminer les réseaux et systèmes de l'installation ou de l'établissement devant être pris en considération.

3. ***Collaboration entre l'AFCN et d'autres autorités***

Le projet de loi habilite le Roi à désigner des autorités, essentiellement pour rendre des avis, échanger des informations ou recevoir des notifications de cyberincidents. Il s'agit du Centre pour la Cybersécurité Belgique (CCB), y compris son service, la "*Computer Emergency Response Team*" (CERT.be), du Centre de crise ou encore d'autres institutions existantes ou qui pourraient être créées à l'avenir.

L'idée est évidemment de faire en sorte que la cybersécurité nucléaire puisse également bénéficier de la collaboration, de l'avis et de l'expérience d'autorités publiques compétentes en matière de cybersécurité, d'infrastructures critiques ou de gestion de crise.

4. ***Habilitations au Roi***

Le projet de loi prévoit plusieurs habilitations au Roi.

De Koning zal alle netwerk- en informatiesystemen van de bedoelde installaties in categorieën moeten indelen, voor zover deze netwerk- en informatiesystemen de controle of de veiligstelling van het beschermde materiaal en de beschermde toestellen en installaties waarborgen of steunen.

De voorkeur moet daarbij uitgaan naar een graduele aanpak. De Koning kan in dat verband, naargelang de gradatie van de cyberrisico's, de nucleaire en de niet-nucleaire infrastructuren indelen op basis van hun al dan niet kritieke aard.

Op de netwerk- en informatiesystemen met de hoogste cyberrisico's zullen "nucleaire cyberbeveiligingsmaatregelen" van toepassing zijn die door de Koning worden bepaald. Voor de netwerk- en informatiesystemen met de laagste cyberrisico's gelden nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer, waarvan de principes door het Agentschap zullen worden vastgelegd.

De Koning bepaalt bovendien het beveiligingsniveau van die netwerk- en informatiesystemen.

Tevens zal hij de noodzakelijke en evenredige nucleaire cyberbeveiligingsmaatregelen bepalen voor het beheer van de cyberrisico's van de categorieën van netwerk- en informatiesystemen die, in het licht van de bestaande kennis, met de hoogste cyberrisico's overeenstemmen, en om cyberincidenten die hierop van invloed kunnen zijn te voorkomen, of om de gevolgen ervan te beperken.

Deze maatregelen bepalen met name hoe cyberincidenten met een aanmerkelijke impact door de exploitant moeten worden gemeld aan het Agentschap en aan de door de Koning aangewezen autoriteiten (het CCB, het Crisiscentrum enzovoort).

Ten slotte zal de Koning de erkenningsprocedure voor de nucleaire cyberbeveiligingsmaatregelen bepalen.

II. — **ALGEMENE BESPREKING**

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

De heer Eric Thiébaut (PS) benadrukt dat de werkgroep waartoe hij behoort uiteraard achter elke maatregel ter versterking van de nucleaire cyberbeveiliging staat, te meer daar de *stress tests* na de kernramp van Fukushima bepaalde kwetsbare punten hebben blootgelegd.

Le Roi devra répartir en catégories tous les réseaux et systèmes d'information des installations visées, dans la mesure cependant où ces réseaux et systèmes assurent ou appuient le contrôle ou la sécurisation des matières, appareils et installations protégées.

C'est une logique d'approche graduée qui doit prévaloir ici. Le Roi pourrait distinguer à cet égard, en fonction des degrés de cyber-risques, le nucléaire critique, le nucléaire non-critique, le non-nucléaire critique et le non-nucléaire non-critique.

Les réseaux et système correspondant aux cyber-risques les plus élevés feront l'objet de "mesures de cybersécurité nucléaire" déterminées par le Roi. Les réseaux et système correspondant au cyber-risque le moins élevé feront l'objet de mesures de cybersécurité nucléaire de gestion prudente dont l'Agence déterminera les principes.

Le Roi détermine en outre le niveau de sécurité de ces réseaux et systèmes d'information.

Il déterminera également les mesures de cybersécurité nucléaire nécessaires et proportionnées pour gérer les cyber-risques des catégories des réseaux et systèmes d'information correspondant aux cyber-risques les plus élevés, compte tenu de l'état des connaissances, et pour prévenir les cyber-incidents pouvant les affecter ou en limiter l'impact.

Ces mesures règlent notamment la notification à l'Agence ainsi qu'aux autorités désignées par le Roi (CCB, Centre de Crise, …) des cyber-incidents ayant un impact significatif que l'exploitant doit effectuer.

Enfin, le Roi déterminera la procédure d'agrément des mesures de cybersécurité nucléaire.

II. — **DISCUSSION GÉNÉRALE**

A. **Questions et observations des membres**

M. Eric Thiébaut (PS) souligne que le groupe auquel il appartient souscrit évidemment à toute mesure visant à renforcer la cybersécurité en matière nucléaire, d'autant plus que les stress tests postérieurs à l'accident nucléaire de Fukushima ont mis en évidence certaines vulnérabilités.

De spreker merkt niettemin op dat de Kamer van volksvertegenwoordigers nu al voor de derde keer moet stemmen over een wetsontwerp over nucleaire aangelegenheden in verband waarmee de Raad van State heeft gewezen op een probleem inzake de delegatie van verordende bevoegdheid aan het FANC. In zijn advies heeft de Raad van State immers de aandacht gevestigd op de gevaren van een dergelijke werkwijze. De Raad wijst erop dat het verlenen van een verordende bevoegdheid aan een openbare instelling in beginsel niet in overeenstemming is met de algemene publiekrechtelijke beginselen omdat aldus geraakt wordt aan het beginsel van de eenheid van de verordende macht en omdat een rechtstreekse parlementaire controle ontbreekt. Bovendien ontbreken de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking en de preventieve controle van de Raad van State, afdeling Wetgeving (DOC 54 3336/001, blz. 37).

Mevrouw Karin Temmerman (sp.a) sluit zich aan bij de opmerkingen van de heer Thiébaut met betrekking tot de Raad van State. Werd met die laatste overleg gepleegd over de vraag of de aan het FANC gedelegeerde bevoegdheid aan de criteria voldoet (cf. DOC 54 3336/001, blz. 37)?

Kan voorts toelichting worden verschaft naar de wetgeving waarnaar in de memorie van toelichting wordt verwezen (DOC 54 3336/001, blz. 9)?

Voorzitter Brecht Vermeulen legt uit dat de data van de regelgeving waar in de memorie wordt verwezen nog niet kunnen worden ingevuld. Het gaat immers om een tweede wetsontwerp, het wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (DOC 54 3340/001) dat in de commissie zal worden besproken.

B. **Antwoord van de minister**

De minister antwoordt dat de delegatie van verordende bevoegdheid aan de FANC zeer beperkt in draagwijdte is: ze is voornamelijk van technische en niet van politieke aard.

Il observe toutefois que c'est la troisième fois que la Chambre des représentants est appelée à voter un projet de loi en matière nucléaire à l'égard duquel le Conseil d'État épingle le problème de la délégation de pouvoir réglementaire à l'AFCN. Dans son avis, le Conseil d'État attire en effet l'attention sur les dangers d'une telle méthode et rappelle que l'attribution d'un pouvoir réglementaire à un organisme public n'est en principe pas conforme aux principes généraux de droit public en ce qu'il est ainsi porté atteinte au principe de l'unité du pouvoir réglementaire et qu'un contrôle parlementaire direct fait défaut. En outre, les garanties dont est assortie la réglementation classique, telles que celles en matière de publication et de contrôle préventif exercé par la section de législation du Conseil d'État, sont absentes (DOC 54 3336/1, p. 37).

Mme Karin Temmerman (sp.a) se rallie aux observations formulées par M. Thiébaut au sujet du Conseil d'État. Le Conseil d'État a-t-il été consulté à propos de la question de savoir si le pouvoir délégué à l'AFCN remplit les critères prévus (*cf.* DOC 54 3336/001, p. 37)?

L'intervenante demande par ailleurs des précisions à propos de la législation à laquelle il est fait référence dans l'exposé des motifs (DOC 54 3336/001, p. 9).

M. Brecht Vermeulen, président, explique que les dates de la réglementation à laquelle renvoie l'exposé des motifs ne peuvent pas encore être complétées dès lors que cette réglementation fait l'objet d'un deuxième projet de loi (projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (DOC 54 3340/001)) qui doit encore être examiné en commission.

B. **Réponse du ministre**

Le ministre répond que la délégation de pouvoir réglementaire à l'AFCN ne présente qu'une portée très limitée, principalement technique et non politique.

III. — **ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN**

Artikel 1

Dit artikel bepaalt de grondwettelijke grondslag van het wetsontwerp.

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Art. 2

Over dit artikel worden geen opmerkingen gemaakt.

Het wordt eenparig aangenomen.

Art. 2/1 *(nieuw)*

De heer Brecht Vermeulen (N-VA) dient amendement nr. 1 (DOC 54 3336/002) in, tot wijziging van artikel 3 van de wet van 6 december 2018 houdende wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle met betrekking tot de milieueffectbeoordeling.

De tekst van deze bepaling stond oorspronkelijk in artikel 7 van wetsontwerp DOC 54 3335/001 dat na de stemming in commissie werd verplaatst en artikel 3 is geworden (zie DOC 54 3335/003, blz.10). Door deze verplaatsing is de vermelding van het opschrift van de gewijzigde wet (namelijk 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) volledig verdwenen. Om hieraan te verhelpen wordt voorgesteld om in het onderhavige wetsontwerp een nieuw artikel in te voegen tot wijziging van artikel 3 van de voornoemde wet van 6 december 2018. Het gaat dus om een louter technische verbetering.

Gezien de draagwijdte van dit amendement moet deze bepaling vóór het huidige artikel 5 (inwerkingtreding) worden ingevoegd.

*
* *

Amendement nr. 1 tot invoeging van een artikel 2/1 wordt eenparig aangenomen.

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

Article 1er

Cet article qui définit la base constitutionnelle du projet de loi ne donne lieu à aucun commentaire.

L'article est adopté à l'unanimité.

Art. 2

Cet article n'appelle aucun commentaire.

Il est adopté à l'unanimité.

Art. 2/1 *(nouveau)*

M.Brecht Vermeulen (N-VA) dépose l'amendement n° 1 (DOC 54 3336/002) qui vise à modifier l'article 3 de la loi du 6 décembre 2018 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, en ce qui concerne l'évaluation des incidences sur l'environnement.

Le texte de cette disposition figurait initialement dans l'article 7 du projet de loi 54 3335/1, qui après le vote en commission a été déplacé et est devenu l'article 3 (voir DOC 54 3335/3, p.10). En raison de ce déplacement, l'intitulé de la loi modifiée (à savoir 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) a complètement disparu. Pour y remédier, il est proposé d'insérer dans le présent projet de loi un nouvel article modifiant l'article 3 de la loi du 6 décembre 2018 précitée. Il s'agit donc d'une correction purement technique.

Compte tenu de la portée de cet amendement, il conviendra d'insérer la disposition avant l'article 5 actuel (entrée en vigueur).

*
* *

L'amendement n° 1 visant à insérer un article 2/1 est adopté à l'unanimité.

Art. 3 en 4

Over deze artikelen worden geen opmerkingen gemaakt.

Ze worden achtereenvolgens eenparig aangenomen.

Art. 5

De heer Brecht Vermeulen (N-VA) dient *amendement nr. 2* (DOC 54 3336/002) in, tot vervanging van artikel 5. Dit amendement heeft tot doel de inwerkingtreding van het nieuwe artikel 2/1 te doen samenvallen met die van de wet van 6 december 2018 houdende wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle met betrekking tot de milieueffectbeoordeling, namelijk op 16 januari 2019.

Amendement nr. 2 tot vervanging van artikel 5 wordt eenparig aangenomen.

*
* *

Het gehele aldus taalkundig en wetgevingstechnisch verbeterde wetsontwerp wordt eenparig aangenomen.

De rapporteur, *De voorzitters,*

Eric THIÉBAUT Brecht VERMEULEN
Koenraad DEGROOTE a.i.

Bepalingen die een uitvoeringsmaatregel vergen (artikel 78.2 van het Reglement van de Kamer): de artikelen 4 en 6 (vroeger artikel 5).

Art. 3 et 4

Ces articles n'appellent aucun commentaire.

Ils sont successivement adoptés à l'unanimité.

Art. 5

M.Brecht Vermeulen (N-VA) dépose *l'amendement n° 2* (DOC 54 3336/002) qui vise à remplacer l'article 5. Cet amendement vise à faire coïncider l'entrée en vigueur du nouvel article 2/1 avec celle de la loi du 6 décembre 2018 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, en ce qui concerne l'évaluation des incidences sur l'environnement, à savoir le 16 janvier 2019.

L'amendement n° 2 visant à remplacer l'article 5 est adopté à l'unanimité.

*
* *

L'ensemble du projet de loi, tel que corrigé sur le plan légistique et linguistique, est adopté à l'unanimité.

Le rapporteur, *Les présidents,*

Eric THIÉBAUT Brecht VERMEULEN
Koenraad DEGROOTE a.i.

Dispositions nécessitant une mesure d'exécution (article 78.2 du Règlement de la Chambre): articles 4 et 6 (ancien article 5).

Centrale drukkerij – Imprimerie centrale