DOC 54 **3336/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

22 oktober 2018

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

INHOUD

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

22 octobre 2018

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

SOMMAIRE

De regering heeft dit wetsontwerp op 22 oktober 2018 ingediend.	*Le gouvernement a déposé ce projet de loi le 22 octobre 2018.*
De "goedkeuring tot drukken" werd op 24 oktober 2018 door de Kamer ontvangen.	*Le "bon à tirer" a été reçu à la Chambre le 24 octobre 2018.*

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

SAMENVATTING

De belangrijkste bepalingen van het ontwerp dat ter beraadslaging wordt voorgelegd, bestaan in de machtiging aan de Koning om de maatregelen inzake nucleaire cyberbeveiliging te bepalen die aan de betrokken operatoren uit de nucleaire sector worden opgelegd.

Het ontwerp voorziet daarenboven dat het FANC verschillende rollen zal spelen, waaronder een bewustmakingsrol, en verantwoordelijk zal zijn voor de inspecties en controles m.b.t. de nucleaire cyberbeveiligingsmaatregelen, waarbij het een beroep doet op de samenwerking, het advies en de ervaring van de door de Koning aangeduide autoriteiten, om hun deskundigheid inzake cyberbeveiliging, kritieke infrastructuren of crisisbeheer te benutten. Het betreft met name het Centrum voor Cybersecurity België ("CCB"), met inbegrip van zijn dienst het "Computer Emergency Response Team" (CERT.be), van het Crisiscentrum.

RÉSUMÉ

Les dispositions essentielles du projet soumis à votre délibération consistent dès lors en l'habilitation au Roi de déterminer des mesures de cybersécurité nucléaire qui s'imposeront aux opérateurs concernés du secteur nucléaire.

Le projet prévoit en outre que l'AFCN jouera divers rôles, y compris de sensibilisation, et sera responsable des inspections et contrôles des mesures de cybersécurité nucléaire. Ce faisant, elle recourt à la collaboration, à l'avis ou à l'expérience des autorités désignées par le Roi afin de bénéficier de leurs compétences en matière de cybersécurité, d'infrastructures critiques ou de gestion de crise. Il s'agit notamment du Centre pour la Cybersécurité Belgique ("CCB"), y compris son service le "Computer Emergency Response Team" (CERT.be), du Centre de Crise.

MEMORIE VAN TOELICHTING

Dames en Heren,

ALGEMENE TOELICHTING

Door de toenemende cyberaanvallen gericht tegen de overheid en de industrie, wordt de cyberbeveiliging, zowel op internationaal als op nationaal gebied, meer en meer een prioriteit. Deze dreigingen, in het bijzonder dan in de nucleaire sector en bij de nucleaire toepassingen, die steeds vaker in de actualiteit komen, leiden tot een groeiende bezorgdheid bij de regeringen en de veiligheidsautoriteiten. Zo is de regering er zich terdege van bewust dat de Belgische nucleaire installaties een mogelijk doelwit vormen voor cyberaanvallen en dat, hetzelfde, meer in het algemeen, geldt voor de inrichtingen waar ioniserende straling wordt gebruikt.

De nucleaire cyberbeveiliging op internationaal vlak

Op internationaal gebied gaat er meer en meer aandacht naar de cyberbeveiliging in het algemeen. Het World Economic Forum (WEF) heeft zo, op 24 januari 2018, op de laatste jaarlijkse vergadering, aangekondigd dat er een Global Centre for Cybersecurity zal worden opgericht, dat, onder zijn auspiciën, kan bijdragen tot de veiligheid en de beveiliging van de wereldwijde cyberspace. Het WEF heeft inderdaad vastgesteld dat de cyberbeveiliging een van de belangrijkste uitdagingen op wereldvlak wordt van onze tijd, dit omwille van de grensoverschrijdende aard van de cyber-aanvallen, waartegen de instanties die zich hiervoor elk afzonderlijk inzetten zich vaak niet opgewassen voelen.

Ook op talrijke internationale fora komt de nucleaire cyberbeveiliging steeds vaker aan bod, zoals bijvoorbeeld op de Nuclear Security Summit, of de IAEA, waar het thema van de cyberbeveiliging meer en meer behandeld wordt als een volwaardige en aparte dimensie van de nucleaire beveiliging. Wij verwijzen in dit verband naar de desbetreffende resoluties van de Algemene Conferentie, de *International Conference on Computer Security in a Nuclear World*, die werd georganiseerd in Wenen van 1 tot 5 juni 2015, het Plan Nucleaire Beveiliging 2018-2021, alsook de verschillende documenten met aanbevelingen hierover die in de *Nuclear Security Series* werden uitgewerkt. Hieruit blijkt ook dat België bijzonder actief is en nauwgezet meewerkt aan de verschillende werkgroepen die deze specifieke aanbevelingen binnen de IAEA ontwikkelen.

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

EXPOSÉ GÉNÉRAL

Suite à la multiplication des cyber-attaques contre des gouvernements et des industries, la cybersécurité apparait toujours plus comme une priorité tant au niveau international que national. Les menaces en la matière, en particulier dans le secteur nucléaire et dans celui des applications nucléaires, fréquemment évoquées dans l'actualité, font l'objet des préoccupations de tous les gouvernements et des autorités de sécurité. Ainsi, le gouvernement est-il tout à fait conscient que les installations nucléaires belges constituent une cible potentielle de cyber-attaques, de même d'ailleurs, de manière plus générale, que les établissements où des rayonnements ionisants sont utilisés.

La cybersécurité nucléaire au plan international

Au plan international, la cybersécurité dans toute sa généralité fait l'objet d'une attention croissante. Le World Economic Forum (WEF) vient ainsi d'annoncer, le 24 janvier 2018, lors de sa dernière assemblée annuelle, la création d'un Global Centre for Cybersecurity, qui, sous ses auspices, pourra contribuer à la sûreté et à la sécurité d'un cyberespace mondial. Le WEF constate en effet que la cybersécurité constitue l'un des défis mondiaux les plus aigus de notre temps, en raison de la nature transfrontières des cyber-attaques, face auxquelles des capacités et des institutions œuvrant de manière isolée peuvent vite s'avérer impuissantes.

Plus spécifiquement, la cybersécurité nucléaire fait également l'objet d'une attention sans cesse accrue dans de nombreux forums internationaux; mentionnons notamment le Nuclear Security Summit, ou encore l'AIEA, au sein de laquelle le thème de la cybersécurité nucléaire est de plus en plus souvent abordé, et est de plus en plus traité comme une dimension à part entière de la sécurité nucléaire. Nous renvoyons à ce sujet aux résolutions pertinentes de la Conférence générale, à *l'International Conference on Computer Security in a Nuclear World*, qui s'est tenue à Vienne du 1er au 5 juin 2015, au Plan de Sécurité nucléaire 2018-2021, ainsi qu'aux différents documents de recommandations sur la question élaborés dans les *Nuclear Security Series*; soulignons que la Belgique se montre particulièrement active et attentive au sein des divers groupes de travail qui, dans le giron de l'AIEA, élaborent ces recommandations spécifiques.

Het wettelijk stelsel van de nucleaire cyberbeveiliging in België – Genese van het project

Het wettelijk stelsel van de cyberbeveiliging van de nucleaire sector in België is hoofdzakelijk opgebouwd vanuit de fysieke beveiliging en de nucleaire beveiliging, omwille van de hieronder aangehaalde redenen.

Dit is een van de redenen waarom de nucleaire sector slechts gedeeltelijk aansluit op de mechanismen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren die voorziet in de omzetting van de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren, die beveiligings- en meldingsverplichtingen voorziet voor de netwerk- en informatiesystemen voor de exploitanten van (nationale en Europese) kritieke infrastructuren. Deze wet van 1 juli 2011 is niet gericht op de nucleaire installaties als dusdanig en nog minder op alle inrichtingen waarop dit ontwerp van toepassing is, maar heeft uitsluitend betrekking op de elementen van nucleaire installaties die dienen voor de transmissie van elektriciteit en werden aangeduid als kritieke infrastructuren.

Anderzijds werd er op 10 oktober 2014, bij koninklijk besluit, een nationale autoriteit opgericht (het Centrum voor Cybersecurity België “CCB”) die belast werd met de supervisie, de coördinatie en het toezicht op de uitvoering van de Belgische strategie inzake Cybersecurity (goedgekeurd in 2012).

Daarvoor waren de inspanningen van de regering op het gebied van de nucleaire beveiliging al jaren vooral gericht op de versterking van de fysieke beveiligingssystemen van de nucleaire installaties. Het doel hierbij was vooral om elke niet-toegestane toegang tot de nucleaire sites te verhinderen, zodat elke kwaadwillige handeling waarbij kernmateriaal betrokken was, kon worden voorkomen.

Door de wereldwijde toename van de cyberaanvallen tegen regeringen, instanties en de industrie, werd de cyberbeveiliging evenwel een prioriteit. Het is in deze context dat de Belgische bevoegde autoriteiten een proces gelanceerd hadden dat erop gericht was een aantal mogelijke kenmerken van eventuele cyberaanvallen tegen de nucleaire sector te identificeren. Deze aanpak heeft ertoe geleid dat de bijzonderheden van een dreiging en de specifieke risico’s van de nucleaire installaties op ons grondgebied in kaart konden worden gebracht.

Le régime légal de la cybersécurité nucléaire en Belgique – Genèse du présent projet

Le régime légal de la cybersécurité du secteur nucléaire en Belgique s’est constitué essentiellement à partir de la protection physique et de la sécurité nucléaire, pour les raisons développées ci-dessous.

C’est une des raisons pour lesquelles le secteur nucléaire ne s’inscrit que partiellement dans les mécanismes de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, qui transpose la Directive 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l’évaluation de la nécessité d’améliorer leur protection, qui prévoit des obligations de sécurité et de notification pour les réseaux et systèmes d’information pour les exploitants d’infrastructures critiques (nationales et européennes). Cette loi du 1er juillet 2011 ne vise pas en tant que telles les installations nucléaires et moins encore l’ensemble des établissements auxquels s’applique le présent projet, mais vise seulement les éléments des installations nucléaires de puissance qui servent au transport de l’électricité et qui ont été désignés comme constituant une infrastructure critique.

D’autre part, c’est le 10 octobre 2014 que fut créée par arrêté royal une autorité nationale (le Centre pour la Cybersécurité Belgique “ CCB”) chargée de superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de Cybersécurité (adoptée en 2012).

Auparavant, et depuis des années, les efforts du gouvernement en matière de sécurité nucléaire avaient 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 de par le monde 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.

Van bij het begin maakt de Belgische aanpak van de nucleaire cyberbeveiliging deel uit van het specifiek stelsel voor de fysieke beveiliging van de nucleaire installaties en de bescherming van de zogenaamde gecategoriseerde informatie, dat met name betrekking heeft op de fysieke beveiligingsmaatregelen voor nucleaire installaties (cf. koninklijke besluiten van 17 oktober 2011). Deze aanpak is het gevolg van de toepassing, door België, van het Verdrag inzake de fysieke beveiliging van kernmateriaal, zoals gewijzigd. Het gewijzigd Verdrag, dat als doel heeft om op wereldschaal een doeltreffende fysieke beveiliging van het kernmateriaal en nucleaire installaties in te voeren en te handhaven, heeft tevens betrekking op de bescherming van de gevoelige informatie. Daarenboven steunt België het standpunt dat het gewijzigd Verdrag tevens van toepassing is op de cyberspace. Dat is de reden waarom de Belgische geldende regelgeving de nucleaire exploitanten ertoe verplicht om elke vorm van informatie te beschermen die als een "nucleair document" (in de zin van artikel 1*bis* 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) gedefinieerd werd, inclusief deze in elektronische of in digitale vorm. Bijgevolg, en hoewel de termen "cyberbeveiliging" en "cyberaanval" niet letterlijk in de nu geldende wetgeving werden opgenomen, heeft elke nucleaire installatie toch *de lege lata* de verplichting om maatregelen te treffen om deze nucleaire documenten te beschermen.

Algemeen beschouwd zijn de Belgische nucleaire veiligheidsautoriteiten er zich terdege van bewust dat de kerninstallaties, net als trouwens, meer algemeen, de inrichtingen waar ioniserende straling wordt gebruikt, een mogelijk doelwit kunnen vormen voor cyberaanvallen.

Het bewijs hiervan is het feit dat België, op eigen initiatief, het toepassingsgebied van de weerstandstests van 2011 had 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 onderworpen aan weerstandstests – "stress tests" genoemd – in het kader van gezamenlijke Europese initiatieven. In ons land bleef het toepassingsgebied van deze weerstandstest niet beperkt tot de extreme natuurfenomenen, maar werd het uitgebreid tot mogelijke bedreigingen die het gevolg zijn van, al dan niet kwaadwillige, menselijke handelingen, waaronder een cyberaanval. De kwetsbaarheid van de installaties voor cyberaanvallen werd door de exploitanten geanalyseerd en vervolgens door het FANC en Bel V op de betrouwbaarheid ervan geëvalueerd.

Depuis l'origine, 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, qui portent notamment sur les mesures de protection physique des installations nucléaires (cfr. les arrêtés royaux du 17 octobre 2011). 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 telle qu'amendée. La Convention amendée, qui a pour objectifs 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. En outre, la Belgique promeut la position selon laquelle la convention amendée est d'application également dans le cyberespace. C'est la raison pour laquelle la législation en vigueur en Belgique oblige les exploitants nucléaires à protéger tout type d'information définie comme constituant un "document nucléaire" (au sens de l'article 1er bis 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'AFCN) y compris celle qui est disponible sur un support informatique et qui se trouve 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 *de lege lata* l'obligation de prendre des mesures afin de protéger ces documents nucléaires.

De manière générale, les autorités de sécurité belges sont tout à fait conscientes du fait que les installations nucléaires, de même d'ailleurs, de manière plus générale, 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 la catastrophe nucléaire qui a frappé la centrale nucléaire de Fukushima-Daiichi en 2011, les installations nucléaires belges de classe I 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, qu'elles soient ou non malveillantes, 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.

De exploitanten hadden de mogelijkheden onderzocht van een eventueel verlies van de controle over hun centrales, rekening gehouden met de bestaande beveiligingsvoorzieningen. Volgens hun analyses was het verlies van de veiligheidsfuncties van de kerncentrales ten gevolge van een cyberaanval weinig waarschijnlijk, met name gelet op de maatregelen (met inbegrip van de fysieke beveiliging) die voorzien zijn om de informaticasystemen die de veiligheidsfuncties ondersteunen, te beschermen.

Hoewel de evaluatie van het FANC en Bel V deze conclusies grotendeels bevestigde, werden er toch een aantal aandachtspunten geïdentificeerd. In het nationaal rapport over deze stresstests werd er gesteld dat de cyberrisico's van nabij dienden te worden opgevolgd, omdat:

— De kwetsbaarheid en het risico toenemen naarmate de informaticatechnologie van de installaties verder moderniseert.

— De kwetsbaarheid van de industriële systemen van het type *SCADA (Supervisory Control and Data Acquisition)* verhoogt met het opduiken van nieuwe malware die ontwikkeld wordt om zulke systemen aan te vallen.

Bovendien werd de voormelde wet van 15 april 1994 onlangs gewijzigd (cf. wijzigingswet van 13 december 2017) om het wettelijk kader t.a.v. de beveiliging van radioactieve stoffen te verduidelijken en te versterken, alsook voor toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is. Het spreekt voor zich dat de bepalingen m.b.t. de cyberbeveiliging bij deze nieuwe regels moeten aansluiten.

Doel van het wetsontwerp

Rekening gehouden met de dreiging en de hierboven uiteengezette beschouwingen, diende het wettelijk stelsel hoofdzakelijk in twee opzichten verder te worden aangevuld en uitgewerkt: enerzijds mocht het niet worden beperkt tot de nucleaire installaties, maar moest het worden uitgebreid tot alle inrichtingen waar ioniserende straling wordt gebruikt. Anderzijds mogen de maatregelen die door de operatoren moeten worden genomen er niet alleen op gericht zijn om de informatie te beschermen, maar tevens de industriële en technische operaties, gelet op de kwetsbaarheid van de systemen van het type SCADA.

De belangrijkste bepalingen van het ontwerp dat ter beraadslaging wordt voorgelegd, bestaan in de machtiging van de Koning om de maatregelen inzake

Les exploitants avaient étudié les possibilités de perte de contrôle de leurs centrales, compte tenu des dispositions de sécurité existantes. Selon leurs analyses, 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 identifiait plusieurs points d'attention. Le rapport national portant sur ces tests de résistance précisait ainsi que les risques de cybersécurité devaient être suivis minutieusement, dès lors que, notamment:

— la vulnérabilité et le risque augmentent de plus en plus au fur et à mesure de la modernisation de la technologie informatique des installations.

— la vulnérabilité 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.

Par ailleurs, la loi du 15 avril 1994 précitée a été récemment amendée (cfr la loi modificative du 13 décembre 2017) afin de clarifier et de renforcer le cadre législatif à l'égard de la sécurité des substances radioactives et des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives. Il va de soi que des dispositions de cybersécurité doivent faire pendant à ces nouvelles règles.

Objectifs du projet de loi

Compte tenu de la menace et des considérations développées ci-dessus, il convenait 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.

Les dispositions essentielles du projet soumis à votre délibération consistent dès lors en l'habilitation au Roi de déterminer des mesures de cybersécurité

nucleaire cyberbeveiliging te bepalen die aan de betrokken operatoren worden opgelegd en in de machtiging van het Agentschap om de grote lijnen te bepalen voor de nucleaire cyberbeveiligingsmaatregelen inzake het behoedzaam beheer voor de categorieën van netwerken informatiesystemen met de minste risico's.

Het ontwerp voorziet daarenboven dat het FANC verschillende rollen zal spelen, waaronder een bewustmakingsrol, en verantwoordelijk zal zijn voor de inspecties en controles m.b.t. de nucleaire cyberbeveiligingsmaatregelen.

Dit ontwerp is niet bedoeld om de cyberaanvallen te criminaliseren en evenmin ander onbetamelijk gedrag. De desbetreffende conventies en internationale teksten, vooral het Cybercrimeverdrag, dat in Budapest op 23 november 2001 werd ondertekend en, meer algemeen, de Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, het Verdrag inzake de fysieke beveiliging van kernmateriaal (VFBK), zoals herzien, voor wat de nucleaire beveiliging betreft, namelijk internationale normen met een dergelijk perspectief, hebben tot de noodzakelijke toepassingswetten geleid (in dit verband vermelden we de wet van *6 juli 2017 houdende vereenvoudiging, harmonisering, informatisering en modernisering van bepalingen van burgerlijke recht en van burgerlijk procesrecht alsook van het notariaat, en houdende diverse bepalingen inzake justitie,* die een titel 14 bevat *waardoor de richtlijn 2013/40/EU van het Europees Parlement en van de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad* werd omgezet in Belgisch recht, of ook nog *de wet van 23 mei 2013 tot wijziging van het Strafwetboek om het in overeenstemming te brengen met het Internationaal Verdrag betreffende de bestrijding van daden van nucleair terrorisme, gedaan te New York op 14 september 2005*, *en met de Wijziging van het Verdrag inzake externe beveiliging van kernmateriaal, aangenomen te Wenen op 8 juli 2005 door de Conferentie van de Staten die partij zijn bij het Verdrag*).

Er moet hierbij worden verduidelijkt dat dit ontwerp in geen geval een aan de nucleaire sector aangepast omzettingsontwerp is van de zogenaamde "NIS-Richtlijn" (d.w.z. de (EU) 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); dit ontwerp sluit eerder aan op de internationale verdragen m.b.t. de nucleaire beveiliging, onze verschillende internationale "commitments" en de werkzaamheden van de IAEA; het lijkt ons geschikt om aan

nucléaire qui s'imposeront aux opérateurs concernés et en l'habilitation à l'Agence de prévoir les grandes lignes de mesures de cybersécurité nucléaire de gestion prudente pour les réseaux et systèmes présentant moins de risques.

Le projet prévoit en outre que l'AFCN jouera divers rôles , y compris de sensibilisation, et sera responsable des inspections et contrôles des mesures de cybersécurité nucléaire.

Le présent projet de loi n'a pas pour objet de criminaliser les cyber-attaques ou d'autres comportements répréhensibles. Les conventions et textes internationaux pertinents, principalement la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, au plan général, la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, la Convention sur la protection physique des matières et des installations nucléaires telle qu'amendée, pour ce qui concerne la sécurité nucléaire, soit des normes internationales ayant une telle perspective, ont fait l'objet des lois d'application nécessaires (mentionnons *la loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice*, qui comporte un titre 14 *transposant en droit belge la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil*, ou encore la *loi du 23 mai 2013 modifiant le Code pénal afin de le mettre en conformité avec la Convention internationale pour la répression des actes de terrorisme nucléaire, faite à New York, le 14 septembre 2005, et avec l'Amendement de la Convention sur la protection physique des matières nucléaires, adopté à Vienne le 8 juillet 2005 par la Conférence des États parties à la Convention*).

Il doit être précisé que le présent projet ne constitue aucunement un projet de transposition de la Directive dite " NIS" (c'est-à-dire la Directive européenne (UE) 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'information dans l'Union) adapté au secteur nucléaire; se situant plutôt dans la perspective des conventions internationales relatives à la sécurité nucléaire, de nos divers "commitments" internationaux et des travaux de l'AIEA, il nous paraît de nature à

de vereisten van een sector te beantwoorden die een intrinsiek beveiligingsrisico inhoudt, maar niet noodzakelijk een risico op de onderbreking van een essentiële dienst (wat de bedoeling is van de "*wet van XX XX XXXX tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*", hierna "de wet van XX XX XXXX" genoemd).

Naast dit fundamentele verschil in perspectief, beoogt dit wetsontwerp een gelijkaardig maar ander stelsel in te voeren dan wat voorzien is door de wet van XX XX XXXX, die o.a. de omzetting van de Richtlijn" tot doel heeft .

Een dergelijke specifieke en aparte aanpak dringt zich niet alleen op omwille van het huidig kader van de nucleaire cyberbeveiliging (zie hierboven), of van de genese van het huidig ontwerp (zie hierboven), maar tevens omwille van de specifieke kenmerken van de nucleaire cyberbeveiliging, in het bijzonder de link met de "categorisering" (classificatie) van de informatie, met de nationale beveiliging en het feit dat de cyberbeveiligingsmaatregelen die moeten worden getroffen, desgevallend, in sommige opzichten, zouden moeten samengaan met, of deel uitmaken van, of tot uiting komen in de "fysieke beveiligingsmaatregelen", de "beveiligingsmaatregelen voor de radioactieve stoffen, met uitzondering van het kernmateriaal" of de "beveiligingsmaatregelen voor de toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is", in de zin van de wet van 15 april 1994 (zie respectievelijk de artikelen 17*bis*, eerste streepje, 17*quater* 3°) en 17*quinquies* 1°)) van de wet.

Gelet op het bovenstaande doet het evenwel geen afbreuk aan de bijzondere bepalingen van bovenvermelde wet van XX XX XXXX die tegelijk betrekking hebben op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit (zie artikel [[4 § 4]] van deze wet) en de inspectiebevoegdheid m.b.t. de uitvoering ervan door het FANC (zie artikel [[79]] van deze wet waardoor een artikel 15*ter* in de wet van 15 april 1994 wordt ingevoegd).

Tot slot moet worden benadrukt dat in de paragrafen 1 en 4 van artikel 17*sexies* van het ontwerp de Koning gemachtigd is 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"), opgericht bij koninklijk besluit van 10 oktober 2014, met inbegrip van zijn dienst het "Computer Emergency Response Team" (CERT.be), van het Crisiscentrum, opgericht bij koninklijk besluit

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 (ce qui est le propos de la "*loi du XX XX XXXX établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*", ci-après "la loi du XX XX 2018").

Au-delà de cette différence fondamentale de perspective, le projet de loi a pour effet d'introduire un régime proche mais distinct de celui que prévoit la loi du XX XX XXXX , qui a notamment pour portée la transposition de la Directive .

Une telle approche spécifique et distincte s'impose non seulement en raison du cadre actuel de la cybersécurité nucléaire (voir *supra*) ainsi que de la genèse du présent projet (voir *supra*), mais également en raison des singularités de la cybersécurité nucléaire, spécialement 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 pourraient, le cas échéant, sous certains aspects, voisiner avec, ou constituer ou ressortir des "mesures de protection physique", des "mesures de sécurité des substances radioactives autres que les matières nucléaires" ou des "mesures de sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives", au sens de ces termes dans la loi du 15 avril 1994 (voir respectivement les articles 17*bis* premier tiret, 17*quater* 3°) et 17*quinquies* 1°)) de la loi).

Cela étant, les dispositions particulières de la susdite loi du XX XX XXXX selon lesquelles elle régit à la fois les éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité (voir article [[4 § 4]] de cette loi) et la compétence d'inspection de sa bonne exécution par l'AFCN (voir article [[79]] de cette loi, qui insère un article 15*ter* dans la loi du 15 avril 1994) ne sont pas affectées.

Soulignons enfin qu'aux paragraphes 1er et 4 de l'article 17*sexies*, le projet habilite le Roi à désigner des autorités, essentiellement pour rendre des avis, échanger des informations ou recevoir des notifications de cyber-incidents. Il s'agit du Centre pour la Cybersécurité Belgique ("CCB"), créé par l'arrêté royal du 10 octobre 2014, y compris son service le "Computer Emergency Response Team" (CERT.be), du Centre de Crise, créé par l'Arrêté royal du 18 avril 1988 "portant création du Centre gouvernemental de Coordination

van 18 april 1988 “tot oprichting van het coördinatie- en Crisiscentrum van de regering” en waarbij de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren (zie haar artikel 3,1°) een fundamentele rol speelt inzake beveiliging en bescherming van de kritieke infrastructuren, of nog van andere bestaande, of nog op te richten instellingen.

Het is natuurlijk 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.

ARTIKELSGEWIJZE TOELICHTING

Artikel 2

Artikel 2 van dit ontwerp voegt 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, in artikel 1 de definities toe die betrekking hebben op de nucleaire cyberbeveiliging.

De definities van de termen “netwerk- en informatiesysteem”, “beveiliging van netwerk- en informatiesystemen”, “cyberincident” en “cyberrisico” sluiten aan bij de desbetreffende definities van de wet van XX XX XXXX.

De definities “nucleaire cyberbeveiliging” en “nucleaire cyberbeveiligingsmaatregelen” zijn daarentegen specifiek voor dit ontwerp.

De nucleaire cyberbeveiliging wordt beschreven als het feit dat de netwerk- en informatiesystemen van de betrokken installaties en inrichtingen beschermd zijn tegen gevaar of schade veroorzaakt door misbruik, verstoring of uitval van deze netwerk- en informatiesystemen. Dit gevaar of deze schade bestaan uit (1) de beperking van de beschikbaarheid en/of betrouwbaarheid van netwerk- en informatiesystemen; (2) de schending van de vertrouwelijkheid van de in netwerk- en informatiesystemen opgeslagen informatie of van de via netwerk- en informatiesystemen verspreide informatie; (3) de schade aan de integriteit van de in netwerk- en informatiesystemen opgeslagen informatie of van de via netwerk- en informatiesystemen verspreide informatie.

De bedoelde netwerk- en informatiesystemen van de installaties en inrichtingen omvatten de netwerk- en informatiesystemen m.b.t.:

et de Crise”, et auquel la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (voir son article 3, 1°) attribue un rôle fondamental en matière de sécurité et de protection des infrastructures critiques, ou encore d’autres institutions existantes ou qui pourraient voir le jour.

L’intention est naturellement de permettre 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.

COMMENTAIRE DES ARTICLES

Article 2

L’article 2 du projet insère les définitions propres à la cybersécurité nucléaire à l’article 1er 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’AFCN.

Les définitions des termes “réseau et système d’information”, “sécurité des réseaux et systèmes d’information”, “cyber-incident” et “cyber-risque” sont en ligne avec les définitions correspondantes de la loi du XX XX XXXX.

Les définitions de “cybersécurité nucléaire” et de “mesures de cybersécurité nucléaire” en revanche sont propres au présent projet.

La cybersécurité nucléaire est définie comme le fait, pour les réseaux et systèmes d’information des installations et des établissements visés, d’être protégés contre les dangers ou les dommages résultant de l’utilisation abusive, de la perturbation ou de la panne de ces réseaux et systèmes. Ces dangers ou dommages consistent en (1.) la limitation de l’accessibilité ou de la fiabilité des réseaux et systèmes d’information; (2.) la violation de la confidentialité de l’information qui y est stockée ou de l’information qu’ils diffusent ou en (3.) l’atteinte à l’intégrité de l’information qui y est stockée ou de l’information qu’ils diffusent.

Les réseaux et systèmes d’information considérés dans les installations et établissements visés incluent les réseaux et systèmes d’information relatifs à:

(a) 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;

(b) de nucleaire en radiologische veiligheid,

(c) de stralingsbescherming,

(d) alsook, zoals vermeld in INFCIRC225Rev 5 van het IAEA (§ 4.10), de boekhouding en de controle van kernmateriaal.

Ze zijn evenwel niet noodzakelijk beperkt tot deze opsomming; het spreekt bijvoorbeeld voor zich dat het netwerk voor de boekhouding en het financieel beheer niets te zien heeft met de punten (a) tot (d), maar dat dit 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 (zie hieronder de toelichting bij ontwerpartikel 17*sexies*, § 1).

Artikel 3

Zoals reeds aan het eind van de algemene beschouwingen hierboven vermeld, is het de bedoeling van dit ontwerp om een gelijkaardig maar ander stelsel in te voeren dan wat door de wet van XX XX XXXX voorzien wordt; vanuit formeel standpunt is het ontwerp geen omzetting van de zogenaamde “NIS-richtlijn” (dat is het onderwerp van de wet van XX XX XXXX), maar kadert hoofdzakelijk in het perspectief van de internationale verdragen met betrekking tot de nucleaire beveiliging. Nochtans, doet huidig ontwerp geen afbreuk aan de bijzondere bepalingen van bovenvermelde wet van XX XX XXXX die tegelijk betrekking hebben op de elementen van een kerninstallatie bestemd voor de industriële elektriciteitsproductie die dienen voor de transmissie van de elektriciteit (zie artikel [[4 § 4]] van deze wet) en de inspectiebevoegdheid m.b.t. de uitvoering ervan door het FANC (zie artikel [[79]] van deze wet waardoor een artikel [15*ter*] in de wet van 15 april 1994 wordt ingevoegd).

Hieruit volgt dat er in de nucleaire installaties twee juridische stelsels die zowel op de fysieke beveiliging als op de cyberbeveiliging betrekking zullen hebben, onverminderd van elkaar van toepassing zullen zijn en naast elkaar zullen bestaan:

— enerzijds is er het stelsel m.b.t. de fysieke beveiliging dat hoofdzakelijk gebaseerd is op de artikels 17*bis* en 17*ter* van de wet van 15 april 1994, en waarbij de cyberbeveiliging wordt gewaarborgd door dit ontwerp;

(a) 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,

(b) la sûreté nucléaire et radiologique,

(c) la radioprotection,

(d) ainsi que, comme le précise l’INFCIRC225Rev 5 de l’AIEA (§ 4.10), la comptabilité et le contrôle des matières nucléaires.

Cependant, ils ne se limitent pas nécessairement à eux; il va sans dire par exemple que le réseau de gestion comptable et financière n’a rien à voir avec ces points (a) à (d), mais pourrait peut-être être utilisé indirectement pour une cyber-attaque. Il reviendra au Roi de déterminer, parmi l’ensemble des réseaux et systèmes de l’installation ou de l’établissement, lesquels d’entre eux doivent être considérés (voir ci-dessous le commentaire de l’article 17*sexies*, § 1er, en projet).

Article 3

Comme mentionné à la fin des considérations générales ci-dessus, le présent projet de loi a pour effet d’introduire un régime proche mais distinct de celui que prévoit la loi du XX XX XXXX; du point de vue formel, le projet ne constitue pas une transposition de la Directive dite “ NIS” (c’est là l’objet de la loi du XX XX XXXX), mais se situe essentiellement dans la perspective des conventions internationales relatives à la sécurité nucléaire . Cela étant, les dispositions particulières de la susdite loi du XX XX XXXX selon lesquelles elle régit à la fois les éléments d’une installation nucléaire destinée à la production industrielle d’électricité qui servent au transport de l’électricité (voir article [[4 § 4 de cette loi]]) et la compétence d’inspection de sa bonne exécution par l’AFCN (voir article [[79]] de cette loi, qui insère un article [15*ter*] dans la loi du 15 avril 1994) ne sont pas affectées par le présent projet.

Il en résulte que dans les installations nucléaires, deux régimes juridiques s’appliqueront l’un sans préjudice de l’autre et coexisteront, au plan de la sécurité physique comme au plan de la cybersécurité:

— d’une part le régime de la protection physique qui trouve sa source essentiellement dans les articles 17*bis* et 17*ter* de la loi du 15 avril 1994, et dont la cybersécurité est assurée par le présent projet;

— anderzijds is er het stelsel dat werd uitgewerkt in toepassing van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, dat betrekking heeft op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit en die werden aangeduid als kritieke infrastructuren en waarvan de cyberbeveiliging wordt gewaarborgd door de wet van XX XX XXXX (zie haar artikel [[4§ 4]]), waardoor het FANC belast wordt met de controle op de toepassing van de wet van 1 juli 2011 zoals gewijzigd door de wet van XX XX XXXX.

Artikel 4

De structuur van artikel 17*sexies* van het ontwerp is gebaseerd op deze van de artikelen 17*bis* (betreffende de fysieke beveiliging), 17*quater* (betreffende de beveiliging van de radioactieve stoffen) en 17*quinquies* (betreffende de beveiliging van toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is).

In het eerste lid van ontwerpartikel 17*sexies* worden, op voorstel van het Agentschap en na advies van de door de Koning aangeduide autoriteiten, vier machtigingen voor de Koning voorzien.

De aanduiding door de Koning van de adviesverlenende autoriteiten moet rekening houden met de opdrachten die werden toegewezen enerzijds aan het Centrum voor Cyberveiligheid België, opgericht door het koninklijk besluit van 10 oktober 2014, en anderzijds, aan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht door het koninklijk besluit van 18 april 1988.

(1) De eerste machtiging voorziet dat de Koning alle netwerk- en informatiesystemen die tot het toepassingsgebied van de nucleaire cyberbeveiliging behoren, zoals dit gedefinieerd werd, in categorieën indeelt, voor zover deze netwerk- en informatiesystemen het beheer, de controle of de veiligstelling van het kernmateriaal, de radioactieve stoffen, of de toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, voor deze installaties of deze inrichtingen, rechtstreeks of onrechtstreeks mogelijk maken, waarborgen of ondersteunen.

De Koning kan in dit verband een onderscheid maken tussen de kritieke aard van de netwerken en systemen, alsook tussen de al dan niet nucleaire aard van de desbetreffende inrichtingen.

— d'autre part le régime établi en application de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, qui porte sur les éléments d'une installation nucléaire destinée à la production industrielle d'électricité, qui servent au transport de l'électricité et qui ont été désignés comme infrastructure critique, et dont la cybersécurité est assurée par la loi du XX XX XXXX (voir son article [[4§ 4]]), l'AFCN y étant chargée du contrôle de l'application de la loi du 1er juillet 2011 telle que modifiée par la loi du XX XX XXXX.

Article 4

La structure de l'article 17*sexies* en projet s'inspire de celle des articles 17*bis* (relatif à la protection physique), 17*quater* (relatif à la sécurité des substances radioactives)et 17*quinquies* (relatif à la sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives).

Le paragraphe premier de l'article 17*sexies* en projet prévoit quatre habilitations au Roi, sur proposition de l'Agence, et après avis donné par les autorités que le Roi désigne.

La désignation par le Roi des autorités appelées à rendre un avis tiendra compte des missions confiées d'une part au Centre pour la Cybersécurité Belgique crée par l'arrêté royal du 10 octobre 2014 et, d'autre part, à la Direction générale Centre de Crise du Service public fédéral Intérieur, créée par l'arrêté royal du 18 avril 1988.

(1) La première habilitation prévoit que le Roi devra répartir en catégories tous les réseaux et systèmes d'information qui appartiennent au champ d'application de la cybersécurité nucléaire telle qu'elle est définie, dans la mesure cependant où ces réseaux et systèmes d'information, pour ces installation ou ces établissements, permettent directement ou indirectement, assurent ou appuient la gestion, le contrôle ou la sécurisation des matières nucléaires, des substances radioactives ou des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives.

Le Roi pourrait distinguer à cet égard le caractère critique des réseaux et systèmes, ainsi que la nature nucléaire ou non des établissements considérés.

De categorisering die zo zal worden doorgevoerd op basis van de gradatie van de cyberrisico's zal, volgens een logica van een graded approach, een onderscheid maken tussen de netwerken en systemen die met de hoogste cyberrisico's overeenstemmen, enerzijds, en waarvoor er nucleaire cyberbeveiligingsmaatregelen in punt 3 voorzien worden, en, anderzijds, de netwerk- en informatiesystemen die met het laagste cyberrisico overeenstemmen en waarvoor de in § 2 voorziene nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer voorzien worden.

(2) Bij de bepaling van het beveiligingsniveau van de netwerk- en informatiesystemen wordt rekening gehouden met de diverse classificaties van fysieke beveiligingssystemen en de veiligheidsfuncties.

(3) de Koning bepaalt enkel de nucleaire cyberbeveiligingsmaatregelen voor de netwerk- en informatiesystemen die met het hoogste cyberrisico overeenstemmen.

Deze nucleaire cyberbeveiligingsmaatregelen worden bepaald "onverminderd de toepassing van het internationaal stelsel van de waarborgen"; met deze formulering wordt verwezen naar de verplichtingen die aan België werden opgelegd uit hoofde van de veiligheidscontrole vermeld in hoofdstuk VII van het Verdrag tot oprichting van de Europese Gemeenschap voor Atoomenergie (Euratom) en uit hoofde van de waarborgen in de zin van artikel III, paragrafen 1 en 4, van het Verdrag van 1 juli 1968 inzake de niet-verspreiding van kernwapens.

In navolging van de wet van XX XX XXXX (zie haar artikel [[20]]en volgende) stelt dit artikel van het ontwerp dat de Koning nucleaire cyberbeveiligingsmaatregelen bepaalt die met name van toepassing zijn op de melding aan het Agentschap en aan de door de Koning aangeduide autoriteiten van cyberincidenten met een significante impact, die door de exploitant van de door deze maatregelen bedoelde installatie of inrichting moet worden gedaan. In dit opzicht kan de Koning incidentieniveaus of drempels bepalen die noodzakelijkerwijze een significante impact moeten hebben.

Bovendien voorziet het ontwerpartikel dat de Koning de adequate uitwisseling regelt tussen het Agentschap en de door de Koning aangeduide autoriteiten (rekening houdend met bovenvermelde overwegingen voor hun aanduiding) van de gegevens waarover zij beschikken in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd. De gegevens en de informatie die zouden worden uitgewisseld, zijn met name die die het Agentschap of de aangeduide autoriteiten van buitenlandse autoriteiten of internationale organisaties zouden

La catégorisation qui sera ainsi effectuée en fonction des degrés de cyber-risques distinguera, selon une logique d'approche graduée, d'une part les réseaux et système correspondant aux cyber-risques les plus élevés, qui feront l'objet de mesures de cybersécurité nucléaire prévues au point 3, et d'autre part les réseaux et système correspondant au cyber-risque le moins élevé, qui feront l'objet de mesures de cybersécurité nucléaire de gestion prudente mentionnées au § 2.

(2) Le niveau de sécurité des réseaux et systèmes pourra être déterminé en prenant en compte les diverses classifications des systèmes de protection physique et des fonctions de sûreté.

(3) Seuls font l'objet de mesures de cybersécurité nucléaire déterminées par le Roi les réseaux et systèmes d'informations présentant les cyber-risques les plus élevés.

Ces mesures de cybersécurité nucléaire sont prises "sans préjudice de l'application du régime international de garanties"; par cette formulation, il est renvoyé aux obligations qui incombent à la Belgique en vertu du contrôle de sécurité établi par le chapitre VII du Traité instituant la Communauté européenne de l'Energie atomique et en vertu des garanties au sens de l'article III, paragraphes 1er et 4, du Traité du 1er juillet 1968 sur la non-prolifération des armes nucléaires.

A l'instar de la loi du XX XX XXXX (voir son article [[20]]et suivants), l'article en projet dispose que le Roi détermine des mesures de cybersécurité nucléaire qui règlent notamment la notification à l'Agence ainsi qu'aux autorités que le Roi désigne, des cyber-incidents ayant un impact significatif que l'exploitant d'une installation ou d'un établissement visé par ces mesures doit effectuer. A cet égard, le Roi pourrait établir des niveaux d'incidence ou des seuils, constituant nécessairement un impact significatif.

Par ailleurs, l'article en projet prévoit que le Roi règle l'échange adéquat entre l'Agence et les autorités qu'il désigne (en tenant compte des considérations précitées pour leur désignation) des données qu'elles possèdent sur les cyber-risques et sur les cyber-incidents auxquels l'exploitant est ou peut être confronté. Ces données et informations qu'il s'agirait d'échanger seraient en particulier celles que l'Agence ou les autorités désignées seraient amenées à recevoir d'autorités étrangères ou d'organisations internationales, ou encore celles qui concernent le Cyberplan d'urgence nationale ou

moeten ontvangen, of die die in verband staan met het nationaal Cybernoodplan of het Cyber Security Early Warning System. Het spreekt voor zich dat dergelijke uitwisselingen deel zouden moeten uitmaken van het positieve juridische kader, meer bepaald de relevante internationale verdragen, de regels met betrekking tot het beroepsgeheim, de classificatie en categorisering van bepaalde gegevens, en de regels met betrekking tot de bescherming van medische gegevens.

4)Punt 4 stelt dat de Koning de erkenningsprocedure voor de nucleaire cyberbeveiligingsmaatregelen bedoeld in punt 3 bepaalt. Het is dan ook wenselijk dat deze procedure rekening houdt met de snelle evolutie van de technieken, door bijvoorbeeld de verplichting te voorzien om bepaalde beveiligingsniveaus te handhaven, eerder dan zich te focussen op de strikte conformiteit van een dossier voor een erkenningsaanvraag die snel verouderd zou kunnen raken.

Lid 2 van ontwerpartikel 17*sexies* voorziet dat het Agentschap de principes bepaalt voor de nucleaire cyberbeveiligingsmaatregelen m.b.t. het behoedzaam beheer van die categorieën van netwerk- en informatiesystemen die met het laagste cyberrisico overeenstemmen. Er wordt hierbij verwezen naar de bemerkingen bij punt 1°, in de eerste lid, voor de *ratio legis* m.b.t. het onderscheid op basis van de gradatie van de cyberrisico's. Het feit dat deze taak aan het Agentschap wordt toevertrouwd voor de netwerk- en informatiesystemen die met het laagste cyberrisico overeenstemmen, drong zich des te meer op daar het getuigt van goed bestuur om hierbij een parallel te trekken met de "fysieke" beveiliging van de categorieën van radioactieve stoffen die met het laagste risico overeenstemmen, waarvan de principes, overeenkomstig het 2e lid van artikel 17*quater*, onder het toepassingsgebied van het Agentschap vallen.

Ingevolge de bemerking 4.2. van de Raad van State, moet worden verduidelijkt dat de maatregelen inzake behoedzaam beheer als dusdanig geval per geval moeten worden bepaald, rekening gehouden met de specificiteiten en de omstandigheden, het zou zeer moeilijk zijn voor het Agentschap om nu iets anders te bepalen dan de grote lijnen en enkele "principes" ter zake. Deze delegatie van verordenende bevoegdheid aan het FANC heeft bijgevolg slechts een zeer beperkte, hoofdzakelijk technische en niet-beleidsmatige draagwijdte.

Lid 3 van ontwerpartikel 17*sexies* heeft betrekking op de eventuele erkenningsvoorwaarden. Deze bepaling is in zeer grote mate gebaseerd op deze van het huidige 3e lid van artikel 17*quater*. Er wordt in dit verband verwezen naar de bemerkingen bij deze bepaling in de memorie van toelichting bij de wet van 13 december 2017 houdende wijziging van de wet van 15 april 1994.

le Cyber Security Early Warning System. Il va sans dire que de tels échanges devraient s'inscrire dans le cadre légal positif, en particulier les conventions internationales pertinentes, les règles relatives au secret professionnel, à la classification et à la catégorisation de certaines informations, et celles relatives à la protection des données médicales.

4) Le point 4 dispose que le Roi détermine la procédure d'agrément des mesures de cybersécurité nucléaire visées au point 3. Il conviendrait que cette procédure prenne en compte les évolutions rapides des techniques, par exemple en assurant surtout une obligation de maintenir des niveaux de sécurité plutôt qu'en se focalisant sur la stricte conformité à un dossier de demande d'agrément qui s'avérerait vite obsolète.

Le paragraphe 2 de l'article 17*sexies* en projet prévoit que l'Agence détermine les principes des mesures de cybersécurité nucléaire de gestion prudente pour les catégories des réseaux et systèmes d'information correspondant au cyber-risque le moins élevé. Il est renvoyé au commentaire du point 1° du paragraphe premier pour la *ratio legis* de la distinction selon le degré de cyber-risque. Confier cette tâche à l'Agence pour les réseaux et systèmes correspondant au cyber-risque le moins élevé s'imposait d'autant plus qu'il est de bonne administration d'assurer un parallélisme de traitement avec la sécurité "physique" des catégories de substances radioactives correspondant au risque le moins élevé, dont les principes relèvent de l'Agence aux termes de l'alinéa 2 de l'article 17*quater*.

Précisons , suite à l'observation 4.2 du Conseil d'État, que les mesures de gestion prudentes en tant que telles devant être déterminées au cas par cas, compte tenu des spécificités et des circonstances, il serait malaisé pour l'Agence de déterminer autre chose que de grands axes et quelques "principes" en la matière. Ainsi, cette délégation de pouvoir réglementaire à l'A.F.C.N. ne présente qu'une portée très limitée, principalement technique et non politique.

Le paragraphe 3 de l'article 17*sexies* en projet porte sur les éventuelles conditions des agréments. Cette disposition s'inspire très fortement de celle qui figure actuellement à l'alinéa 3 de l'article 17*quater*. Il est renvoyé à ce sujet aux commentaires de cette disposition dans l'exposé des motifs de la loi du 13 décembre 2017 portant modification de la loi du 15 avril 1994.

Lid 4 van ontwerpartikel 17*sexies* voorziet verschillende rollen voor het Agentschap. Zo wordt er op het einde van het algemeen gedeelte van deze memorie van toelichting m.b.t. de door de Koning aangeduide autoriteiten vermeld dat het vanzelfsprekend is dat het Agentschap, bij de uitoefening van deze verschillende rollen, een beroep doet op de samenwerking, het advies en de ervaring van deze autoriteiten, om hun deskundigheid inzake cyberbeveiliging, kritieke infrastructuren of crisisbeheer te benutten.

Lid 5 van ontwerpartikel 17*sexies* bepaalt dat artikel 17*sexies* van toepassing is onverminderd (a) de hierboven uiteengezette wettelijke bepalingen betreffende het stelsel van de kritieke infrastructuren (artikelen 15*bis* en 15*ter* van de wet van 15 april 1994 en artikel 4§ 4 van de wet tot omzetting van de NIS-Richtlijn), (b) deze m.b.t. de fysieke beveiliging, de beveiliging van radioactieve stoffen of van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is (artikelen 17*bis*, 17*quater* en 17*quinquies*), en (c) tenslotte van de toepassing van het internationaal stelsel van de waarborgen (waarover hierboven in de bemerking bij punt 3 van het eerste lid meer uitleg werd verstrekt).

Artikel 5

Dit artikel wil gevolg geven aan de bemerking 4.3. van de Raad van State, om te verzekeren dat huidig ontwerp niet in voege treedt voor het ontwerp van de wet van XX XX XXXX “tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

De minister van Veiligheid en Binnenlandse Zaken,

Jan JAMBON

Le paragraphe 4 de l’article 17*sexies* en projet prévoit divers rôles de l’Agence. Ainsi qu’il est mentionné à la fin de la partie générale du présent exposé des motifs à propos des autorités que le Roi désigne, il va de soi que, dans l’exercice de ces divers rôles, l’Agence recourt à la collaboration, à l’avis ou à l’expérience de ces autorités afin de bénéficier de leurs compétences en matière de cybersécurité, d’infrastructures critiques ou de gestion de crise.

Le paragraphe 5 de l’article 17*sexies* en projet précise que l’article 17*sexies* s’applique sans préjudice (a) des dispositions légales exposées ci-dessus relatives au régime des infrastructures critiques (articles 15*bis* et 15*ter* de la loi du 15 avril 1994 et article 4§ 4 de la loi de transposition de la Directive NIS) (b) ni de celles relatives à la protection physique, à la sécurité des substances radioactives ou à celle des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives (articles 17*bis*, 17*quater* et 17*quinquies*),(c) ni , enfin, de l’application du régime international de safeguards (à propos duquel quelques explications sont fournies ci-dessus en commentaire du point 3 du paragraphe premier).

Article 5

Cette disposition entend donner suite à l’observation 4.3. du Conseil d’État, afin d’assurer que l’entrée en vigueur du présent projet ne se fera pas avant celle du projet de loi du XX XX XXXX “établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique”.

Le ministre de la Sécurité et de l’Intérieur,

Jan JAMBON

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

Voorontwerp van wet 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

Artikel 1

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 74 van de Grondwet.

Artikel 2

In artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, gewijzigd bij de wetten van 2 april 2003, 30 maart 2011, 26 januari 2014, 19 maart 2014, 15 mei 2014 en 13 december 2017 worden de volgende definities toegevoegd:

— Nucleaire cyberbeveiligingsmaatregelen

De maatregelen betreffende de beveiliging van netwerk- en informatiesystemen van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, met het oog op de nucleaire cyberbeveiliging.

— Nucleaire cyberbeveiliging

De beveiliging van netwerk- en informatiesystemen van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is.

Netwerk- en informatiesysteem

1. een elektronisch communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

2. een apparaat of groep van permanente of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische bestanddelen van dit apparaat die onder meer de automatisering van een operationeel proces mogelijk maken, alsook de controle op afstand of het verkrijgen van werkingsgegevens in real time;

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

Avant-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

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Article 2

A l'article 1er 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, modifié par les lois du 2 avril 2003, 30 mars 2011, 26 janvier 2014, 19 mars 2014, 15 mai 2014 et 13 décembre 2017 les définitions suivantes sont ajoutées:

"— Mesures de cybersécurité nucléaire

Les mesures relatives à la sécurité des réseaux et des systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives, à des fins de cybersécurité nucléaire.

— Cybersécurité nucléaire

La sécurité des réseaux et systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;

— Réseau et système d'information

1. un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;

2. un dispositif ou un ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation d'un processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel;

3. of digitale gegevens die via de in de punten 1 en 2 bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

— Beveiliging van netwerk- en informatiesystemen

Het vermogen van netwerken en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.

— Cyberincident

Elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen;

— Cyberrisico

Elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen."

Art. 3

In dezelfde wet wordt volgende bepaling toegevoegd aan artikel 15, 4e lid:

"Onverminderd de artikelen 15*bis* en 15*ter* van deze wet is het Agentschap eveneens belast met de controle op de nucleaire cyberbeveiligingsmaatregelen."

Art. 4

In hoofdstuk III van dezelfde wet wordt een afdeling 3*quater* ingevoegd die een artikel 17*sexies* bevat, luidende:

"Afdeling 3*quater*. Bevoegdheid op het gebied van de nucleaire cyberbeveiliging

Art. 17*sexies*. § 1.Op voorstel van het Agentschap en na advies van de door de Koning aangewezen autoriteiten:

1° Verdeelt de Koning de netwerk- en informatiesystemen van de nucleaire installaties, de inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt en de inrichtingen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, voor zover deze netwerk- en informatiesystemen het beheer, de controle of de veiligstelling van het kernmateriaal, de radioactieve stoffen, of de toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, voor deze installaties of deze inrichtingen, rechtstreeks of onrechtstreeks mogelijk maken, waarborgen of ondersteunen, in categorieën, op basis van het cyberrisico dat eraan verbonden is.

3. ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points 1 et 2 en vue de leur fonctionnement, leur utilisation, leur protection et leur maintenance.

— Sécurité des réseaux et des systèmes d'information

La capacité des réseaux et des systèmes d'information de résister, à un niveau de fiabilité donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

— Cyber-incident

Tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.

— Cyber-risques

Toute circonstance ou tout événement raisonnablement identifiable ayant une incidence négative potentielle sur la sécurité des réseaux et des systèmes d'information."

Art. 3

Dans la même loi, la disposition suivante est ajoutée à l'article 15, alinéa 4 :

"Sans préjudice des articles 15*bis* et 15*ter* de la présente loi , l'Agence est également chargée du contrôle des mesures de cybersécurité nucléaire."

Art. 4

Dans le chapitre III de la même loi, il est inséré une section 3*quater* comportant l'article 17*sexies* rédigé comme suit:

"Section 3*quater*. Compétence en matière de cybersécurité nucléaire

Art. 17*sexies*. § 1er. Sur proposition de l'Agence, et après avis des autorités désignées par le Roi:

1° le Roi répartit en catégories , en fonction du cyber-risque qu'ils présentent, les réseaux et systèmes d'information des installations nucléaires, des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, et des établissements où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives, dans la mesure où ces réseaux et systèmes d'information, pour ces installations ou ces établissements, permettent directement ou indirectement, assurent ou appuient la gestion, le contrôle ou la sécurisation des matières nucléaires, des substances radioactives ou des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives.

2° bepaalt de Koning het beveiligingsniveau van de netwerk- en informatiesystemen bedoeld in punt 1);

3° bepaalt de Koning de noodzakelijke en evenredige nucleaire cyberbeveiligingsmaatregelen voor het beheer van de cyberrisico's van de categorieën van netwerk- en informatiesystemen bedoeld in punt 1 die, in het licht van de bestaande kennis, met het hoogste cyberrisico overeenstemmen en voor het voorkomen van cyberincidenten die hierop van invloed kunnen zijn, of om de impact ervan te beperken, onverminderd de toepassing van het internationaal stelsel van de waarborgen. Deze maatregelen regelen met name de melding aan het Agentschap en aan de door de Koning aangewezen autoriteiten, van cyberincidenten met een significante impact die door de exploitant van de door deze maatregelen bedoelde installatie of inrichting moet worden gedaan;

4° regelt de Koning de uitwisseling tussen het Agentschap en de door de Koning aangewezen autoriteiten van de gegevens waarover ze beschikken in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd.

5° bepaalt de Koning de erkenningsprocedure voor de nucleaire cyberbeveiligingsmaatregelen bedoeld in punt 3.

§ 2. Het Agentschap bepaalt, na advies van de door de Koning aangewezen autoriteiten, de principes voor de nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer voor de categorieën van netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, die met het laagste cyberrisico overeenstemmen.

§ 3. Het Agentschap kan de in paragraaf 1, 4°, bedoelde erkenningen aan voorwaarden onderwerpen. Het Agentschap kan deze erkenningen en de hierin opgelegde voorwaarden, te allen tijde, op eigen initiatief en op gemotiveerde wijze, wijzigen of aanvullen, indien deze wijzigingen of aanvullingen bedoeld zijn om de naleving te garanderen van de door of krachtens de wet voorziene eisen inzake de nucleaire cyberbeveiliging en deze wijzigingen of aanvullingen kennelijk gepast, evenredig en billijk zijn.

§ 4. Het Agentschap is voor de netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, belast met:

1° het informeren van de exploitanten van de installaties en inrichtingen bedoeld in paragraaf 1, 1°, over de cyberrisico's waarvan het op de hoogte is en die betrekking hebben op de netwerk- en informatiesystemen, of de daaraan gerelateerde diensten;

2° het verrichten van analyses en technisch onderzoeken ten behoeve van de in de punt 1 bedoelde opdrachten naar aanleiding van cyberrisico's of cyberincidenten, of van elementen die daarop wijzen, die niet bestaan in het onderzoek, of verplichtingen die door de gerechtelijke overheid werden opgelegd met het oog op de identificatie van personen of organisaties die voor deze cyberrisico's en cyberincidenten verantwoordelijk zijn, of daar anderszins aan bijdragen of hebben bijgedragen;

2° le Roi détermine le niveau de sécurité des réseaux et systèmes d'information visés au point 1);

3° le Roi détermine les mesures de cybersécurité nucléaire nécessaires et proportionnées pour gérer les cyber-risques des catégories des réseaux et systèmes d'information visés au point 1 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, sans préjudice de l'application du régime international de garanties. Ces mesures règlent notamment la notification à l'Agence ainsi qu' aux autorités désignées par le Roi, des cyber-incidents ayant un impact significatif que l'exploitant d'une installation ou d'un établissement visé par ces mesures doit effectuer;

4° le Roi règle l'échange entre l'Agence et les autorités désignées par le Roi des données qu'elles possèdent sur les cyber-risques et sur les cyber-incidents auxquels l'exploitant est ou peut être confronté.

5° le Roi détermine la procédure d'agrément des mesures de cybersécurité nucléaire visées au point 3.

§ 2. L'Agence détermine, après avis des autorités désignées par le Roi, les principes des mesures de cybersécurité nucléaire de gestion prudente pour les catégories des réseaux et systèmes d'information visés au paragraphe 1er, 1°,correspondant au cyber-risque le moins élevé.

§ 3. L'Agence peut subordonner les agréments visés au paragraphe 1er, 4°, à des conditions. L'Agence peut en tout temps modifier ou compléter, d'initiative et de manière motivée, ces agréments et les conditions qui leur sont imposées, si ces modifications ou compléments visent à assurer le respect des exigences prévues par ou en vertu de la loi et en relation avec la cybersécurité nucléaire ces modifications ou compléments sont manifestement appropriés, proportionnés et équitables.

§ 4. L'Agence est chargée, pour les réseaux et systèmes d'information visés au paragraphe 1er, 1°:

1°. d'informer les exploitants des installations et des établissements visés au paragraphe 1er, 1°, des cyber-risques dont elle a connaissance et qui sont en lien avec leurs réseaux et systèmes d'information, ou les services connexes;

2°. de réaliser, en présence de cyber-risques ou de cyber-incidents ou de tout élément donnant à penser qu'ils existent, des analyses et des enquêtes techniques bénéficiant aux missions visées au point 1, en dehors de l'instruction ou de devoirs prescrits par l'autorité judiciaire visant à identifier les personnes ou organisations qui sont responsables de ces cyber-risques ou cyber incidents, ou qui y contribuent ou y ont contribué de quelque manière que ce soit.

3° het informeren en sensibiliseren van gebruikers van deze netwerk- en informatiesystemen

Het Agentschap doet hiertoe een beroep op de samenwerking, het advies en de ervaring van de door de Koning aangewezen autoriteiten.

De Koning kan, op voordracht van het Agentschap, dat het advies inwint van de door hem aangewezen autoriteiten, de nadere regelen voor de toepassing van deze paragraaf bepalen.

§ 5. Dit artikel is van toepassing onverminderd de artikelen 15*bis*, 15*ter*, 17*bis*, 17*quater* en 17*quinquies* van deze wet en artikel 4§ 4 van de wet van [xx] tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid en onverminderd de toepassing van het internationaal stelsel van de waarborgen."

3° d'informer et de sensibiliser les utilisateurs de ces réseaux et systèmes d'information

A cette fin, l'Agence recourt à la collaboration, à l'avis et à l'expérience des autorités désignées par le Roi.

Le Roi peut déterminer les modalités de l'application du présent paragraphe sur proposition de l'Agence, qui sollicite l'avis des autorités qu'il désigne.

§ 5. Le présent article s'applique sans préjudice des articles 15*bis*, 15*ter*, 17*bis*, 17*quater* et 17*quinquies* de la présente loi et de l'article 4§ 4 de la loi du [XX] établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et sans préjudice de l'application du régime international de garanties."

Geïntegreerde Impactanalyse

Zie handleiding om deze impactanalyse in te vullen

Indien u vragen heeft, contacteer ria-air@premier.fed.be

Beschrijvende fiche

A. Auteur

- Bevoegd regeringslid > De heer J. Jambon, Min Binnenl zaken
- Contactpersoon beleidscel (Naam, E-mail, Tel. Nr.) > Joris.creemers@ibz.fgov.be 02/504 8518
- Overheidsdienst > FANC
- Contactpersoon overheidsdienst (Naam, E-mail, Tel. Nr.) > Rony Dresselaers, rony.dresselaers@fanc.fgov.be, 02/ 289 20 25, Stephane Célestin, Stéphane.celestin@fanc.fgov.be; 02/289 20 51

B. Ontwerp

- Titel van de regelgeving: **ONTWERP VAN WET 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**
- Korte beschrijving van het ontwerp van regelgeving met vermelding van de oorsprong (verdrag, richtlijn, samenwerkingsakkoord, actualiteit, …), de beoogde doelen van uitvoering.

Op internationaal gebied gaat er meer en meer aandacht naar de cyberbeveiliging in het algemeen.
Ook op de talrijke internationale fora komt de nucleaire cyberbeveiliging steeds vaker aan bod, zoals bijvoorbeeld op de Nuclear Security Summit, of de IAEA, waar het thema van de cyberbeveiliging meer en meer behandeld wordt als een volwaardige en aparte dimensie van de nucleaire beveiliging. Wij verwijzen in dit verband naar de desbettrefende resoluties van de Algemene Conferentie, de *International Conference on Computer Security in a Nuclear World*, die werd georganiseerd in Wenen van 1 tot 5 juni 2015, het Plan Nucleaire Beveiliging 2018-2021, alsook de verschillende documenten met aanbevelingen hierover die in de *Nuclear Security Series* werden uitgewerkt. Hieruit blijkt ook dat België bijzonder actief is en nauwgezet meewerkt aan de verschillende werkgroepen die deze **specifieke aanbevelingen** binnen de IAEA **ontwikkelen**.

Sinds jaren waren de inspanningen van de regering op het gebied van de nucleaire beveiliging vooral gericht op de **versterking van de fysieke beveiligingssystemen** van de nucleaire installaties. Het doel hierbij was vooral om elke niet-toegestane toegang tot de nucleaire sites te verhinderen, zodat elke kwaadwillige handeling waarbij kernmateriaal betrokken was, kon worden vermeden.
Door de **wereldwijde toename van de cyberaanvallen** tegen regeringen, instanties en de industrie, werd de cyberbeveiliging **evenwel een prioriteit**. Het is in deze context dat de Belgische bevoegde **autoriteiten een proces gelanceerd hadden dat erop gericht was een aantal mogelijke kenmerken van eventuele cyberaanvallen tegen de nucleaire sector te identificeren.** Deze aanpak heeft ertoe geleid dat de **bijzonderheden** van een dreiging en de specifieke risico's van de nucleaire installaties op ons grondgebied **in kaart konden worden gebracht.**

Rekening gehouden met de dreiging en de hierboven uiteengezette beschouwingen, diende het wettelijk stelsel hoofdzakelijk in twee opzichten verder te worden aangevuld en uitgewerkt: enerzijds mocht het niet worden beperkt tot de nucleaire installaties, maar moest het worden uitgebreid tot alle inrichtingen waar ioniserende straling wordt gebruikt. Anderzijds mochten de maatregelen die door de operatoren moesten worden genomen er niet alleen op gericht zijn om de informatie te beschermen, maar tevens de industriële en technische operaties, gelet op de kwetsbaarheid van de systemen van het type SCADA.

De belangrijkste bepalingen van het ontwerp dat ter beraadslaging wordt voorgelegd, bestaan in de machtiging van de Koning om de maatregelen inzake nucleaire cyberbeveiliging te bepalen die aan de betrokken operatoren worden opgelegd en in de machtiging van het Agentschap om de grote lijnen te bepalen voor de nucleaire cyberbeveiligingsmaatregelen inzake het behoedzaam beheer voor de categorieën van netwerk- en informatiesystemen met de minste risico's.

Het ontwerp voorziet daarenboven dat het FANC verschillende rolllen zal spelen, waaronder een bewustmakingsrol, en verantwoordelijk zal zijn voor de inspecties en controles m.b.t. de nucleaire cyberbeveiligingsmaatregelen.

Dit ontwerp is niet bedoeld om de **cyberaanvallen te criminaliseren** en evenmin ander onbetamelijk gedrag. De desbetreffende conventies en internationale teksten, vooral dan het Cybercrimeverdrag, dat in Budapest op 23 november 2001 werd ondertekend en, meer algemeen, de Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit **2005/222/JBZ van de Raad**, het Verdrag inzake de fysieke beveiliging van kernmateriaal (VFBK), zoals herzien, voor wat de nucleaire beveiliging betreft, of internationale normen met een dergelijk perspectief, hebben tot de noodzakelijke toepassingswetten geleid (in dit verband vermelden we de wet van *6 juli 2017 houdende vereenvoudiging, harmonisering, informatisering en modernisering van bepalingen van burgerlijke recht en van burgerlijk procesrecht alsook van het notariaat, en houdende diverse bepalingen inzake justitie,* die een titel 14 bevat *waardoor de richtlijn 2013/40/EU van het Europees Parlement en van de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad* werd omgezet in Belgisch recht, of ook nog *de wet van 23 mei 2013 tot wijziging van het Strafwetboek om het in overeenstemming te brengen met het Internationaal Verdrag betreffende de bestrijding van daden van nucleair terrorisme, gedaan te New York op 14 september 2005*, *en met de Wijziging van het Verdrag inzake externe beveiliging van kernmateriaal, aangenomen te Wenen op 8 juli 2005 door de Conferentie van de Staten die partij zijn bij het Verdrag*).

Dit wetsontwerp beoogt een **ander maar zeer gelijkaardig stelsel** in te voeren **dan wat voorzien werd door de omzetting van de zogenaamde "NIS-richtlijn**"(« *wet van XX XX XXXX tot vaststelling van een* ***kader voor de beveiliging van de netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid***»), [die onlangs werd goedgekeurd].

Een dergelijke specifieke en aparte aanpak dringt zich niet alleen op omwille van het huidig kader van de nucleaire cyberbeveiliging (zie hierboven), of van de genese van het huidig ontwerp (zie hierboven), maar tevens omwille van de specifieke kenmerken van de nucleaire cyberbeveiliging, in het bijzonder de link met de « categorisering » (classificatie) van de informatie, met de nationale beveiliging en het feit dat de cyberbeveiligingsmaatregelen die moeten worden getroffen, desgevallend, in sommige opzichten, zouden moeten samengaan met, of deel uitmaken van, of tot uiting komen in de « fysieke beveiligingsmaatregelen», de « beveiligingsmaatregelen voor de radioactieve stoffen, met uitzondering van het kernmateriaal » of de « beveiligingsmaatregelen voor de toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is », in de zin van de wet van 15 april 1994 (zie respectievelijk de artikelen 17bis, eerste streepje, 17quater 3°) en 17quinquies 1°)) van de wet.

Gelet op het bovenstaande doet het evenwel geen afbreuk aan de bijzondere bepalingen van bovenvermelde wet tot omzetting van de NIS-richtlijn die tegelijk betrekking hebben op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit (zie artikel 4 §4 van deze wet) en de inspectiebevoegdheid m.b.t. de uitvoering ervan door het FANC (zie artikel 43 van deze wet waardoor een artikel 15ter in de wet van 15 april 1994 wordt ingevoegd).

- Impactanalyses reeds uitgevoerd > ☐ Ja / X Nee
  Indien ja, gelieve een kopie bij te voegen of de referentie van het document te vermelden .

C. Raadpleging over het ontwerp van regelgeving

- Verplichte, facultatieve of informele raadplegingen:

  Advies IF, Ministerraad

D. Bronnen gebruikt om de impactanalyse uit te voeren

- Statistieken, referentiedocumenten, organisaties en contactpersonen:

  Interne analyse FANC

E. Datum van beëindiging van de impactanalyse

- 28 mei 2018

Impactanalyse formulier

Welke impact heeft het ontwerp van regelgeving op deze 21 thema's?

Een ontwerp van regelgeving zal meestal slechts impact hebben op enkele thema's.

- Er wordt een niet-exhaustieve lijst van trefwoorden gegeven om de inschatting van elk thema te vergemakkelijken zonder hiervoor telkens de handleiding te moeten raadplegen.
  Indien er een positieve en/of negatieve impact is, leg deze uit (gebruik indien nodig trefwoorden) en vermeld welke maatregelen worden genomen om de eventuele negatieve effecten te verlichten/te compenseren.
- Voor de **thema's 3, 10, 11 et 21** worden meer gedetailleerde vragen gesteld.

Kansarmoedebestrijding [1]

Menswaardig minimuminkomen, toegang tot kwaliteitsvolle diensten, schuldenoverlast, risico op armoede of sociale uitsluiting (ook bij minderjarigen), ongeletterdheid, digitale kloof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit (gebruik indien nodig trefwoorden) | X Geen impact

Click here to enter text.

Gelijke Kansen en sociale cohesie [2]

Non-discriminatie, gelijke behandeling, toegang tot goederen en diensten, toegang tot informatie, tot onderwijs en tot opleiding, loonkloof, effectiviteit van burgerlijke, politieke en sociale rechten (in het bijzonder voor kwetsbare bevolkingsgroepen, kinderen, ouderen, personen met een handicap en minderheden).

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Gelijkheid van vrouwen en mannen [3] **X geen impact**

Toegang van vrouwen en mannen tot bestaansmiddelen: inkomen, werk, verantwoordelijkheden, gezondheid/zorg/welzijn, veiligheid, opleiding/kennis/vorming, mobiliteit, tijd, vrije tijd, etc.

Uitoefening door vrouwen en mannen van hun fundamentele rechten: burgerlijke, sociale en politieke rechten.

1. Op welke personen heeft het ontwerp (rechtstreeks of onrechtstreeks) een impact en wat is de naar geslacht uitgesplitste samenstelling van deze groep(en) van personen? Indien geen enkele persoon betrokken is, leg uit waarom.

   Click here to enter text.

   → *Indien er personen betrokken zijn, beantwoord dan volgende vragen:*

   2. Identificeer de eventuele verschillen in de respectieve situatie van vrouwen en mannen binnen de materie waarop het ontwerp van regelgeving betrekking heeft.

      Niet van toepassing

      → *Indien er verschillen zijn, beantwoord dan volgende vraag:*

      3. Beperken bepaalde van deze verschillen de toegang tot bestaansmiddelen of de uitoefening van fundamentele rechten van vrouwen of mannen (problematische verschillen)? [J/N] > Leg uit

         Niet van toepassing

      4. Identificeer de positieve en negatieve impact van het ontwerp op de gelijkheid van vrouwen en mannen, rekening houdend met de voorgaande antwoorden?

         Niet van toepassing

         → *Indien er een negatieve impact is, beantwoord dan volgende vraag:*

         5. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

            Niet van toepassing

Gezondheid [4]

Toegang tot kwaliteitsvolle gezondheidszorg, efficiëntie van het zorgaanbod, levensverwachting in goede gezondheid, behandelingen van

chronische ziekten (bloedvatenziekten, kankers, diabetes en chronische ademhalingsziekten), gezondheidsdeterminanten (sociaaleconomisch niveau, voeding, verontreiniging), levenskwaliteit.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Werkgelegenheid [5]

Toegang tot de arbeidsmarkt, kwaliteitsvolle banen, werkloosheid, zwartwerk, arbeids- en ontslagomstandigheden, loopbaan, arbeidstijd, welzijn op het werk, arbeidsongevallen, beroepsziekten, evenwicht privé- en beroepsleven, gepaste verloning, mogelijkheid tot beroepsopleiding, collectieve arbeidsverhoudingen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Consumptie- en productiepatronen [6]

Prijsstabiliteit of -voorzienbaarheid, inlichting en bescherming van de consumenten, doeltreffend gebruik van hulpbronnen, evaluatie en integratie van (sociale- en milieu-) externaliteiten gedurende de hele levenscyclus van de producten en diensten, beheerpatronen van organisaties.

☐Positieve impact ☐ Negatieve impact ↓ Leg uit | Geen impact

Economische ontwikkeling [7]

Oprichting van bedrijven, productie van goederen en diensten, arbeidsproductiviteit en productiviteit van hulpbronnen/grondstoffen, competitiviteitsfactoren, toegang tot de markt en tot het beroep, markttransparantie, toegang tot overheidsopdrachten, internationale handels- en financiële relaties, balans import/export, ondergrondse economie, bevoorradingszekerheid van zowel energiebronnen als minerale en organische hulpbronnen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Investeringen [8]

Investeringen in fysiek (machines, voertuigen, infrastructuren), technologisch, intellectueel (software, onderzoek en ontwikkeling) en menselijk kapitaal, nettoinvesteringscijfer in procent van het bbp.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | Geen impact

Onderzoek en ontwikkeling [9]

Mogelijkheden betreffende onderzoek en ontwikkeling, innovatie door de invoering en de verspreiding van nieuwe productiemethodes, nieuwe ondernemingspraktijken of nieuwe producten en diensten, onderzoeks- en ontwikkelingsuitgaven.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Blijft op huidige niveau.

Kmo's [10]

Impact op de ontwikkeling van de kmo's.

1. Welke ondernemingen zijn rechtstreeks of onrechtstreeks betrokken? Beschrijf de sector(en), het aantal ondernemingen, het % kmo's (< 50 werknemers), waaronder het % micro-ondernemingen (< 10 werknemers).

Ondernemingen in de nucleaire sector .

→ *Indien er kmo's betrokken zijn, beantwoord dan volgende vraag:*

2. Identificeer de positieve en negatieve impact van het ontwerp op de kmo's.
[N.B. de impact op de administratieve lasten moet bij thema 11 gedetailleerd worden]

het bedrijf wordt beveiligd tegen cyberrisico's, waardoor ook de werkomgeving en de werknemers beter

beveiligd worden

→ *Indien er een negatieve impact is, beantwoord dan volgende vragen:*

3. Is deze impact verhoudingsgewijs zwaarder voor de kmo's dan voor de grote ondernemingen? [J/N] > Leg uit

   Neen, er word teen graded approach toegepast.

4. Staat deze impact in verhouding tot het beoogde doel? [J/N] > Leg uit

   ja, omwille van de graded approach

5. Welke maatregelen worden genomen om deze negatieve impact te verlichten / te compenseren?

   graded approach

Administratieve lasten [11]

Verlaging van de formaliteiten en administratieve verplichtingen die direct of indirect verbonden zijn met de uitvoering, de naleving en/of de instandhouding van een recht, een verbod of een verplichting.

→ *Indien ondernemingen en/of burgers betrokken zijn, beantwoord dan volgende vraag:*

1. Identificeer, per betrokken doelgroep, de nodige formaliteiten en verplichtingen voor de toepassing van de regelgeving. Indien geen enkele onderneming of burger betrokken is, leg uit waarom.

→ *Indien er formaliteiten en/of verplichtingen zijn, beantwoord dan volgende vragen:*

2. Welke documenten en informatie moet elke betrokken doelgroep verschaffen?

   Huidige regelgeving > Ontwerp van regelgeving

3. Hoe worden deze documenten en informatie, per betrokken doelgroep, ingezameld?

   Huidige regelgeving > Ontwerp van regelgeving

4. Welke is de periodiciteit van de formaliteiten en verplichtingen, per betrokken doelgroep?

   Huidige regelgeving > Ontwerp van regelgeving

5. Welke maatregelen worden genomen om de eventuele negatieve impact te verlichten / te compenseren?

   Click here to enter text.

* Invullen indien er momenteel formaliteiten/verplichtingen bestaan.

** Invullen indien het ontwerp van regelgeving formaliteiten/verplichtingen wijzigt of nieuwe toevoegt.

Energie [12]

Energiemix (koolstofarm, hernieuwbaar, fossiel), gebruik van biomassa (hout, biobrandstoffen), energie-efficiëntie, energieverbruik van de industrie, de dienstensector, de transportsector en de huishoudens, bevoorradingszekerheid, toegang tot energiediensten en -goederen.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Mobiliteit [13]

Transportvolume (aantal afgelegde kilometers en aantal voertuigen), aanbod van gemeenschappelijk personenvervoer, aanbod van wegen, sporen en zee- en binnenvaart voor goederenvervoer, verdeling van de vervoerswijzen (modal shift), veiligheid, verkeersdichtheid.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Voeding [14]

Toegang tot veilige voeding (kwaliteitscontrole), gezonde en voedzame voeding, verspilling, eerlijke handel.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Impactanalyse formulier

Klimaatverandering [15]

Uitstoot van broeikasgassen, aanpassingsvermogen aan de gevolgen van de klimaatverandering, veerkracht, energie overgang, hernieuwbare energiebronnen, rationeel energiegebruik, energie-efficiëntie, energieprestaties van gebouwen, winnen van koolstof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Natuurlijke hulpbronnen [16]

Efficiënt beheer van de hulpbronnen, recyclage, hergebruik, waterkwaliteit en -consumptie (oppervlakte- en grondwater, zeeën en oceanen), bodemkwaliteit en -gebruik (verontreiniging, organisch stofgehalte, erosie, drooglegging, overstromingen, verdichting, fragmentatie), ontbossing.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Buiten- en binnenlucht [17]

Luchtkwaliteit (met inbegrip van de binnenlucht), uitstoot van verontreinigende stoffen (chemische of biologische agentia: methaan, koolwaterstoffen, oplosmiddelen, SO_x, NO_x, NH3), fijn stof.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Biodiversiteit [18]

Graad van biodiversiteit, stand van de ecosystemen (herstelling, behoud, valorisatie, beschermde zones), verandering en fragmentatie van de habitatten, biotechnologieën, uitvindingsoctrooien in het domein van de biologie, gebruik van genetische hulpbronnen, diensten die de ecosystemen leveren (water- en luchtzuivering, enz.), gedomesticeerde of gecultiveerde soorten, invasieve uitheemse soorten, bedreigde soorten.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Hinder [19]

Geluids-, geur- of visuele hinder, trillingen, ioniserende, niet-ioniserende en elektromagnetische stralingen, lichtoverlast.

☐ Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Click here to enter text.

Overheid [20]

Democratische werking van de organen voor overleg en beraadslaging, dienstverlening aan gebruikers, klachten, beroep, protestbewegingen, wijze van uitvoering, overheidsinvesteringen.

☐Positieve impact ☐ Negatieve impact ↓ Leg uit | X Geen impact

Beleidscoherentie ten gunste van ontwikkeling [21]

Inachtneming van de onbedoelde neveneffecten van de Belgische beleidsmaatregelen op de belangen van de ontwikkelingslanden.

1. Identificeer de eventuele rechtstreekse of onrechtstreekse impact van het ontwerp op de ontwikkelingslanden op het vlak van: voedselveiligheid, gezondheid en toegang tot geneesmiddelen, waardig werk, lokale en internationale handel, inkomens en mobilisering van lokale middelen (taxatie), mobiliteit van personen, leefmilieu en klimaatverandering (mechanismen voor schone ontwikkeling), vrede en veiligheid. Indien er geen enkelen ontwikkelingsland betrokken is, leg uit waarom.

   Niet van toepassing

   → *Indien er een positieve en/of negatieve impact is, beantwoord dan volgende vraag:*

   2. Verduidelijk de impact per regionale groepen of economische categorieën (eventueel landen oplijsten). zie

bijlage

Niet van toepassing.

→ *Indien er een negatieve impact is, beantwoord dan volgende vraag:*

3. Welke maatregelen worden genomen om de negatieve impact te verlichten / te compenseren?

Niet van toepassing

Formulaire d'analyse d'impact

Analyse d'impact intégrée

Référez-vous au manuel pour compléter l'analyse d'impact

Contactez le helpdesk ria-air@premier.fed.be pour toute question

Fiche signalétique

A. Auteur

- Membre du Gouvernement compétent > Monsieur Jan Jambon
  Ministre de l'Intérieur.
- Contact cellule stratégique (Nom, E-mail, Tél.) > Joris.Creemers@ibz.fgov.be , tél. 02/504.85.18
- Administration > AFCN
- Contact administration (Nom, E-mail, Tél.) >
  - Rony Dresselaers, rony.dresselaers@fanc.fgov.be, 02/ 289 20 25, Stephane Célestin, Stéphane.celestin@fanc.fgov.be; 02/289 20 51

B. Projet

- Titre de la réglementation > PROJET DE LOI PORTANT MODIFICATION DE LA LOI DU 15 AVRIL 1994 RELATIVE A LA PROTECTION DE LA POPULATION ET DE L'ENVIRONNEMENT CONTRE LES DANGERS RESULTANT DES RAYONNEMENTS IONISANTS ET RELATIVE A L'AGENCE FEDERALE DE CONTROLE NUCLEAIRE CONCERNANT LA CYBER-SECURITÉ NUCLEAIRE
- Description succincte du projet de réglementation en mentionnant l'origine réglementaire (traités, directive, accord de coopération, actualité, …), les objectifs poursuivis et la mise en œuvre.

Au plan international, la cyber-sécurité dans toute sa généralité fait l'objet d'une attention croissante.
Plus spécifiquement, la cyber-sécurité nucléaire fait également l'objet d'une attention sans cesse accrue dans de nombreux forums internationaux; ; mentionnons notamment le Nuclear Security Summit, ou encore l'AIEA, au sein de laquelle le thème de la cyber-sécurité nucléaire est de plus en plus souvent abordé, et est de plus en plus traité comme une dimension à part entière de la sécurité nucléaire. Nous renvoyons à ce sujet aux résolutions pertinentes de la Conférence générale, à l'International Conference on Computer Security in a Nuclear World, qui s'est tenue à Vienne du 1er au 5 juin 2015, au Plan de Sécurité nucléaire 2018-2021, ainsi qu'aux différents documents de recommandations sur la question élaborés dans les Nuclear Security Series. ; soulignons que la Belgique se montre particulièrement active et attentive au sein des divers groupes de travail qui, dans le giron de l'AIEA, élaborent ces recommandations spécifiques.

Depuis des années, les efforts du gouvernement en matière de sécurité nucléaire avaient 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 de par le monde des cyber-attaques contre des gouvernements, des institutions ou des industries, la cyber-sécurité 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.

Compte tenu de la menace et des considérations développées ci-dessus, il convenait 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.

Les dispositions essentielles du projet soumis à votre délibération consistent dès lors en l'habilitation au Roi de déterminer des mesures de cyber-sécurité nucléaire qui s'imposeront aux opérateurs concernés et en l'habilitation à l'Agence de prévoir les grandes lignes de mesures de cyber-sécurité nucléaire de gestion prudente pour les réseaux et systèmes présentant moins de risques.
Le projet prévoit en outre que l'AFCN jouera divers rôles , y compris de sensibilisation, et sera responsable des inspections et contrôles des mesures de cyber-sécurité nucléaire.

Le présent projet de loi n'a pas pour objet de criminaliser les cyber-attaques ou d'autres comportements répréhensibles. Les conventions et textes internationaux pertinents, principalement la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, au plan général, la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, la Convention sur la protection physique des matières et des installations nucléaires telle qu'amendée, pour ce qui concerne la sécurité nucléaire, soit des normes internationales ayant une telle perspective, ont fait l'objet des lois d'application nécessaires (mentionnons la loi du 6 juillet 2017 portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice, qui comporte un titre 14 transposant en droit belge la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, ou encore la loi du 23 mai 2013 modifiant le Code pénal afin de le mettre en conformité avec la Convention internationale pour la répression des actes de terrorisme nucléaire, faite à New York, le 14 septembre 2005, et avec l'Amendement de la Convention sur la protection physique des matières nucléaires, adopté à Vienne le 8 juillet 2005 par la Conférence des États parties à la Convention).

Le projet de loi a pour effet d'introduire un régime proche mais distinct de celui que prévoit la « « directive NIS » (loi du XX XX XXXX établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique), ci-après loi de transposition de la Directive dite « NIS » [qui vient d'être approuvée].

Une telle approche spécifique et distincte s'impose non seulement en raison du cadre actuel de la cyber-sécurité nucléaire (voir supra) ainsi que de la genèse du présent projet (voir supra), mais également en raison des singularités de la cyber-sécurité nucléaire, spécialement ses liens avec la « catégorisation » (classification) de l'information, avec la sécurité nationale, et le fait que les mesures de cyber-sécurité qui devront être prises pourraient, le cas échéant, sous certains aspects, voisiner avec , ou constituer ou ressortir des « mesures de protection physique », des « mesures de sécurité des substances radioactives autres que les matières nucléaires » ou des « mesures de sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives », au sens de ces termes dans la loi du 15 avril 1994 (voir respectivement les articles 17bis premier tiret, 17quater 3°) et 17quinquies 1°)) de la loi) .
Cela étant, les dispositions particulières de la susdite loi de transposition de la Directive NIS selon lesquelles elle régit à la fois les éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité (voir article 4 §4 de cette loi) et la compétence d'inspection de sa bonne exécution par l'AFCN (voir article 43 de cette loi, qui insère un article 15ter dans la loi du 15 avril 1994) ne sont pas affectées.

- Analyses d'impact déjà réalisées > ☐ Oui / ☒ Non
  Si oui, veuillez joindre une copie ou indiquer la référence du document >

C. Consultations sur le projet de réglementation

- Consultations obligatoires, facultatives ou informelles :

  Avis IF, Budget, Conseil des ministres

D. Sources utilisées pour effectuer l'analyse d'impact

Formulaire d'analyse d'impact

- Statistiques, documents de référence, organisations et personnes de référence :

  Analyse interne AFCN

E. Date de finalisation de l'analyse d'impact

- 28/05/2018

Quel est l'impact du projet de réglementation sur ces 21 thèmes ?

Un projet de réglementation sera, dans la majorité des dossiers, seulement concerné par quelques thèmes.

- Une liste non-exhaustive de mots-clés est présentée pour faciliter l'appréciation de chaque thème, sans pour cela consulter systématiquement le manuel.
  S'il y a des impacts positifs et/ou négatifs, expliquez-les (sur base des mots-clés si nécessaire) et indiquez les mesures prises pour alléger / compenser les éventuels impacts négatifs.
- Pour les **thèmes 3, 10, 11 et 21**, des questions plus approfondies sont posées.

Lutte contre la pauvreté [1]

Revenu minimum conforme à la dignité humaine, accès à des services de qualité, surendettement, risque de pauvreté ou d'exclusion sociale (y compris chez les mineurs), illettrisme, fracture numérique.

☐ Impact positif ☐ Impact négatif ↓ Expliquez (utiliser les mots-clés si nécessaire) ☒ Pas d'impact

Égalité des chances et cohésion sociale [2]

Non-discrimination, égalité de traitement, accès aux biens et services, accès à l'information, à l'éducation et à la formation, écart de revenu, effectivité des droits civils, politiques et sociaux (en particulier pour les populations fragilisées, les enfants, les personnes âgées, les personnes handicapées et les minorités).

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Égalité des femmes et les hommes [3]

Accès des femmes et des hommes aux ressources : revenus, travail, responsabilités, santé/soins/bien-être, sécurité, éducation/savoir/formation, mobilité, temps, loisirs, etc.

Exercice des droits fondamentaux par les femmes et les hommes : droits civils, sociaux et politiques.

1. Quelles personnes sont concernées (directement et indirectement) par le projet et quelle est la composition sexuée de ce(s) groupe(s) de personnes ? Si aucune personne n'est concernée, expliquez pourquoi.

   Ne s'applique pas

   → *Si des personnes sont concernées, répondez aux questions suivantes :*

   2. Identifiez les éventuelles différences entre la situation respective des femmes et des hommes dans la matière relative au projet de réglementation.

      Ne s'applique pas.

      → *S'il existe des différences, répondez à la question suivante :*

      3. Certaines de ces différences limitent-elles l'accès aux ressources ou l'exercice des droits fondamentaux des femmes ou des hommes (différences problématiques) ? [NON > expliquez

         Ne s'applique pas.

Formulaire d'analyse d'impact

4. Compte tenu des réponses aux questions précédentes, identifiez les impacts positifs et négatifs du projet sur l'égalité des femmes et les hommes ?

Ne s'applique pas.

→ *S'il y a des impacts négatifs, répondez à la question suivante :*

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

Ne s'applique pas.

Santé [4]

Accès aux soins de santé de qualité, efficacité de l'offre de soins, espérance de vie en bonne santé, traitements des maladies chroniques (maladies cardiovasculaires, cancers, diabètes et maladies respiratoires chroniques), déterminants de la santé (niveau socio-économique, alimentation, pollution), qualité de la vie.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Emploi [5]

Accès au marché de l'emploi, emplois de qualité, chômage, travail au noir, conditions de travail et de licenciement, carrière, temps de travail, bien-être au travail, accidents de travail, maladies professionnelles, équilibre vie privée - vie professionnelle, rémunération convenable, possibilités de formation professionnelle, relations collectives de travail.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Modes de consommation et production [6]

Stabilité/prévisibilité des prix, information et protection du consommateur, utilisation efficace des ressources, évaluation et intégration des externalités (environnementales et sociales) tout au long du cycle de vie des produits et services, modes de gestion des organisations.

☒ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Développement économique [7]

Création d'entreprises, production de biens et de services, productivité du travail et des ressources/matières premières, facteurs de compétitivité, accès au marché et à la profession, transparence du marché, accès aux marchés publics, relations commerciales et financières internationales, balance des importations/exportations, économie souterraine, sécurité d'approvisionnement des ressources énergétiques, minérales et organiques.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Investissements [8]

Investissements en capital physique (machines, véhicules, infrastructures), technologique, intellectuel (logiciel, recherche et développement) et humain, niveau d'investissement net en pourcentage du PIB.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Recherche et développement [9]

Opportunités de recherche et développement, innovation par l'introduction et la diffusion de nouveaux modes de production, de nouvelles pratiques d'entreprises ou de nouveaux produits et services, dépenses de recherche et de développement.

☐ Impact positif ☐ Impact ↓ Expliquez ☒ Pas d'impact

Formulaire d'analyse d'impact

négatif

Niveau inchangé.

PME [10]

Impact sur le développement des PME.

1. Quelles entreprises sont directement et indirectement concernées ? Détaillez le(s) secteur(s), le nombre d'entreprises, le % de PME (< 50 travailleurs) dont le % de micro-entreprise (< 10 travailleurs). Si aucune entreprise n'est concernée, expliquez pourquoi.

Entreprises du secteur nucléaire.

→ *Si des PME sont concernées, répondez à la question suivante :*

2. Identifiez les impacts positifs et négatifs du projet sur les PME.
[N.B. les impacts sur les charges administratives doivent être détaillés au thème 11]

Les entreprises sont protégées contre les cyberrisques, ce qui garantit une meilleure sécurité de l'environnement de travail et des travailleurs.

→ *S'il y a un impact négatif, répondez aux questions suivantes :*

3. Ces impacts sont-ils proportionnellement plus lourds sur les PME que sur les grandes entreprises ? [NON > expliquez

Une approche graduée est appliquée.

4. Ces impacts sont-ils proportionnels à l'objectif poursuivi ? [QUI > expliquez

Oui, grâce à l'approche graduée.

5. Quelles mesures sont prises pour alléger / compenser les impacts négatifs ?

Une approche graduée.

Charges administratives [11]

Réduction des formalités et des obligations administratives liées directement ou indirectement à l'exécution, au respect et/ou au maintien d'un droit, d'une interdiction ou d'une obligation.

→ *Si des entreprises et/ou des citoyens sont concernés, répondez à la question suivante :*

1. Identifiez, par groupe concerné, les formalités et les obligations nécessaires à l'application de la réglementation. Si aucune entreprise et aucun citoyen n'est concerné, expliquez pourquoi.

* > **

→ *S'il y a des formalités et/ou des obligations, répondez aux questions suivantes :*

2. Quels documents et informations chaque groupe concerné doit-il fournir ?

Réglementation actuelle > Projet de réglementation

3. Comment s'effectue la récolte des informations et des documents, par groupe concerné ?

Réglementation actuelle > Projet de réglementation

4. Quelles est la périodicité des formalités et des obligations, par groupe concerné ?

Réglementation actuelle > Projet de réglementation

5. Quelles mesures sont prises pour alléger / compenser les éventuels impacts négatifs ?

Ne s'applique pas

* Ne remplir que s'il y a des formalités/obligations actuellement dans la matière relative au projet.

** Remplir si le projet modifie ou introduit de nouvelles formalités/obligations.

Énergie [12]

Mix énergétique (bas carbone, renouvelable, fossile), utilisation de la biomasse (bois, biocarburants), efficacité énergétique, consommation d'énergie de l'industrie, des services, des transports et des ménages, sécurité d'approvisionnement, accès aux biens et services énergétiques.

Formulaire d'analyse d'impact

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Mobilité [13]

Volume de transport (nombre de kilomètres parcourus et nombre de véhicules), offre de transports collectifs, offre routière, ferroviaire, maritime et fluviale pour les transports de marchandises, répartitions des modes de transport (modal shift), sécurité, densité du trafic.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Alimentation [14]

Accès à une alimentation sûre (contrôle de qualité), alimentation saine et à haute valeur nutritionnelle, gaspillages, commerce équitable.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Changements climatiques [15]

Émissions de gaz à effet de serre, capacité d'adaptation aux effets des changements climatiques, résilience, transition énergétique, sources d'énergies renouvelables, utilisation rationnelle de l'énergie, efficacité énergétique, performance énergétique des bâtiments, piégeage du carbone.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Ressources naturelles [16]

Gestion efficiente des ressources, recyclage, réutilisation, qualité et consommation de l'eau (eaux de surface et souterraines, mers et océans), qualité et utilisation du sol (pollution, teneur en matières organiques, érosion, assèchement, inondations, densification, fragmentation), déforestation.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Air intérieur et extérieur [17]

Qualité de l'air (y compris l'air intérieur), émissions de polluants (agents chimiques ou biologiques : méthane, hydrocarbures, solvants, SOx, NOx, NH3), particules fines.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Biodiversité [18]

Niveaux de la diversité biologique, état des écosystèmes (restauration, conservation, valorisation, zones protégées) , altération et fragmentation des habitats, biotechnologies, brevets d'invention sur la matière biologique, utilisation des ressources génétiques, services rendus par les écosystèmes (purification de l'eau et de l'air, …), espèces domestiquées ou cultivées, espèces exotiques envahissantes, espèces menacées.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Nuisances [19]

Formulaire d'analyse d'impact

Nuisances sonores, visuelles ou olfactives, vibrations, rayonnements ionisants, non ionisants et électromagnétiques, nuisances lumineuses.

☐ Impact positif ☐ Impact négatif ↓ Expliquez ☒ Pas d'impact

Autorités publiques [20]

Fonctionnement démocratique des organes de concertation et consultation, services publics aux usagers, plaintes, recours, contestations, mesures d'exécution, investissements publics.

☒ Impact positif ☐ Impact négatif ↓ Expliquez ☐ Pas d'impact

Simplification administrative pour l'Agence. Réglementation plus claire avec intégration de règles internationales.

Cohérence des politiques en faveur du développement [21]

Prise en considération des impacts involontaires des mesures politiques belges sur les intérêts des pays en voie de développement.

1. Identifiez les éventuels impacts directs et indirects du projet sur les pays en voie de développement dans les domaines suivants : sécurité alimentaire, santé et accès aux médicaments, travail décent, commerce local et international, revenus et mobilisations de ressources domestiques (taxation), mobilité des personnes, environnement et changements climatiques (mécanismes de développement propre), paix et sécurité. Expliquez si aucun pays en voie de développement n'est concerné

Ne s'applique pas.

→ *S'il y a des impacts positifs et/ou négatifs, répondez à la question suivante :*

2. Précisez les impacts par groupement régional ou économique (lister éventuellement les pays). cf. annexe

Ne s'applique pas.

→ *S'il y a des impacts négatifs, répondez à la question suivante :*

3. Quelles mesures sont prises pour les alléger / compenser les impacts négatifs?

Ne s'applique pas.

ADVIES VAN DE RAAD VAN STATE NR. 63.963/1/V VAN 16 AUGUSTUS 2018

Op 19 juli 2018 is de Raad van State, afdeling Wetgeving, door de minister van Veiligheid en Binnenlandse Zaken verzocht binnen een termijn van dertig dagen, van rechtswege verlengd tot 4 september 2018,(*) een advies te verstrekken over een voorontwerp van wet "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".

Het voorontwerp is door de eerste vakantiekamer onderzocht op 7 augustus 2018. De kamer was samengesteld uit Jeroen Van Nieuwenhove, staatsraad, voorzitter, Stephan De Taeye en Koen Muylle, staatsraden, Michel Tison, assessor, en Greet Verberckmoes, griffier.

Het verslag is uitgebracht door Tim Corthaut, auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Marnix Van Damme, kamervoorzitter.

Het advies, waarvan de tekst hierna volgt, is gegeven op 16 augustus 2018.

*

1. Met toepassing van artikel 84, § 3, eerste lid, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, heeft de afdeling Wetgeving zich toegespitst op het onderzoek van de bevoegdheid van de steller van de handeling, van de rechtsgrond[1], alsmede van de vraag of aan de te vervullen vormvereisten is voldaan.

*

STREKKING VAN HET VOORONTWERP

2.1. Het voor advies voorgelegde voorontwerp van wet strekt tot 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" (hierna: de FANC-wet), teneinde een kader tot stand te brengen voor de cyberveiligheid van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd,

(*) Deze verlenging vloeit voort uit artikel 84, § 1, eerste lid, 2°, *in fine*, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, waarin wordt bepaald dat deze termijn van rechtswege verlengd wordt met vijftien dagen wanneer hij begint te lopen tussen 15 juli en 31 juli of wanneer hij verstrijkt tussen 15 juli en 15 augustus.

1 Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

AVIS DU CONSEIL D'ÉTAT N° 63.963/1/V DU 16 AOÛT 2018

Le 19 juillet 2018, le Conseil d'État, section de législation, a été invité par le ministre de la Sécurité et de l'Intérieur à communiquer un avis, dans un délai de trente jours, prorogé de plein droit jusqu'au 4 septembre 2018,(**) sur un avant-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".

L'avant-projet a été examiné par la première chambre des vacations le 7 août 2018. La chambre était composée de Jeroen Van Nieuwenhove, conseiller d'État, président, Stephan De Taeye et Koen Muylle, conseillers d'État, Michel Tison, assesseur, et Greet Verberckmoes, greffier.

Le rapport a été présenté par Tim Corthaut, auditeur.

La concordance entre la version française et la version néerlandaise de l'avis a été vérifiée sous le contrôle de Marnix Van Damme, président de chambre.

L'avis, dont le texte suit, a été donné le 16 août 2018.

*

1. En application de l'article 84, § 3, alinéa 1er, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973, la section de législation a fait porter son examen essentiellement sur la compétence de l'auteur de l'acte, le fondement juridique [1] et l'accomplissement des formalités prescrites.

*

PORTÉE DE L'AVANT-PROJET

2.1 L'avant-projet de loi soumis pour avis a pour objet de modifier 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" (ci-après: la loi A.F.C.N.), afin d'élaborer un cadre pour la cybersécurité des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent

(**) Ce délai résulte de l'article 84, § 1er, alinéa 1er, 2°, *in fine*, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973 qui précise que ce délai est prolongé de plein droit de quinze jours lorsqu'il prend cours du 15 juillet au 31 juillet ou lorsqu'il expire entre le 15 juillet et le 15 août.

1 S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité avec les normes supérieures.

vervaardigd, gehouden of gebruikt, of waar zich toestellen bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is.

2.2. Artikel 2 van het voorontwerp strekt tot het toevoegen van een aantal definities aan artikel 1 van de FANC-wet ("nucleaire cyberbeveiligingsmaatregelen", "nucleaire cyberbeveiliging", "netwerk- en informatiesysteem", "beveiliging van netwerk- en informatiesystemen", "cyberincident" en "cyberrisico"). Artikel 3 van het voorontwerp strekt tot aanvulling van artikel 14, vierde lid, van de FANC-wet om het FANC te belasten met taken op het vlak van de controle op de nucleaire cyberbeveiligingsmaatregelen. Artikel 4 van het voorontwerp strekt tot het invoegen van een afdeling 3*quater* in hoofdstuk III van de FANC-wet, bestaande uit een enig artikel 17*sexies*, dat een reeks regelgevende en praktische delegaties aan de Koning en het FANC bevat op het vlak van de nucleaire cyberbeveiliging.

ALGEMENE OPMERKING

3. Wat de verwijzing in het ontworpen artikel 17*sexies*, § 5, van de FANC-wet, naar artikel 4, § 4, van de aan te nemen wet "tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid"[2] betreft, dient te worden opgemerkt dat deze laatste bepaling de verhouding regelt tussen het thans voorliggende voorontwerp en die aan te nemen wet. Dat is van belang omdat die wet strekt tot omzetting van richtlijn (EU) 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 nucleaire elektriciteitsproductie-installaties die ook door dit voorontwerp worden geviseerd, vallen eveneens onder die richtlijn, en dus ook onder die aan te nemen wet. Het verdient aanbeveling om in de memorie van toelichting de verhouding tussen de voorliggende regeling en de aan te nemen wet "tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid" te verduidelijken. De voorliggende regeling is immers uitdrukkelijk niet bedoeld als omzetting van richtlijn (EU) 2016/1148, maar is er duidelijk wel door geïnspireerd en lijkt neer te komen op een uitbreiding van de kernbegrippen van die richtlijn tot niet-geharmoniseerde aangelegenheden.

ONDERZOEK VAN DE TEKST

Artikel 4

4.1. Het ontworpen artikel 17*sexies*, § 1, 1°, van de FANC-wet is – zeker in de Nederlandse versie – vrijwel onleesbaar door de opeenvolging van neven- en ondergeschikte zinnen. Daaraan kan tegemoet worden gekomen door in artikel 1 van de FANC-wet een definitie van de te beveiligen installaties ("de

[2] Over dit voorontwerp van wet 'tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' is de adviesaanvraag hangende bij de Raad van State, afdeling Wetgeving, onder rolnummer 63.972/4.

des appareils émettant des rayonnements ionisants ne provenant pas de substances radioactives.

2.2. L'article 2 de l'avant-projet vise à ajouter un certain nombre de définitions à l'article 1er de la loi A.F.C.N. ("mesures de cybersécurité nucléaire", "cybersécurité nucléaire", "réseau et système d'information", "sécurité des réseaux et des systèmes d'information", "cyber-incident" et "cyber-risques"). L'article 3 de l'avant-projet tend à compléter l'article 14, alinéa 4, de la loi A.F.C.N. afin de charger l'A.F.C.N. de tâches relatives au contrôle des mesures de cybersécurité nucléaire. L'article 4 de l'avant-projet vise à insérer une section 3*quater* dans le chapitre III de la loi A.F.C.N., comprenant le seul article 17*sexies* qui comporte une série de délégations réglementaires et pratiques au Roi et à l'A.F.C.N. en matière de cybersécurité nucléaire.

OBSERVATION GÉNÉRALE

3. En ce qui concerne la référence que l'article 17*sexies*, § 5, en projet, de la loi A.F.C.N., fait à l'article 4, § 4, de la loi à adopter "établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" [2], il convient d'observer que cette dernière disposition règle l'articulation entre l'avant-projet actuellement examiné et cette loi à adopter. Il s'agit d'un élément important étant donné que cette loi vise à transposer la directive (UE) 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'information dans l'Union". Les installations de production nucléaire d'électricité, qui sont également visées par cet avant-projet, relèvent également de cette directive, et donc aussi de cette loi à adopter. Il est recommandé de préciser dans l'exposé des motifs le rapport entre le régime à l'examen et la loi à adopter "établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique". En effet, le régime à l'examen n'a pas expressément vocation à transposer la directive (UE) 2016/1148, mais il s'en inspire clairement et semble s'analyser comme une extension des notions clés de cette directive à des matières non harmonisées.

EXAMEN DU TEXTE

Article 4

4.1. L'article 17*sexies,* § 1er, 1°, en projet, de la loi A.F.C.N. est – certainement dans la version néerlandaise – quasiment illisible en raison de la succession de phrases coordonnées et subordonnées. Il peut y être remédié en insérant dans l'article 1er de la loi A.F.C.N. une définition des installations

[2] En ce qui concerne cet avant-projet de loi 'établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique', le Conseil d'État, section de législation, est saisi de la demande d'avis, inscrite au rôle sous le numéro 63.972/4.

nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is") in te voegen, zodat die omschrijving in het ontworpen artikel 17*sexies*, § 1, 1°, kan worden weggelaten. Daartoe kan artikel 2 van het voorontwerp worden aangevuld. Door die lange omschrijving niet telkens te moeten herhalen, zullen overigens ook enkele andere bepalingen van het voorontwerp vlotter leesbaar worden.

4.2. Het ontworpen artikel 17*sexies*, § 2, van de FANC-wet houdt een delegatie van verordenende bevoegdheid aan het FANC in. Het verlenen van verordenende bevoegdheid aan een openbare instelling is in beginsel niet in overeenstemming met de algemene publiekrechtelijke beginselen omdat erdoor geraakt wordt aan het beginsel van de eenheid van de verordenende macht en 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. Dergelijke delegaties kunnen dan ook enkel worden gebillijkt om praktische redenen en voor zover zij een zeer beperkte of een hoofdzakelijk technische en niet-beleidsmatige draagwijdte hebben, en er mag worden van uitgegaan dat de instellingen die de betrokken reglementering dienen toe te passen of er toezicht op uitoefenen, ook het best geplaatst zijn om deze met kennis van zaken uit te werken.

De aan het FANC gedelegeerde bevoegdheid zal aan de voormelde criteria moeten voldoen. Zoniet dient de delegatie aan de Koning te worden verleend.

4.3. Artikel 15*ter* van de FANC-wet, w*aarnaa*r in het ontworpen artikel 17*sexies*, § 5, van de FANC-wet wordt verwezen, bestaat nog niet. Het betreft een bepaling waarvan de invoering wordt beoogd door artikel 79 van het voorontwerp van wet "tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid", waarover de adviesaanvraag bij de Raad van State, afdeling Wetgeving, hangende is.[3] Bijgevolg zal de aanneming en inwerkingtreding van het voorliggende voorontwerp op dat andere voorontwerp moeten worden afgestemd.

De griffier, *De voorzitter,*

Greet VERBERCKMOES — Jeroen VAN NIEUWENHOVE

[3] Adviesaanvraag 63.972/4.

à sécuriser ("les installations nucléaires et établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives"), de sorte que cette définition peut être omise à l'article 17*sexies*, § 1er, 1°, en projet. L'article 2 de l'avant-projet peut être complété à cet effet. Par ailleurs, quelques autres dispositions de l'avant-projet gagneront également en lisibilité en évitant chaque fois la répétition de cette longue définition.

4.2. L'article 17*sexies*, § 2, en projet, de la loi A.F.C.N. accorde une délégation de pouvoir réglementaire à l'A.F.C.N. 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. Pareilles délégations ne se justifient dès lors que pour des raisons pratiques et pour autant qu'elles ont une portée très limitée ou principalement technique et non politique et qu'il peut être considéré que les organismes qui doivent appliquer la réglementation concernée ou la contrôler sont également les mieux placés pour l'élaborer en connaissance de cause.

Le pouvoir délégué à l'A.F.C.N. devra satisfaire aux critères précités, à défaut de quoi la délégation doit être conférée au Roi.

4.3. L'article 15*ter* de la loi A.F.C.N., auquel l'article 17*sexies*, § 5, en projet, de la loi A.F.C.N. fait référence, n'existe pas encore. Il s'agit d'une disposition que vise à instaurer l'article 79 de l'avant-projet de loi "établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique" dont la demande d'avis a été soumise au Conseil d'État, section de législation [3]. Par conséquent, l'adoption et l'entrée en vigueur de l'avant-projet à l'examen devront être alignées sur cet autre avant-projet.

Le greffier, *Le président,*

Greet VERBERCKMOES — Jeroen VAN NIEUWENHOVE

[3] Demande d'avis 63.972/4.

WETSONTWERP

FILIP,

KONING DER BELGEN,

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van de minister van Veiligheid en Binnenlandse Zaken,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De minister van Veiligheid en Binnenlandse Zaken is ermee belast het ontwerp van wet, waarvan de tekst hierna volgt, in onze naam bij de Kamer van volksvertegenwoordigers in te dienen:

Artikel 1

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 74 van de Grondwet.

Artikel 2

In artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, gewijzigd bij de wetten van 2 april 2003, 30 maart 2011, 26 januari 2014, 19 maart 2014, 15 mei 2014 en 13 december 2017 worden de volgende definities toegevoegd:

— Nucleaire cyberbeveiligingsmaatregelen

De maatregelen betreffende de beveiliging van netwerk- en informatiesystemen van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, met het oog op de nucleaire cyberbeveiliging.

— Nucleaire cyberbeveiliging

De beveiliging van netwerk- en informatiesystemen van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties

PROJET DE LOI

PHILIPPE,

ROI DES BELGES,

À tous, présents et à venir,
SALUT.

Sur la proposition du ministre de la Sécurité et de l'Intérieur,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le ministre de la Sécurité et de l'Intérieur est chargé de présenter, en notre nom, à la Chambre des représentants, le projet de loi dont la teneur suit:

Article 1er

La présente loi règle une matière visée à l'article 74 de la Constitution.

Article 2

A l'article 1er 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, modifié par les lois du 2 avril 2003, 30 mars 2011, 26 janvier 2014, 19 mars 2014, 15 mai 2014 et 13 décembre 2017 les définitions suivantes sont ajoutées:

"— Mesures de cybersécurité nucléaire

Les mesures relatives à la sécurité des réseaux et des systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives, à des fins de cybersécurité nucléaire.

— Cybersécurité nucléaire

La sécurité des réseaux et systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils

bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is.

Netwerk- en informatiesysteem

1. een elektronisch communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

2. een apparaat of groep van permanente of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische bestanddelen van dit apparaat die onder meer de automatisering van een operationeel proces mogelijk maken, alsook de controle op afstand of het verkrijgen van werkingsgegevens in real time;

3. of digitale gegevens die via de in de punten 1 en 2 bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

— Beveiliging van netwerk- en informatiesystemen

Het vermogen van netwerken en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen.

— Cyberincident

Elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen.

— Cyberrisico

Elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen."

Art. 3

In dezelfde wet wordt volgende bepaling toegevoegd aan artikel 15, 4e lid:

"Onverminderd de artikelen 15*bis* en [15*ter*] van deze wet is het Agentschap eveneens belast met de controle op de nucleaire cyberbeveiligingsmaatregelen."

et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives.

— Réseau et système d'information

1. un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques;

2. un dispositif ou un ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation d'un processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel;

3. ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points 1 et 2 en vue de leur fonctionnement, leur utilisation, leur protection et leur maintenance.

— Sécurité des réseaux et des systèmes d'information

La capacité des réseaux et des systèmes d'information de résister, à un niveau de fiabilité donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

— Cyber-incident

Tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.

— Cyber-risques

Toute circonstance ou tout événement raisonnablement identifiable ayant une incidence négative potentielle sur la sécurité des réseaux et des systèmes d'information."

Art. 3

Dans la même loi, la disposition suivante est ajoutée à l'article 15, alinéa 4 :

"Sans préjudice des articles 15*bis* et [15*ter*] de la présente loi , l'Agence est également chargée du contrôle des mesures de cybersécurité nucléaire."

Art. 4

In hoofdstuk III van dezelfde wet wordt een afdeling 3*quater* ingevoegd die een artikel 17*sexies* bevat, luidende:

"Afdeling 3*quate.* Bevoegdheid op het gebied van de nucleaire cyberbeveiliging

Art. 17sexies. § 1.Op voorstel van het Agentschap en na advies van de door de Koning aangeduide autoriteiten:

1° Verdeelt de Koning de netwerk- en informatiesystemen van de installaties en de inrichtingen waarop de nucleaire cyberbeveiliging zoals omschreven in artikel 1, gericht is, voor zover deze netwerk- en informatiesystemen het beheer, de controle of de veiligstelling van het kernmateriaal, de radioactieve stoffen, of de toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, voor deze installaties of deze inrichtingen, rechtstreeks of onrechtstreeks mogelijk maken, waarborgen of ondersteunen, in categorieën, op basis van het cyberrisico dat eraan verbonden is.

2° bepaalt de Koning het beveiligingsniveau van de netwerk- en informatiesystemen bedoeld in punt 1°;

3° bepaalt de Koning de noodzakelijke en evenredige nucleaire cyberbeveiligingsmaatregelen voor het beheer van de cyberrisico's van de categorieën van netwerk- en informatiesystemen bedoeld in punt 1° die, in het licht van de bestaande kennis, met het hoogste cyberrisico overeenstemmen en voor het voorkomen van cyberincidenten die hierop van invloed kunnen zijn, of om de impact ervan te beperken, onverminderd de toepassing van het internationaal stelsel van de waarborgen.

Deze maatregelen regelen met name de melding aan het Agentschap en aan de door de Koning aangeduide autoriteiten, van cyberincidenten met een significante impact die door de exploitant van de door deze maatregelen bedoelde installatie of inrichting moet worden gedaan;

4° regelt de Koning de uitwisseling tussen het Agentschap en de door de Koning aangewezen autoriteiten van de gegevens waarover ze beschikken in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd.

5° bepaalt de Koning de erkenningsprocedure voor de nucleaire cyberbeveiligingsmaatregelen bedoeld in punt 3°.

Art. 4

Dans le chapitre III de la même loi, il est inséré une section 3*quater* comportant l'article 17*sexies* rédigé comme suit:

"Section 3*quater*- Compétence en matière de cybersécurité nucléaire

Art. 17*sexies*. § 1er. Sur proposition de l'Agence, et après avis des autorités désignées par le Roi:

1° le Roi répartit en catégories , en fonction du cyberrisque qu'ils présentent, les réseaux et systèmes d'information des installations et des établissements que vise la cybersécurité nucléaire telle que définie à l'article 1er, dans la mesure où ces réseaux et systèmes d'information, pour ces installations ou ces établissements, permettent directement ou indirectement, assurent ou appuient la gestion, le contrôle ou la sécurisation des matières nucléaires, des substances radioactives ou des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives.

2° le Roi détermine le niveau de sécurité des réseaux et systèmes d'information visés au point 1°;

3° le Roi détermine les mesures de cybersécurité nucléaire nécessaires et proportionnées pour gérer les cyber-risques des catégories des réseaux et systèmes d'information visés au point 1° 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, sans préjudice de l'application du régime international de garanties.

Ces mesures règlent notamment la notification à l'Agence ainsi qu' aux autorités désignées par le Roi, des cyber-incidents ayant un impact significatif que l'exploitant d'une installation ou d'un établissement visé par ces mesures doit effectuer;

4° le Roi règle l'échange entre l'Agence et les autorités désignées par le Roi des données qu'elles possèdent sur les cyber-risques et sur les cyber-incidents auxquels l'exploitant est ou peut être confronté.

5° le Roi détermine la procédure d'agrément des mesures de cybersécurité nucléaire visées au point 3°.

§ 2. Het Agentschap bepaalt, na advies van de door de Koning aangewezen autoriteiten, de principes voor de nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer voor de categorieën van netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, die met het laagste cyberrisico overeenstemmen.

§ 3. Het Agentschap kan de in paragraaf 1, 4°, bedoelde erkenningen aan voorwaarden onderwerpen. Het Agentschap kan deze erkenningen en de hierin opgelegde voorwaarden, te allen tijde, op eigen initiatief en op gemotiveerde wijze, wijzigen of aanvullen, indien deze wijzigingen of aanvullingen bedoeld zijn om de naleving te garanderen van de door of krachtens de wet voorziene eisen inzake de nucleaire cyberbeveiliging en deze wijzigingen of aanvullingen kennelijk gepast, evenredig en billijk zijn.

§ 4.Het Agentschap is voor de netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, belast met:

1° het informeren van de exploitanten van de installaties en inrichtingen bedoeld in paragraaf 1, 1°, over de cyberrisico's waarvan het op de hoogte is en die betrekking hebben op de netwerk- en informatiesystemen, of de daaraan gerelateerde diensten;

2° het verrichten van analyses en technisch onderzoeken ten behoeve van de in de punt 1° bedoelde opdrachten naar aanleiding van cyberrisico's of cyberincidenten, of van elementen die daarop wijzen, die niet bestaan in het onderzoek, of verplichtingen die door de gerechtelijke overheid werden opgelegd met het oog op de identificatie van personen of organisaties die voor deze cyberrisico's en cyberincidenten verantwoordelijk zijn, of daar anderszins aan bijdragen of hebben bijgedragen;

3° het informeren en sensibiliseren van gebruikers van deze netwerk- en informatiesystemen.

Het Agentschap doet hiertoe een beroep op de samenwerking, het advies en de ervaring van de door de Koning aangewezen autoriteiten.

De Koning kan, op voordracht van het Agentschap, dat het advies inwint van de door hem aangeduide autoriteiten, de nadere regelen voor de toepassing van deze paragraaf bepalen.

§ 5. Dit artikel is van toepassing onverminderd de artikelen 15*bis*, [[15*ter*]], 17*bis*, 17*quater* en 17*quinquies* van deze wet en artikel 4§ 4 van [[de wet van [xx] tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor

§ 2. L'Agence détermine, après avis des autorités désignées par le Roi, les principes des mesures de cybersécurité nucléaire de gestion prudente pour les catégories des réseaux et systèmes d'information visés au paragraphe 1er, 1°, correspondant au cyber-risque le moins élevé.

§ 3. L'Agence peut subordonner les agréments visés au paragraphe 1er, 4°, à des conditions. L'Agence peut en tout temps modifier ou compléter, d'initiative et de manière motivée, ces agréments et les conditions qui leur sont imposées, si ces modifications ou compléments visent à assurer le respect des exigences prévues par ou en vertu de la loi et en relation avec la cybersécurité nucléaire et si ces modifications ou compléments sont manifestement appropriés, proportionnés et équitables.

§ 4. L'Agence est chargée, pour les réseaux et systèmes d'information visés au paragraphe 1er, 1°:

1°. d'informer les exploitants des installations et des établissements visés au paragraphe 1er, 1°, des cyber-risques dont elle a connaissance et qui sont en lien avec leurs réseaux et systèmes d'information, ou les services connexes;

2°. de réaliser, en présence de cyber-risques ou de cyber-incidents ou de tout élément donnant à penser qu'ils existent, des analyses et des enquêtes techniques bénéficiant aux missions visées au point 1°, en dehors de l'instruction ou de devoirs prescrits par l'autorité judiciaire visant à identifier les personnes ou organisations qui sont responsables de ces cyber-risques ou cyber incidents, ou qui y contribuent ou y ont contribué de quelque manière que ce soit.

3° d'informer et de sensibiliser les utilisateurs de ces réseaux et systèmes d'information.

A cette fin, l'Agence recourt à la collaboration, à l'avis et à l'expérience des autorités désignées par le Roi.

Le Roi peut déterminer les modalités de l'application du présent paragraphe sur proposition de l'Agence, qui sollicite l'avis des autorités qu'il désigne.

§ 5. Le présent article s'applique sans préjudice des articles 15*bis*, [[15*ter*]], 17*bis*, 17*quater* et 17*quinquies* de la présente loi et de l'article [4§ 4] de la [loi du [XX] établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité

de openbare veiligheid]] en onverminderd de toepassing van het internationaal stelsel van de waarborgen."

Art. 5

De Koning bepaalt de datum van inwerkingtreding van de bepalingen van deze wet.

Gegeven te Brussel, 27 september 2018

FILIP

VAN KONINGSWEGE:

de minister van Veiligheid en Binnenlandse Zaken,

Jan JAMBON

publique] et sans préjudice de l'application du régime international de garanties."

Art. 5

Le Roi fixe la date d'entrée en vigueur des dispositions de la présente loi

Donné à Bruxelles, le 27 septembre 2018

PHILIPPE

PAR LE ROI:

le ministre de la Sécurité et de l'Intérieur,

Jan JAMBON

Coördinatie van de artikelen	
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	**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**
Hoofdstuk I Algemene bepalingen	
Artikel 1	Artikel 1
Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder: –ioniserende stralingen: stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken; –radioactieve stof: elke stof [of elk materiaal die/dat] één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd; –bevoegde overheid: [de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten]; –[algemeen reglement: het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;] –erkende instellingen: de instellingen die door het algemeen reglement met bepaalde taken worden belast; –dienst voor fysische controle: de dienst die krachtens het algemeen reglement door de bedrijfsleider moet worden opgericht en die belast is met de organisatie van en het toezicht op de maatregelen die nodig zijn om de bepalingen van dat reglement te doen naleven; –het Agentschap: de openbare instelling opgericht door deze wet voor de nucleaire controle; –[kernmateriaal: de volgende bijzondere splijtbare producten en kerngrondstoffen: a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233: elk product dat één of meerdere van de hierboven vermelde isotopen bevat. Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium; b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten; –nationaal nucleair vervoer: het vervoer, met om het	Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder: –ioniserende stralingen: stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken; –radioactieve stof: elke stof [of elk materiaal die/dat] één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd; –bevoegde overheid: [de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten]; –[algemeen reglement: het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen;] –erkende instellingen: de instellingen die door het algemeen reglement met bepaalde taken worden belast; –dienst voor fysische controle: de dienst die krachtens het algemeen reglement door de bedrijfsleider moet worden opgericht en die belast is met de organisatie van en het toezicht op de maatregelen die nodig zijn om de bepalingen van dat reglement te doen naleven; –het Agentschap: de openbare instelling opgericht door deze wet voor de nucleaire controle; –[kernmateriaal: de volgende bijzondere splijtbare producten en kerngrondstoffen: a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233: elk product dat één of meerdere van de hierboven vermelde isotopen bevat. Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium; b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten;

even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt; –internationaal nucleair vervoer: het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expediteur in de Staat van oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming; –fysieke beveiligingsmaatregelen: alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel [de nucleaire documenten] te beschermen tegen voornoemde handelingen; –[beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel: a)om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; b)om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: 1)de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan; 2)de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer;] –[beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel: a)om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; b)om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: 1)voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties; 2)de inrichtingen waar deze toestellen of installaties zich bevinden;] –[sabotage: alle opzettelijke handelingen: a)die zijn gericht tegen: 1)kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan; 2)nucleaire installaties; 3)het nationaal of internationaal nucleair vervoer; 4)radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan; 5)inrichtingen of delen van inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt;	–nationaal nucleair vervoer: het vervoer, met om het even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt; –internationaal nucleair vervoer: het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expediteur in de Staat van oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming; –fysieke beveiligingsmaatregelen: alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel [de nucleaire documenten] te beschermen tegen voornoemde handelingen; –[beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel: a)om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; b)om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: 1)de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan; 2)de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer;] –[beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel: a)om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; b)om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: 1)voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties; 2)de inrichtingen waar deze toestellen of installaties zich bevinden;] –[sabotage: alle opzettelijke handelingen: a)die zijn gericht tegen: 1)kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan; 2)nucleaire installaties; 3)het nationaal of internationaal nucleair vervoer; 4)radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan; 5)inrichtingen of delen van inrichtingen waar

6)toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; 7)het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; 8)inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; En b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen;] –nucleaire inspecteurs: de directeur-generaal en de leden van het departement toezicht en controle van het Agentschap die een zelfde of een hogere rang hebben als de deskundigen bij voornoemde instelling en die door de Koning worden aangeduid;] –[beroepshalve blootgestelde persoon: iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; –aan dosimetrisch toezicht onderworpen persoon: iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; –exploitant: elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17;– -externe onderneming: elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden;– -erkende geneesheer: de preventieadviseur-arbeidsgeneesheer werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien erkend is overeenkomstig de uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19; -externe werker: iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige; -opdracht met blootstellingsrisico: de activiteit van ongeacht welke aard, van een externe werker bij een	radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt; 6)toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; 7)het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; 8)inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; En b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen;] –nucleaire inspecteurs: de directeur-generaal en de leden van het departement toezicht en controle van het Agentschap die een zelfde of een hogere rang hebben als de deskundigen bij voornoemde instelling en die door de Koning worden aangeduid;] –[beroepshalve blootgestelde persoon: iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; –aan dosimetrisch toezicht onderworpen persoon: iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; –exploitant: elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17;– -externe onderneming: elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden;– -erkende geneesheer: de preventieadviseur-arbeidsgeneesheer werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien erkend is overeenkomstig de uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19; -externe werker: iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige;

exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden; -blootstellingsregister: het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosime-trisch toezicht onderworpen personen bevat;– -stralingspaspoort: het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland;– -beroepsbeoefenaar in de gezondheidszorg: de beroepsbeoefenaar in de gezondheidszorg bedoeld in artikel 7, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals aangesteld binnen het Agentschap. Zolang geen uitvoering wordt gegeven aan de voormelde bepaling van de wet van 8 december 1992, wordt begrepen onder'beroepsbeoefenaar in de gezondheidszorg': de persoon die houder is van het wettelijk diploma van doctor in de genees-, heel- en verloskunde;– -consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer: de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap;– -verantwoordelijke voor de verwerking: de persoon bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in casu het Agentschap; -vestigingseenheid: een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend;– -werknemer: de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;– -werkgever: de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; -dosimetrisch toezicht: het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement;– -authentieke bronnen: het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid;	-opdracht met blootstellingsrisico: de activiteit van ongeacht welke aard, van een externe werker bij een exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden; -blootstellingsregister: het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosime-trisch toezicht onderworpen personen bevat;– -stralingspaspoort: het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland;– -beroepsbeoefenaar in de gezondheidszorg: de beroepsbeoefenaar in de gezondheidszorg bedoeld in artikel 7, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals aangesteld binnen het Agentschap. Zolang geen uitvoering wordt gegeven aan de voormelde bepaling van de wet van 8 december 1992, wordt begrepen onder'beroepsbeoefenaar in de gezondheidszorg': de persoon die houder is van het wettelijk diploma van doctor in de genees-, heel- en verloskunde;– -consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer: de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap;– -verantwoordelijke voor de verwerking: de persoon bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in casu het Agentschap; -vestigingseenheid: een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend;– -werknemer: de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk;– -werkgever: de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; -dosimetrisch toezicht: het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement;– -authentieke bronnen: het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid;

[...]] -[vermogensreactor: een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de bescherming tegen ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd.]	[...]] -[vermogensreactor: een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de bescherming tegen ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd.] -Nucleaire cyberbeveiliging: De beveiliging van netwerk- en informatiesystemen van nucleaire installaties en inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, of waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is. -Netwerk- en informatiesysteem: 1. een elektronisch communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie; 2. een apparaat of groep van permanente of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische bestanddelen van dit apparaat die onder meer de automatisering van een operationeel proces mogelijk maken, alsook de controle op afstand of het verkrijgen van werkingsgegevens in real time; 3. of digitale gegevens die via de in de punten 1) en 2) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan. -Beveiliging van netwerk- en informatiesystemen: Het vermogen van netwerken en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen. -Cyberincident: Elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen; -Cyberrisico: Elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen.”

Artikel 1bis	
Artikel 2	
Artikel 2bis	
Artikel 2ter	
Hoofdstuk II Bevoegde overheid	
Artikel 3	
Artikel 4	
Artikel 5	
Artikel 6	
Artikel 7	
Artikel 8	
Artikel 9	
Artikel 9bis	
Artikel 10	
Artikel 10bis	
Artikel 10ter	
Artikel 10quater	
Artikel 10quinquies	
Artikel 10sexies	
Artikel 10septies	
Artikel 11	
Artikel 12 [...]	
Artikel 13 [...]	
Hoofdstuk III Opdrachten van het Agentschap	
Afdeling 1 Algemene opdrachtomschrijving	
Artikel 14	
Artikel 15 [Algemeen gesteld omvat de opdracht van het Agentschap de onderzoekingen die dienstig zijn voor	

het omschrijven van alle exploitatievoorwaarden van de inrichtingen waarin ioniserende stralingen worden aangewend en tot het bestuderen van de veiligheid en de beveiliging van de inrichtingen waarin [kernmateriaal of radioactieve stoffen] worden aangewend of bewaard.] Deze opdracht omvat ook het toezicht, de controles en de inspecties die eruit voortvloeien, de stralingsbescherming, de opleiding en de voorlichting, de contacten met de overheid en met de betrokken nationale instellingen en de interventies in noodgevallen. Het Agentschap verleent zijn technische medewerking aan de minister bevoegd voor Buitenlandse Zaken. [Onverminderd de toepassing van artikel 8 van deze wet is het Agentschap eveneens belast met de controle op de fysieke beveiligingsmaatregelen [, de beveiligingsmaatregelen voor radioactieve stoffen, met uitzondering van het kernmateriaal, opgesteld krachtens artikel 17quater en de beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, opgesteld krachtens artikel 17quinquies].]	Algemeen gesteld omvat de opdracht van het Agentschap de onderzoekingen die dienstig zijn voor het omschrijven van alle exploitatievoorwaarden van de inrichtingen waarin ioniserende stralingen worden aangewend en tot het bestuderen van de veiligheid en de beveiliging van de inrichtingen waarin [kernmateriaal of radioactieve stoffen] worden aangewend of bewaard.] Deze opdracht omvat ook het toezicht, de controles en de inspecties die eruit voortvloeien, de stralingsbescherming, de opleiding en de voorlichting, de contacten met de overheid en met de betrokken nationale instellingen en de interventies in noodgevallen. Het Agentschap verleent zijn technische medewerking aan de minister bevoegd voor Buitenlandse Zaken. [Onverminderd de toepassing van artikel 8 van deze wet is het Agentschap eveneens belast met de controle op de fysieke beveiligingsmaatregelen [, de beveiligingsmaatregelen voor radioactieve stoffen, met uitzondering van het kernmateriaal, opgesteld krachtens artikel 17quater en de beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, opgesteld krachtens artikel 17quinquies].] "Onverminderd de artikelen 15bis en 15ter van deze wet is het Agentschap eveneens belast met de controle op de nucleaire cyberbeveiligingsmaatregelen."
Afdeling 2 Bevoegdheid inzake de vergunning van inrichtingen	
Artikel 16	
Artikel 17	
Afdeling 3 Bevoegdheid inzake fysieke beveiliging van kernmateriaal	
Artikel 17bis	
Artikel 17ter	
Afdeling 3bis Bevoegdheid op het gebied van de beveiliging van de radioactieve stoffen met uitzondering van het kernmateriaal	
Artikel 17quater	
Afdeling 3ter Bevoegdheid inzake de beveiliging van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is	
Artikel 17quinquies	

	« Afdeling 3quater – Bevoegdheid op het gebied van de nucleaire cyberbeveiliging Art. 17sexies §1.Op voorstel van het Agentschap en na advies van de door de Koning aangeduide autoriteiten: 1° Verdeelt de Koning de **netwerk- en informatiesystemen van de installaties en de inrichtingen waarop de nucleaire cyberbeveiliging zoals omschreven in artikel 1, gericht is**, voor zover deze netwerk- en informatiesystemen het beheer, de controle of de veiligstelling van het kernmateriaal, de radioactieve stoffen, of de toestellen en installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is, voor deze installaties of deze inrichtingen, rechtstreeks of onrechtstreeks mogelijk maken, waarborgen of ondersteunen, **in categorieën, op basis van het cyberrisico dat eraan verbonden is.** 2° bepaalt de Koning het beveiligingsniveau van de **netwerk- en informatiesystemen bedoeld in punt 1°;** 3° bepaalt de Koning de noodzakelijke en evenredige nucleaire cyberbeveiligingsmaatregelen voor het beheer van de cyberrisico's van de categorieën van netwerk- en informatiesystemen bedoeld in punt 1° die, in het licht van de bestaande kennis, met het hoogste cyberrisico overeenstemmen en voor het voorkomen van cyberincidenten die hierop van invloed kunnen zijn, of om de impact ervan te beperken, onverminderd de toepassing van het internationaal stelsel van de waarborgen. Deze maatregelen regelen met name de melding aan het Agentschap en aan de door de Koning aangeduide autoriteiten, van cyberincidenten met een significante impact die door de exploitant van de door deze maatregelen bedoelde installatie of inrichting moet worden gedaan; 4° regelt de Koning de uitwisseling tussen het Agentschap en de door de Koning aangewezen autoriteiten van de gegevens waarover ze beschikken in verband met de cyberrisico's en de cyberincidenten waarmee de exploitant wordt of kan worden geconfronteerd. 5° bepaalt de Koning de erkenningsprocedure voor de nucleaire cyberbeveiligingsmaatregelen bedoeld in punt 3°. §2. – Het Agentschap bepaalt, na advies van de door de Koning aangewezen autoriteiten, de principes voor de nucleaire cyberbeveiligingsmaatregelen inzake behoedzaam beheer voor de categorieën van netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, die met het laagste cyberrisico overeenstemmen. §3. – Het Agentschap kan de in paragraaf 1, 4°,

	bedoelde erkenningen aan voorwaarden onderwerpen. Het Agentschap kan deze erkenningen en de hierin opgelegde voorwaarden, te allen tijde, op eigen initiatief en op gemotiveerde wijze, wijzigen of aanvullen, indien deze wijzigingen of aanvullingen bedoeld zijn om de naleving te garanderen van de door of krachtens de wet voorziene eisen inzake de nucleaire cyberbeveiliging en deze wijzigingen of aanvullingen kennelijk gepast, evenredig en billijk zijn. §4.Het Agentschap is voor de netwerk- en informatiesystemen bedoeld in paragraaf 1, 1°, belast met: 1° het informeren van de exploitanten van de installaties en inrichtingen bedoeld in paragraaf 1, 1°, over de cyberrisico's waarvan het op de hoogte is en die betrekking hebben op de netwerk- en informatiesystemen, of de daaraan gerelateerde diensten; 2° het verrichten van analyses en technisch onderzoeken ten behoeve van de in de punt 1° bedoelde opdrachten naar aanleiding van cyberrisico's of cyberincidenten, of van elementen die daarop wijzen, die niet bestaan in het onderzoek, of verplichtingen die door de gerechtelijke overheid werden opgelegd met het oog op de identificatie van personen of organisaties die voor deze cyberrisico's en cyberincidenten verantwoordelijk zijn, of daar anderszins aan bijdragen of hebben bijgedragen; 3° het informeren en sensibiliseren van gebruikers van deze netwerk- en informatiesystemen. Het Agentschap doet hiertoe een beroep op de samenwerking, het advies en de ervaring van de door de Koning aangewezen autoriteiten. De Koning kan, op voordracht van het Agentschap, dat het advies inwint van de door hem aangeduide autoriteiten, de nadere regelen voor de toepassing van deze paragraaf bepalen. §5. Dit artikel is van toepassing onverminderd de artikelen 15bis, [[15ter]], 17bis, 17quater en 17quinquies van deze wet en artikel 4§4 van [[de wet van [xx] tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid]] en onverminderd de toepassing van het internationaal stelsel van de waarborgen.»

Coordination des articles

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	**PROJET DE LOI PORTANT MODIFICATION DE LA LOI DU 15 AVRIL 1994 RELATIVE A LA PROTECTION DE LA POPULATION ET DE L'ENVIRONNEMENT CONTRE LES DANGERS RESULTANT DES RAYONNEMENTS IONISANTS ET RELATIVE A L'AGENCE FEDERALE DE CONTROLE NUCLEAIRE CONCERNANT LA CYBERSECURITE NUCLEAIRE**
Chapitre I.er Dispositions générales	
Article 1.er	**Article 1.er**
Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par: –rayonnements ionisants: rayonnements composés de photons ou de particules capables de déterminer la formation d'ions directement ou indirectement; –substance radioactive: toute substance [ou toute matière] contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection; –autorités compétentes: [les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution]; –[règlement général: l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;] –organismes agréés: les organismes chargés de certaines missions par le règlement général; –service de contrôle physique: le service qu'est tenu d'organiser le chef d'entreprise en vertu du règlement général, qui est chargé de l'organisation et de la surveillance des mesures nécessaires pour assurer l'observation des dispositions dudit règlement; –l'Agence: l'établissement public créé par la présente loi pour le contrôle nucléaire; –[matières nucléaires: les produits fissiles spéciaux et les matières brutes suivantes: a)les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou 233; tout produit contenant un ou plusieurs des isotopes ci-dessus. L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel; b)les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés; –transport nucléaire national: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge; –transport nucléaire international: le transport de	Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par: –rayonnements ionisants: rayonnements composés de photons ou de particules capables de déterminer la formation d'ions directement ou indirectement; –substance radioactive: toute substance [ou toute matière] contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection; –autorités compétentes: [les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution]; –[règlement général: l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants;] –organismes agréés: les organismes chargés de certaines missions par le règlement général; –service de contrôle physique: le service qu'est tenu d'organiser le chef d'entreprise en vertu du règlement général, qui est chargé de l'organisation et de la surveillance des mesures nécessaires pour assurer l'observation des dispositions dudit règlement; –l'Agence: l'établissement public créé par la présente loi pour le contrôle nucléaire; –[matières nucléaires: les produits fissiles spéciaux et les matières brutes suivantes: a)les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou 233; tout produit contenant un ou plusieurs des isotopes ci-dessus. L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel; b)les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés; –transport nucléaire national: le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge; –transport nucléaire international: le transport de

matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale ; –mesures de protection physique: toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités [les documents nucléaires]; –[mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: a)de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol ; b)de protéger contre les risques de sabotage ou de toute utilisation malveillante: 1)les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage; 2)les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport;] –[mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: a)de protéger les dits appareils ou installations contre les risques de détention illicite et de vol; b)de protéger contre les risques de sabotage ou de toute utilisation malveillante: 1)lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations; 2)les établissements et lieux où se trouvent ces appareils et installations;] –[sabotage: tout acte délibéré: a)qui est dirigé contre: 1)des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport; 2)des installations nucléaires; 3)des transports nucléaires nationaux ou internationaux; 4)des substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation, d'entreposage ou de transport; 5)des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées; 6)des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; 7)le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de	matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale ; –mesures de protection physique: toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités [les documents nucléaires]; –[mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: a)de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol ; b)de protéger contre les risques de sabotage ou de toute utilisation malveillante: 1)les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage; 2)les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport;] –[mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: a)de protéger les dits appareils ou installations contre les risques de détention illicite et de vol; b)de protéger contre les risques de sabotage ou de toute utilisation malveillante: 1)lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations; 2)les établissements et lieux où se trouvent ces appareils et installations;] –[sabotage: tout acte délibéré: a)qui est dirigé contre: 1)des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport; 2)des installations nucléaires; 3)des transports nucléaires nationaux ou internationaux; 4)des substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation, d'entreposage ou de transport; 5)des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées; 6)des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; 7)le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de

substances radioactives; 8)des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; Et b)qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives;] –inspecteurs nucléaires: le directeur général et les membres du département contrôle et surveillance de l'Agence revêtus d'un grade égal à ou supérieur à celui d'expert à cette institution et désignés par le Roi;]	substances radioactives; 8)des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; Et b)qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives;] –inspecteurs nucléaires: le directeur général et les membres du département contrôle et surveillance de l'Agence revêtus d'un grade égal à ou supérieur à celui d'expert à cette institution et désignés par le Roi;]
-[personne professionnellement exposée: chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;	-[personne professionnellement exposée: chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;
-personne soumise à la surveillance dosimétrique: chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;	-personne soumise à la surveillance dosimétrique: chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public;
-exploitant: toute personne physique ou morale qui assume la responsabilité de l'établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17;	-exploitant: toute personne physique ou morale qui assume la responsabilité de l'établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17;
-entreprise extérieure: toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel;	-entreprise extérieure: toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel;
-médecin agréé: le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19;	-médecin agréé: le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19;
-travailleur extérieur: toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant;	-travailleur extérieur: toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant;

-mission comportant un risque d'exposition: l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée;	-mission comportant un risque d'exposition: l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée;
-registre d'exposition: le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2	-registre d'exposition: le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2
-passeport radiologique: le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger;	-passeport radiologique: le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger;
-professionnel des soins de santé: le professionnel des soins de santé visé à l'article 7, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence. Tant que les mesures d'exécution de la disposition précitée de la loi du 8 décembre 1992 ne sont pas prises, on entend par professionnel des soins de santé': la personne titulaire du diplôme légal de docteur en médecine, chirurgie et accouchements;	-professionnel des soins de santé: le professionnel des soins de santé visé à l'article 7, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence. Tant que les mesures d'exécution de la disposition précitée de la loi du 8 décembre 1992 ne sont pas prises, on entend par professionnel des soins de santé': la personne titulaire du diplôme légal de docteur en médecine, chirurgie et accouchements;
-consultant en sécurité de l'information et protection de la vie privée: le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence;	-consultant en sécurité de l'information et protection de la vie privée: le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence;
-responsable du traitement: la personne visée à l'article 1.er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence;	-responsable du traitement: la personne visée à l'article 1.er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence;
-unité d'implantation: le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée;	-unité d'implantation: le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée;
-travailleur: le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;	-travailleur: le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;
-employeur: l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;	-employeur: l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail;
-surveillance dosimétrique: la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général;	-surveillance dosimétrique: la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général;
-sources authentiques: le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de	-sources authentiques: le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant

guichets-entreprises agréés et portant diverses dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale;	création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale;
[...]]	[...]]
-[réacteur de puissance: un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée.]	-[réacteur de puissance: un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée.] -Mesures de cybersécurité nucléaire : Les mesures relatives à la sécurité des réseaux et des systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives, à des fins de cyber-sécurité nucléaire. -Cybersécurité nucléaire : La sécurité des réseaux et systèmes d'information des installations nucléaires et des établissements où des substances radioactives sont produites, fabriquées, détenues ou utilisées, ou où se trouvent des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives ; -Réseau et système d'information 1. un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques; 2. un dispositif ou un ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation d'un processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel; 3. ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points 1) et 2) en vue de leur fonctionnement, leur utilisation, leur protection et leur maintenance. -Sécurité des réseaux et des systèmes d'information : La capacité des réseaux et des systèmes d'information de résister, à un niveau de fiabilité donné, à des actions qui compromettent la disponibilité,

	l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles. -Cyber-incident : Tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information. - Cyber-risques : Toute circonstance ou tout événement raisonnablement identifiable ayant une incidence négative potentielle sur la sécurité des réseaux et des systèmes d'information. »
Article 1.erbis **Article 2** **Article 2bis** **Article 2ter** **Chapitre II Autorités compétentes** **Article 3** **Article 4** **Article 5** **Article 6** **Article 7** **Article 8** **Article 9** **Article 9bis** **Article 10** **Article 10bis** **Article 10ter** **Article 10quater** **Article 10quinquies** **Article 10sexies** **Article 10septies** **Article 11** **Chapitre III Des missions de l'Agence**	

Section 1.re Description générale de la mission	
Article 14	
Article 14bis	
Article 14quater	
Article 15 [D'une manière générale, la mission de l'Agence comprend les investigations utiles à la définition de toutes les conditions d'exploitation des établissements où sont mis en œuvre des rayonnements ionisants et à l'étude de la sécurité et de la sûreté des établissements où sont utilisées ou détenues [des matières nucléaires ou des substances radioactives].] Elle comprend également la surveillance, les contrôles et les inspections qui en découlent, la radioprotection, la formation et l'information, les contacts avec les autorités et les organismes nationaux concernés et des interventions en cas d'urgence. L'Agence prête son concours technique au ministre qui a les Affaires étrangères dans ses attributions. [Sans préjudice de l'article 8 de cette loi, l'Agence est également chargée du contrôle des mesures de protection physique [, des mesures de sécurité pour les substances radioactives autres que les matières nucléaires arrêtées en vertu de l'article 17quater et des mesures de sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives arrêtées en vertu de l'article 17quinquies].]	[D'une manière générale, la mission de l'Agence comprend les investigations utiles à la définition de toutes les conditions d'exploitation des établissements où sont mis en œuvre des rayonnements ionisants et à l'étude de la sécurité et de la sûreté des établissements où sont utilisées ou détenues [des matières nucléaires ou des substances radioactives].] Elle comprend également la surveillance, les contrôles et les inspections qui en découlent, la radioprotection, la formation et l'information, les contacts avec les autorités et les organismes nationaux concernés et des interventions en cas d'urgence. L'Agence prête son concours technique au ministre qui a les Affaires étrangères dans ses attributions. [Sans préjudice de l'article 8 de cette loi, l'Agence est également chargée du contrôle des mesures de protection physique [, des mesures de sécurité pour les substances radioactives autres que les matières nucléaires arrêtées en vertu de l'article 17quater et des mesures de sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives arrêtées en vertu de l'article 17quinquies].]Sans préjudice des articles 15bis et 15ter de la présente loi , l'Agence est également chargée du contrôle des mesures de cybersécurité nucléaire. »
Article 15bis	
Section 2 Compétence en matière d'autorisation des établissements	
Article 16	
Article 17	
Section 3 Compétence en matière de protection physique des matières nucléaires	
Article 17bis	
Article 17ter	
Section 3bis Compétence en matière de sécurité des substances radioactives	

autres que les matières nucléaires **Article 17quater** **Section 3ter Compétence en matière de sécurité des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives** **Article 17quinquies**	« Section 3quater- Compétence en matière de cybersécurité nucléaire Art. 17sexies §1er. Sur proposition de l'Agence, et après avis des autorités désignées par le Roi : 1° le Roi répartit en catégories , en fonction du cyber-risque qu'ils présentent, les réseaux et systèmes d'information des installations et des établissements que vise la cybersécurité nucléaire telle que définie à l'article 1er , dans la mesure où ces réseaux et systèmes d'information, pour ces installations ou ces établissements, permettent directement ou indirectement, assurent ou appuient la gestion, le contrôle ou la sécurisation des matières nucléaires, des substances radioactives ou des appareils et installations émettant des rayonnements ionisants ne provenant pas de substances radioactives. 2° le Roi détermine le niveau de sécurité des réseaux et systèmes d'information visés au point 1° ; 3° le Roi détermine les mesures de cybersécurité nucléaire nécessaires et proportionnées pour gérer les cyber-risques des catégories des réseaux et systèmes d'information visés au point 1° 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, sans préjudice de l'application du régime international de garanties. Ces mesures règlent notamment la notification à l'Agence ainsi qu' aux autorités désignées par le Roi, des cyber-incidents ayant un impact significatif que l'exploitant d'une installation ou d'un établissement visé par ces mesures doit effectuer ; 4° le Roi règle l'échange entre l'Agence et les autorités désignées par le Roi des données qu'elles possèdent sur les cyber-risques et sur les cyber-incidents auxquels l'exploitant est ou peut être confronté.

	5° le Roi détermine la procédure d'agrément des mesures de cybersécurité nucléaire visées au point 3°. §2.- L'Agence détermine, après avis des autorités désignées par le Roi, les principes des mesures de cybersécurité nucléaire de gestion prudente pour les catégories des réseaux et systèmes d'information visés au paragraphe 1, 1°, correspondant au cyber-risque le moins élevé. §3.- L'Agence peut subordonner les agréments visés au paragraphe 1er, 4°, à des conditions. L'Agence peut en tout temps modifier ou compléter, d'initiative et de manière motivée, ces agréments et les conditions qui leur sont imposées, si ces modifications ou compléments visent à assurer le respect des exigences prévues par ou en vertu de la loi et en relation avec la cybersécurité nucléaire et si ces modifications ou compléments sont manifestement appropriés, proportionnés et équitables. § 4.- L'Agence est chargée, pour les réseaux et systèmes d'information visés au paragraphe 1, 1°: 1°. d'informer les exploitants des installations et des établissements visés au paragraphe 1, 1°, des cyber-risques dont elle a connaissance et qui sont en lien avec leurs réseaux et systèmes d'information, ou les services connexes ; 2°. de réaliser, en présence de cyber-risques ou de cyber-incidents ou de tout élément donnant à penser qu'ils existent, des analyses et des enquêtes techniques bénéficiant aux missions visées au point 1°, en dehors de l'instruction ou de devoirs prescrits par l'autorité judiciaire visant à identifier les personnes ou organisations qui sont responsables de ces cyber-risques ou cyber incidents, ou qui y contribuent ou y ont contribué de quelque manière que ce soit. 3° d'informer et de sensibiliser les utilisateurs de ces réseaux et systèmes d'information. A cette fin, l'Agence recourt à la collaboration, à l'avis et à l'expérience des autorités désignées par le Roi. Le Roi peut déterminer les modalités de l'application du présent paragraphe sur proposition de l'Agence, qui sollicite l'avis des autorités qu'il désigne. §5.- Le présent article s'applique sans préjudice des articles 15bis, [[15ter]], 17bis, 17quater et 17quinquies de la présente loi et de l'article [4§4] de la [loi du [XX] établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique] et sans préjudice de l'application du régime international de garanties.»