DOC 54 **2274/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

20 januari 2017

HOORZITTING

De cyberveiligheid van de kerncentrales in België

VERSLAG

NAMENS DE SUBCOMMISSIE VOOR DE NUCLEAIRE VEILIGHEID UITGEBRACHT DOOR DE HEER **Eric THIÉBAUT**

INHOUD Blz.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

20 janvier 2017

AUDITION

La cybersécurité des centrales nucléaires en Belgique

RAPPORT

FAIT AU NOM DE LA SOUS-COMMISSION DE LA SÉCURITÉ NUCLÉAIRE PAR M. **Eric THIÉBAUT**

SOMMAIRE Pages

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

A. — Vaste leden / Titulaires:		**B. — Plaatsvervangers / Suppléants:**
Nieuw-Vlaamse Alliantie	Bert Wollants	Brecht Vermeulen
Parti Socialiste	Eric Thiébaut	Karine Lalieux
Mouvement Réformateur	David Clarinval	Denis Ducarme
Christen-Democratisch & Vlaams	Leen Dierick	N
Open Vlaamse liberalen en democraten	Egbert Lachaert	Katja Gabriëls
Socialistische partij anders	Peter Vanvelthoven	Karin Temmerman
Ecologistes Confédérés pour l'organisation de luttes originales	Kristof Calvo	Jean-Marc Nollet
Groen		
centre démocrate Humaniste	Michel de Lamotte	Vanessa Matz

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

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

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

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

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

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

Les publications sont imprimées exclusivement sur du papier certifié FSC

DAMES EN HEREN,

Deze hoorzitting heeft in uw commissie plaatsgevonden op 22 november 2016.

I. — **HOORZITTING MET DE HEER MIGUEL DE BRUYCKER, DIRECTEUR VAN HET CENTRUM VOOR CYBERSECURITY BELGIË**

A. **Inleidende uiteenzetting door de heer Miguel de Bruycker, directeur van het Centrum voor Cybersecurity België**

De heer Miguel de Bruycker, directeur van het Centrum voor Cybersecurity België, schetst eerst het bij een koninklijk besluit bepaalde wettelijke kader waarbinnen het Centrum functioneert. Overeenkomstig dit wettelijk kader is het Centrum belast met de opvolging en de coördinatie van het Belgisch beleid inzake cyberveiligheid en met het toezicht op de uitvoering ervan. Het beheert vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid. Het verzekert tevens de coördinatie tussen de betrokken diensten en overheden, alsook tussen de publieke overheden en de private en de wetenschappelijke sector. Het Belgisch beleid steunt dus op een gecoördineerde en geïntegreerde benadering inzake cyberveiligheid.

Het Centrum formuleert voorstellen tot aanpassing van het wet- en regelgevend kader op het vlak van cyberveiligheid. Het verzekert het crisisbeheer bij cyberincidenten, in samenwerking met het Coördinatie- en Crisiscentrum van de regering. Het werkt richtlijnen en veiligheidsnormen uit voor de verschillende informaticasystemen van de administraties en publieke instellingen, verspreidt deze en ziet erop toe dat ze in acht worden genomen. Het coördineert de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, de opvolging van internationale verplichtingen en de presentatie van het nationale standpunt ter zake. Ook coördineert het de evaluatie en certificatie van de veiligheid van de informatie- en communicatiesystemen. Bovendien informeert en sensibiliseert het Centrum de gebruikers van de informatie- en communicatiesystemen.

De doelgroepen van de acties van het Centrum zijn de bevolking, de ondernemingen en de vitale sectoren.

Ten eerste is het noodzakelijk in te zetten op bewustmaking van de bevolking, wat een kerntaak is. Bovendien is er het project *"Botnet eradication"*, gezien de ernstige bedreiging voor de burger. Het Centrum biedt voorts een beter informatieportaal en het neemt

MESDAMES, MESSIEURS,

Cette audition s'est tenue dans votre commission le 22 novembre 2016.

I. — **AUDITION DE M. MIGUEL DE BRUYCKER, DIRECTEUR DU CENTRE CYBERSÉCURITÉ BELGIQUE**

A. **Exposé introductif de M. Miguel de Bruycker, directeur du Centre Cybersécurité Belgique**

M. Miguel de Bruycker, directeur du Centre Cybersécurité Belgique revient tout d'abord sur le cadre légal, basé sur un arrêté royal, dans lequel fonctionne le Centre. En vertu de ce cadre légal, le Centre vise à superviser, coordonner et à veiller à la mise en œuvre de la stratégie belge en la matière; il doit gérer par une approche intégrée et centralisée les différents projets relatif à la cybersécurité. Il doit assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique. La Belgique fonctionne donc sur base d'une approche coordonnée et intégrée en matière de cybersécurité.

Le Centre formule des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité. Il veille à assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement. Il élabore, diffuse et veille à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics; il coordonne la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière. Il coordonne l'évaluation et la certification de la sécurité des systèmes d'information et de communication. En outre, il informe et sensibilise les utilisateurs des systèmes d'information et de communication.

L'orateur précise que les groupes cibles pour lesquels le Centre travaille sont la population, les entreprises et les secteurs vitaux.

Premièrement, il s'agit de conscientiser la population, ce qui est une mission essentielle. En outre, il y a un projet de "*Botnet eradication*", vu l'importante menace pour le citoyen. Il y a aussi un meilleur portail d'informations. Le Centre participe aussi à un projet

deel aan het Europese *"Anti-Phishing"*-project, alsook aan het project *"No More Ransomware".*

Wat de bedrijfswereld betreft, wijst de spreker op het *"Webinars"*-project, dat bestaat in een dertigtal gratis online-cursussen met een duur van 10 tot 30 minuten. De gids voor kmo's is bovendien bijna klaar en zal nog dit jaar aan de kmo's worden aangeboden. Voorts worden partnerschappen gesloten met de bedrijven en ziet het Centrum toe op het aanbieden van betrouwbare technologieën.

De vitale sectoren behelzen met name de kritische infrastructuur, de overheid, de volksgezondheid enzovoort. De voornaamste projecten in dat verband zijn:

— *"early warning system"*: het is cruciaal gevoelige informatie en informatie over incidenten voortdurend te delen;

— de opsporing van anomalieën: via een centrale databank waarin alle diensten hun gegevens kunnen invoeren, die automatisch gedeeld zullen worden met de operatoren van de noodzakelijke diensten. Op basis van een samenwerkingsakkoord met Luxemburg en van een risicoanalysetool analyseert het Centrum de vijf belangrijkste bedreigingen, afhankelijk van het gevoeligheidsniveau van de installatie. Die vijf bedreigingen zijn: externe bedreiging, interne bedreiging – door een ontevreden werknemer dan wel door een menselijke fout – rampen en technische mankementen;

— voorts is een *"baseline security norm"*-project van start gegaan. Elke sector werkt voor zichzelf een dergelijke norm uit. Het Centrum is van mening dat er een overkoepelende standaardnorm moet bestaan voor de verschillende sectoren. Dit project zal worden uitgewerkt in samenwerking met de sectoren en op internationaal niveau. Het is belangrijk een gemeenschappelijke internationale norm te bereiken;

— samen met het Crisiscentrum werd een noodplan uitgewerkt voor de aanpak van incidenten.

De spreker benadrukt dat de verantwoordelijkheid voor de cyberveiligheid in de eerste plaats de operator zelf toekomt. De overheid heeft een normatieve, ondersteunende en controlerende rol. Bovendien is het parket belast met de instructies dienaangaande.

Tussen 2016 en 2018 zullen meer dan twintig projecten worden gelanceerd. De spreker vermeldt CERT.BE (integratie en versterking van de CERT-capaciteiten in het CCB). Het *"National cyber security emergency plan"* werd uitgewerkt met verschillende actoren, waaronder het crisiscentrum. Het beschrijft de verschillende

européen d' *"Anti-Phishing"*, ainsi qu'au projet "*No More Ransomware".*

Concernant les entreprises, l'orateur mentionne le projet "*Webinars*", consistant en une trentaine de cours en ligne gratuits d'une durée de 10 à 30 minutes. Par ailleurs, le guide PME est presque prêt et sera mis à disposition des PME cette année encore. En outre, il y a des partenariats conclus avec les entreprises, et le Centre veille à fournir des technologies fiables.

Les secteurs vitaux concernent notamment les infrastructures critiques, les autorités, la santé publique etc. Les projets principaux dans cette optique sont:

— *"early warning system*": il est crucial de partager en permanence les informations sensibles et les informations sur les incidents;

— la détection d'anomalies: via une base de données centrale dans laquelle tous les services peuvent entrer leurs données et qui seront automatiquement partagées avec les opérateurs des services essentiels. Sur base d'un accord de coopération avec le Luxembourg, et d'un outil d'analyse des risques, le Centre examine les cinq menaces principales en fonction du niveau de sensibilité de l'installation. Il s'agit de la menace extérieure, de la menace interne – d'une part du travailleur mécontent et d'autre part de l'erreur humaine – , des calamités et des failles techniques;

— en outre, un projet de "*Baseline security norm*" a démarré. Chaque secteur travaille à une telle norme pour son secteur. Le Centre est d'avis qu'il faut disposer d'une norme standard qui chapeaute les différents secteurs. Ce projet se fera en collaboration avec les secteurs et au niveau international. Il est important de pouvoir arriver à une norme commune au niveau international;

— un plan d'urgence pour le traitement des incidents a été élaboré avec le Centre de crise.

L'orateur insiste sur le fait que la responsabilité de la cybersécurité incombe en premier lieu à l'opérateur lui-même. Les autorités ont un rôle normatif, de soutien et de contrôle. Par ailleurs, c'est le parquet qui est en charge des instructions en la matière.

Plus d'une vingtaine de projets seront lancés entre 2016 et 2018. L'orateur mentionne le CERT.BE (l'intégration et le renforcement des capacités CERT dans le CCB). Le "*National cyber security emergency plan*" a été élaboré avec différents acteurs dont le centre de crise. Il décrit les différents types d'incidents, la manière

soorten incidenten, de manier waarop ze worden geevalueerd, ieders verantwoordelijkheden enzovoort. Wanneer zich een incident voordoet, moet enerzijds de schadelijke actie worden stopgezet, en anderzijds de dader gezocht. Deze twee elementen moeten worden gecoördineerd, onder meer om vernielingen van materiaal te voorkomen. Het komt echter niet de politie- en gerechtelijke diensten toe om uit te maken hoe de zaken moeten worden beveiligd.

De spreker citeert voorts de projecten inzake risicoanalyse en opleiding van deskundigen, het *Responsible disclosure policy* en het *Cyber diplomacy framework*, alsook, tot slot, het informatie-uitwisselingsplatform ISACS en de omzetting van de Europese richtlijn 2016/1148.

De heer de Bruycker bespreekt vervolgens de documenten over Tihange. Begin oktober 2016 werd het CCB ingelicht over het feit dat gevoelige informatie op het *dark web* stond. Het *deep web* en het *dark web* vormen dat deel van het internet dat niet via de traditionele zoekmotoren kan worden gevonden. Het gaat over meer dan 90 % van het internet. Die websites zijn toegankelijk voor de kenners, maar kunnen niet gegoogeld worden. Het gaat hier om gevoelige informatie die een potentieel risico kan vormen voor een kritieke infrastructuur. Het CCB heeft de Veiligheid van de Staat en ADIV derhalve gevraagd om de betrokken documenten op het *dark web* op te sporen. Dit onderzoek werd gecoördineerd door enerzijds het FANC en anderzijds de *Federal Computer Crime Unit* van de federale politie. Een spontane mededeling van een *ethical hacker* wees op het bestaan van documenten over gepubliceerde bestekken die iets te gevoelige informatie bevatten. Het CCB heeft een gespecialiseerd privébedrijf tegelijkertijd verzocht om diezelfde informatie op te sporen. Dat verzoek werd enerzijds gedaan wegens de vereiste technische capaciteiten en anderzijds omdat het een uitgelezen kans was om de toegevoegde waarde van dergelijke ondernemingen voor de Staat te evalueren.

De hoofddoelstelling van die initiatieven was om de eventuele veiligheidsrisico's ten gevolge van het lekken van documenten onverwijld tot nul te herleiden.

Die verschillende diensten hebben de documenten in kwestie niet gevonden, noch andere documenten die ernstige veiligheidsrisico's voor deze nucleaire installaties inhouden.

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

De heer Eric Thiébaut (PS) komt terug op de verklaringen van de Europees coördinator voor terrorismebestrijding, de heer Gilles de Kerchove, die een terreuraanslag

dont ils sont évalués, les responsabilités des uns et des autres etc. En cas d'incident, il y a d'une part le fait de mettre fin à l'action dommageable, et, d'autre part, la recherche de l'auteur. Ces deux éléments doivent être coordonnés, notamment pour éviter des destructions de matériel. Mais ce n'est pas aux autorités de police et de justice à dire la manière dont les choses doivent être sécurisées.

L'orateur cite aussi les projets consistants en l'analyse de risques et les formations d'experts, ainsi que la "*Responsible disclosure policy*" et le "*Cyber diplomacy framework*"; et la plateforme d'échange d'informations ISACS et la transposition de la directive européenne 2016/1148.

M. de Bruycker en vient ensuite aux documents concernant Tihange. Au début du mois d'octobre 2016, le CCB a été informé du fait que de l'information sensible était disponible sur le "*dark web*". Le "*deep web*" et "*dark web*" constituent la partie d'Internet introuvable via les moteurs de recherche classiques. Cela concerne plus de 90 % d'Internet. Il s'agit de sites internet accessibles par les connaisseurs, mais qu'on ne peut pas "*googler*". L'information sensible en question ici pouvait potentiellement engendrer un risque pour une infrastructure critique. Le CCB a donc fait une demande d'informations auprès de la Sûreté de l'État et du SGRS, afin de savoir s'ils trouvaient ces documents sur le "*dark web*". Une coordination a été réalisée avec, d'une part, l'AFCN, et d'autre part, la *"Federal Computer Crime Unit"* de la police fédérale. En outre, une communication spontanée a eu lieu de la part d'un "*ethical hacker*"; celle-ci concernait des documents sur des cahiers des charges publiés contenant des informations un peu trop sensibles. Le CCB a simultanément demandé à une entreprise privée spécialisée de rechercher cette même information, d'une part pour des raisons de capacités techniques et d'autre part car il s'agissait d'une opportunité d'évaluer la valeur ajoutée de ce type d'entreprise pour l'État.

L'objectif principal de ces initiatives était de réduire immédiatement les risques de sécurité éventuels par la fuite de documents.

Ces différentes instances n'ont pas trouvé les documents en question, ni aucun document contenant des risques de sécurité sérieux pour ces installations nucléaires.

B. **Questions et interventions des membres**

M. Eric Thiébaut (PS) revient sur les déclarations du coordinateur européen pour la lutte contre le terrorisme M. Gilles de Kerchove, selon qui il y a un risque

op kerncentrales en de mogelijkheid om kerncentrales via het internet onder controle te nemen, niet uitsluit. Hoe schat het CCB een en ander in?

De heer Michel de Lamotte (cdH) vraagt zich af waarom het CCB de privésector moest inschakelen. Kampt het met een capaciteits- en personeelstekort? Hoe is het met de algemene bekwaamheid van de medewerkers gesteld? Zou het voorts mogelijk zijn dat niet alle opties werden overwogen om dit onderzoek grondig te voeren? Werd de kwaliteit van deze onderzoeken gecontroleerd?

De heer Egbert Lachaert (Open Vld) vraagt of het CCB er zeker van kan zijn dat er geen voor de kerncentrales gevoelige documenten op het *dark web* hebben gestaan. Of moeten uit het feit dat niets werd gevonden, geen conclusies worden getrokken?

Is het feit dat onze centrales uit de jaren 1970 dateren en dus analoog – zonder internetverbinding – worden beheerd, een goede zaak in het kader van de risico's van aanvallen op de cyberveiligheid? Dat schijnt niet echt een garantie te zijn. Hoe wordt het beleid inzake cyberveiligheid vandaag overigens toegepast? Hoe staat het met de plannen ter zake?

De heer David Geerts (sp.a) vraagt zich ook af in welke mate de uit het onderzoek getrokken conclusies garanderen dat die documenten niet bestaan. Bestaat er een procedure die het mogelijk maakt om snel en gepast te reageren indien zou blijken dat documenten de ronde doen? Hoe verloopt, tot slot, concreet de samenwerking tussen de verschillende partners in termen van cyberveiligheid?

De heer Jean-Marc Nollet (Ecolo-Groen) herinnert eraan dat het CCB in april 2016 aanstipte dat België nul op vier scoorde inzake nucleaire cyberveiligheid en dat absoluut actie moest worden ondernomen.

Zijn de zaken voldoende geëvolueerd? België heeft een grote achterstand opgelopen in deze materie en er is haast bij.

Het FANC telde in april 2016 één enkele deskundige inzake cyberveiligheid. Het CCB lijkt voorts niet te beschikken over de interne bekwaamheden om de controle uit te voeren. Waarom moet deze opdracht aan een privébedrijf worden uitbesteed? Veiligheid moet in handen van de Staat blijven. Die privatisering is problematisch. Wat zijn de vooruitzichten?

In het kader van de zoektocht naar de gevoelige documenten had de minister van Buitenlandse Zaken

d'attaque terroriste sur les centrales nucléaires et une possibilité de prendre le contrôle de centrales nucléaires via Internet. Quel est l'avis du CCB sur cette question?

M. Michel de Lamotte (cdH) se demande pourquoi le CCB a eu besoin de l'aide du secteur privé. Est-il trop limité en capacité et moyens? Qu'en est-il de la compétence générale des collaborateurs? Par ailleurs, est-il possible que des pistes n'aient pas été sollicitées pour pouvoir aller plus loin dans la recherche? Y a-t-il eu un contrôle de la qualité de ces recherches?

M. Egbert Lachaert (Open Vld) demande si le CCB peut avoir la certitude qu'il n'y avait pas de documents sensibles pour les centrales sur le "*dark web*". Ou bien le fait de n'avoir rien trouvé ne veut-il rien dire sur les conclusions à tirer?

Par ailleurs, le fait que nos centrales datent des années 70 et sont donc gérées par analogie – donc sans lien avec Internet – est-il une bonne chose dans le cadre des risques d'attaques pour la cybersécurité? Cela ne semble pas être vraiment une garantie. En outre, comment les politiques en matière de cybersécurité sont-elles mises en œuvre à l'heure actuelle? Qu'en est-il des plans en la matière?

M. David Geerts (sp.a) se demande lui aussi dans quelle mesure les conclusions tirées apportent la garantie que ces documents n'existent pas. Par ailleurs, en cas d'indications de documents circulants, existe-t-il une procédure permettant d'y répondre de manière rapide et adéquate? Enfin, comment se passe concrètement la collaboration entre les différents partenaires en termes de cybersécurité?

M. Jean-Marc Nollet (Ecolo-Groen) rappelle qu'en avril dernier, le CCB indiquait que la Belgique avait un score de zéro sur quatre en matière de cybersécurité nucléaire et qu'il était nécessaire d'agir absolument.

Les choses ont-elles suffisamment évolué? La Belgique a un grand retard en la matière et il y a urgence.

L'AFCN disposait en avril dernier d'un seul expert en cybersécurité. En outre, le CCB ne semble pas disposer des compétences internes pour pouvoir procéder au contrôle. Pourquoi faut-il déléguer cela à une firme privée? La sécurité doit rester dans les mains de l'État. Cette privatisation est problématique. Dans quelle perspective devrions-nous nous situer?

Sur la question de la recherche des documents sensibles, le ministre de l'Intérieur indiquait qu'un document

aangestipt dat er een document op het *dark net* was verschenen, dat het gelekt zou kunnen zijn en dat het FANC op basis van informatie van het CCB onderzocht waarover het zou kunnen gaan. Het verrast de spreker bijgevolg dat het CCB zegt dat er niets werd gevonden. Gaat het over informatie die met gesloten deuren moet worden besproken? Welke garantie hebben we dat deze documenten niet op het *dark net* staan? Het is belangrijk om de algemene context van deze vragen beter te kennen.

De heer David Clarinval (MR) verheugt zich over de oprichting in 2015 van het CCB, dat zijn nut bewijst. De spreker neemt er akte van dat de documenten niet op het "*dark net*" werden gevonden, in tegenstelling tot wat in de pers is geschreven. Aangaande het internationaal aspect wenst de spreker te weten hoe het CCB met de andere Europese of internationale agentschappen samenwerkt.

De heer Bert Wollants (N-VA) wenst te weten of men misschien documenten met beperkte veiligheidsrisico's heeft gevonden, nu het CCB heeft gezegd dat er geen sprake is van documenten met "ernstige" veiligheidsrisico's". Heeft het CCB voorts contact gehad met de "*hacker*" die het bestaan van die documenten aan de pers heeft meegedeeld?

C. **Antwoorden en gedachtewisseling**

De heer Miguel de Bruycker geeft aan dat het CCB is opgericht om een antwoord te bieden op gewettigde bezorgdheid inzake cyberveiligheid. Het CCB functioneert goed, hoewel het maar over een beperkte capaciteit beschikt. Volgend jaar stijgt het aantal medewerkers tot 34, wat een eerste verbetering is.

Het OCAD heeft een analyse uitgevoerd over het risico van cyberterrorisme na de aanslagen in Brussel. Als reactie op die analyse werden, in coördinatie met de verschillende betrokken diensten, maatregelen genomen. Er is met de beschikbare middelen dus een *follow-up* van die dreiging met betrekking tot kritieke infrastructuur. Er is dreiging van cybercrime, activisten en cyberterrorisme. Het komt er allemaal op aan die dreiging correct in te schatten, om er de geschikte beschermingsmiddelen voor in te zetten. Dat is de rol van het CCB.

Aangaande de inschakeling van privéondernemingen voor de opsporingen op het internet herinnert de spreker er allereerst aan dat het internet niet Belgisch is, maar mondiaal. De spreker geeft opnieuw aan dat het om een goede gelegenheid ging om de samenwerking

avait été aperçu sur le "*dark net*" et aurait pu faire l'objet d'une fuite et que l'AFCN était en train d'examiner de quoi il pouvait s'agir sur base d'informations du CCB. L'orateur fait donc part de sa surprise d'entendre le CCB dire que rien n'a été trouvé. S'agit-il d'informations nécessitant un huis-clos? Quelle est la garantie que ces documents ne sont pas sur le "*dark net*"? Il est important de connaitre mieux le contexte général de ces questions.

M. David Clarinval (MR) se réjouit de la création en 2015 de ce CCB qui prouve son utilité. L'orateur prend acte du fait que les documents n'ont pas été trouvés sur le "*dark net*", contrairement aux informations qu'avait notamment donné la presse. Sur l'aspect international, l'orateur voudrait savoir comment le CCB travaille avec les autres agences européennes ou mondiales.

M. Bert Wollants (N-VA) se demande si des documents contenant des risques de sécurité limités auraient pu être trouvés, sachant que le CCB a parlé de l'absence de documents contenant des risques de sécurité "sérieux"? Par ailleurs, le CCB a-t-il eu des contacts avec le "*hacker*" qui avait indiqué la présence de ces documents à la presse?

C. **Réponses et débat**

M. Miguel de Bruycker indique que le CCB a été mis en place afin de répondre à la préoccupation légitime en matière de cybersécurité. Le CCB fonctionne bien, tout en ayant une capacité limitée. L'an prochain, on passera à 34 personnes, ce qui est une première amélioration.

Une analyse de l'OCAM a été réalisée concernant le risque de cyberterrorisme suite aux attentats de Bruxelles. Des mesures ont été prises, en coordination avec les différents services concernés, en réponse à cette analyse. Il y a donc un suivi de cette menace vis-à-vis de l'infrastructure critique, avec les moyens disponibles. Il y a une menace, de cybercrimes, d'activistes, de cyberterrorisme. Le tout est d'arriver à estimer cette menace de manière correcte afin de mettre les moyens adaptés à cette menace pour se protéger. C'est le rôle du CCB.

Concernant l'utilisation de firmes privées pour la recherche sur Internet, M. de Bruycker rappelle tout d'abord qu'Internet n'est pas Belge mais est mondial. L'orateur indique à nouveau qu'il s'agissait d'une bonne opportunité pour évaluer la collaboration avec le secteur

met de privésector bij dit soort onderzoek op het internet te evalueren. Er moet nog een beslissing worden genomen over de eventuele toekomst van dergelijke samenwerkingsverbanden.

Dat de documenten ook door een privéonderneming werden opgespoord, betekent evenmin dat ze niet op het internet bestaan. Men moet in dat verband eerlijk zijn: er is geen zekerheid. De vaststelling is evenwel dat er niets werd gevonden, ook niet door de in dat soort onderzoek gespecialiseerde firma.

Het "*dark web*" is heel ingewikkeld en maakt het voor iedereen mogelijk informatie te delen met wie hij maar wil, zonder dat de autoriteiten daar enige vat op hebben.

Segmentering vormt een belangrijke wijze om een netwerk te beschermen. Dat wordt bijvoorbeeld gedaan als men het openbare net van het intranet van een onderneming scheidt. Materiële scheiding van een netwerk houdt in dat de informatie moet worden overgedragen via een "*information exchange gateway*". Sommige systemen zorgen er enerzijds voor dat het gevaar van besmetting van het beveiligde netwerk wordt geminimaliseerd en anderzijds dat lekken worden beperkt. Dat soort beveiliging is uiteraard heel duur en beperkt de vrijheid van de gebruiker. Het is dus volstrekt mogelijk om, naargelang van bepaalde risico's, voldoende beveiligde systemen te bouwen, meer bepaald wat de kerncentrales betreft.

Als gevolg van de slechte score die België in het voorjaar op cyberveiligheidsgebied heeft behaald, zijn het CCB en het FANC onmiddellijk bijeen gekomen om na te gaan welke maatregelen moesten worden genomen om het probleem op te lossen. Voor de spreker kwijten de exploitanten van de kritieke infrastructuur zich op een heel ernstige wijze van hun taak. Het gaat dus de goede richting uit.

Op het gebied van controles, is het niet de taak van de medewerkers van het CCB alle infrastructuur door te lichten, aangezien dat niet het gekozen model is. De samenwerking geschiedt met de sectoren. De installaties mogen al dan niet worden gecertificeerd door *auditors* in het licht van de geldende normen die door een overheidsinstantie zijn erkend. Dat is het te volgen model en de norm is internationaal.

De "*ethical hacker*" heeft documenten aan het licht gebracht die niet van dien aard waren dat ze een ernstige bedreiging vormden. Die documenten werden aan het FANC overhandigd zodat het zijn eigen risico-evaluatie kon uitvoeren. Het CCB kan zelf niet het

privé pour ce genre de recherche sur Internet. Il faut encore décider du futur éventuel de telles collaborations.

Le fait que les documents aient été recherchés par une firme privée également ne signifie pas non plus qu'ils n'existent pas sur Internet. Il faut être honnête à cet égard, il n'y a pas de certitude. La constatation est cependant que rien n'a été trouvé, y compris par cette firme spécialisée dans ce type de recherche.

Le "*dark web*" est très complexe et permet à n'importe qui de partager de l'information avec qui il veut, sans que les autorités n'aient de moyen de le contrôler.

Le fait de segmenter est une manière très importante de protéger un réseau. C'est ce qui se fait par exemple en segmentant réseau public et réseau interne d'une entreprise. La séparation physique d'un réseau signifie que l'information doit être transférée via un "*Information exchange gateway*". Certains systèmes permettent d'une part de minimaliser le risque d'infection sur le réseau protégé et d'autre part de limiter les fuites. Un tel type de sécurisation est évidemment très couteux et limite la liberté de l'utilisateur. Il est donc tout à fait possible de construire des systèmes suffisamment sécurisés en fonction de certains risques, notamment pour ce qui concerne les centrales nucléaires.

Suite aux mauvais résultats de la Belgique en matière de cybersécurité au printemps dernier, le CCB et l'AFCN se sont immédiatement réunis afin d'évaluer quelles actions devraient être prises afin de résoudre le problème. Pour l'orateur, les opérateurs des infrastructures critiques prennent leur mission très au sérieux. Le travail va donc dans la bonne direction.

En matière de contrôles, ce ne sont pas les collaborateurs du CCB qui vont aller auditer toutes les infrastructures, car ce n'est pas le modèle choisi. La collaboration se fait avec les secteurs. Ce sont les auditeurs agréés par une instance publique par rapport aux normes posées, qui peuvent certifier les installations ou pas. C'est ce modèle qui doit être suivi et la norme doit être internationale.

Le "*ethical hacker*" a communiqué des documents qui n'étaient pas de nature à constituer une menace sérieuse. Ces documents ont été remis à l'AFCN pour qu'elle fasse sa propre évaluation du risque. Le CCB ne peut évaluer lui-même le caractère dangereux de ces

gevaarlijke karakter van die informatie voor alle sectoren evalueren; daarom verwijst het naar de autoriteiten uit de betrokken sector.

De privéonderneming dacht het document onmiddelijk te vinden, wat niet het geval was. Dat onderzoek heeft echter uitgewezen dat er aanwijzingen waren dat een jaar voordien op de server van een buitenlandse onderneming documenten beschikbaar zijn geweest. Het CCB heeft een overzicht ontvangen van documenten die potentieel beschikbaar zijn, maar de privéonderneming beschikt niet over de documenten in kwestie en weet niet of iemand die ooit van die server heeft kunnen plukken. Het CCB heeft die informatie gevalideerd en ze aan het FANC meegedeeld. Het ging echter om onvoldoende concrete informatie om verder in aanmerking te worden genomen.

De spreker benadrukt dat cyberveiligheid een internationaal vraagstuk is. De normen moeten dus eveneens internationaal zijn. De heer de Bruycker maakt zelf deel uit van het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA). In 2017 zal dat agentschap de lijst opstellen van de minimumveiligheidsmaatregelen voor de kritieke infrastructuur in Europa. Er rest nog veel werk.

Een veiligheidsrisico moet kunnen worden gekwantificeerd en geïdentificeerd. Het CCB staat open voor eenieder die informatie wil delen en is politiek neutraal.

De heer Eric Thiébaut (PS) is niet gerustgesteld door de verstrekte antwoorden. Hij ziet twee gevaren: enerzijds zouden vertrouwelijke documenten inzake nucleaire veiligheid kunnen worden gekaapt en gebruikt voor bijvoorbeeld terroristische doeleinden; anderzijds wordt het proces door informatica aangestuurd. Is dat proces extern toegankelijk? Dit is een heel eenvoudige vraag. De minister heeft onlangs aangegeven dat het om een analoog systeem gaat, dat dus niet met het internet is verbonden.

De heer Michel de Lamotte (cdH) heeft het gevoel dat er geen waterdichte methode bestaat om voor de kerncentrales een cyberveiligheidsproces te ontwikkelen. De indruk bestaat dat nattevingerwerk wordt geleverd. Bepaalde vragen blijven onbeantwoord. Er moet structureel vooruitgang worden geboekt, met de passende middelen. Dit is een belangrijk vraagstuk.

De heer Jean-Marc Nollet (Ecolo-Groen) geeft aan dat er stilaan duidelijkheid komt aangaande de werkzaamheden van het CCB en de grenzen waarbinnen het opereert. Het CCB levert goed werk om ons land te doen bijbenen. De dreiging van cyberterrorisme is reëel.

informations pour tous les secteurs, c'est pour ça qu'il se réfère aux autorités du secteur concerné.

L'entreprise privée pensait trouver le document directement, ce qui n'a pas été le cas. Cependant, ses recherches lui ont permis de constater qu'il y avait des indications que des documents avaient été disponibles un an auparavant sur le serveur d'un entrepreneur étranger. Le CCB a reçu un aperçu de documents potentiellement disponibles, mais l'entreprise privée ne dispose pas des documents en question et ne sait pas si quelqu'un a pu un jour les prendre de ce serveur. Le CCB a validé cette information et l'a communiquée à l'AFCN. Cependant, il s'agissait d'une information trop peu concrète pour la prendre en considération plus loin.

L'orateur insiste sur le fait que la cybersécurité est une problématique internationale. Les normes doivent donc aussi être internationales. M. de Bruycker fait lui-même partie de l'agence européenne de la cybersécurité (ENISA). Cette agence devra, en 2017, établir la liste des mesures de sécurité minimales pour l'infrastructure critique en Europe. Il y a encore beaucoup de travail à réaliser.

Un risque de sécurité doit pouvoir être quantifié et identifié. Le CCB est ouvert vis-à-vis de chacun qui souhaite partager de l'information et le centre est neutre politiquement.

M. Eric Thiébaut (PS) n'est pas rassuré par les réponses données. Il distingue d'une part le risque de voir des documents confidentiels en matière de sécurité nucléaire être dérobés et utilisés à des fins par exemple terroristes; et, d'autre part, le processus qui est piloté de manière informatique. Peut-on accéder à ce processus de l'extérieur? Il s'agit d'une question très simple. Le ministre a indiqué récemment que le système est analogue et donc sans connexion avec Internet.

M. Michel de Lamotte (cdH) a le sentiment qu'il n'y a pas une méthode solide pour construire un processus de cybersécurité pour les centrales nucléaires. On a l'impression d'avancer à tâtons. Certaines interrogations subsistent. Il faudrait avancer de manière structurée avec les moyens adéquats. C'est un sujet essentiel.

M. Jean-Marc Nollet (Ecolo-Groen) indique que le travail du CCB et ses limites commencent à se clarifier. Le CCB effectue un bon travail pour tenter de rattraper le retard de notre pays. La menace de cyberterrorisme existe. Il y a une faille structurelle dans la capacité des

Er bestaat een structureel manco in de capaciteit van de overheid op dat vlak. Er moeten waarborgen komen zodat dit manco zo snel mogelijk kan worden verholpen; onvermijdelijk gaat dat met een hogere beveiligingskostprijs gepaard.

Voorts wijst de spreker erop dat de aanwijzingen als zouden in het verleden documenten hebben gestaan op een server van een buitenlandse onderneming, vragen oproepen aangaande de onderaanneming, meer bepaald met betrekking tot buitenlandse onderaannemers, en de risico's daarvan op het vlak van de cyberveiligheid.

II. — **HOORZITTING MET DE HEREN JAN BENS (DIRECTEUR-GENERAAL) EN RONY DRESSELAERS (DIRECTEUR BEVEILIGING EN VERVOER), VERTEGENWOORDIGERS VAN HET FANC, EN DE DAMES ELS THOELEN (DIRECTEUR HEALTH & SAFETY / NUCLEAR SAFETY / SECURITY) EN GRIET HEYVAERT (CHIEF REGULATORY AUTHORITIES AND PUBLIC AFFAIRS OFFICER), VERTEGENWOORDIGSTERS VAN ENGIE ELECTRABEL**

A. **Uiteenzetting van de heren Jan Bens (directeur-generaal) en Rony Dresselaers (directeur beveiliging en vervoer), vertegenwoordigers van het FANC**

De heer Rony Dresselaers (FANC) verduidelijkt dat de presentatie uit de volgende delen bestaat:

1. Het nationaal kader

2. De erkenningsprocedure

3. Machtiging van natuurlijke en rechtspersonen

4. Inspectie Hoofdzetel Engie

5. Cyber security

Op 12 september 2001, de dag na 9-11, is de wereld wakker geworden in een totaal andere wereld. Niet enkel in de maatschappij is er evolutie op de wijze waarop naar beveiliging wordt gekeken, maar dit is eveneens van toepassing op de nucleaire sector. De nucleaire beveiliging was voor 2001 voornamelijk gefocust op non-proliferatie, zowel naar materialen als naar kennis. Na 2001 werd de internationale gemeenschap zich ervan bewust dat kwaadwillige handelingen, zoals sabotage tegen installaties of transporten een reëel risico konden zijn. Internationaal bindende instrumenten werden geamendeerd, zoals de CPPRM, de Conventie over de fysische beveiliging van nucleaire materialen. Het heeft ongeveer 10 jaar geduurd vooraleer deze conventie in

pouvoirs publics en la matière. Il faut des garanties pour combler au plus vite cette faille, qui n'est pas sans lien avec le coût élevé de la sécurisation.

Par ailleurs, l'orateur indique que les indications que des documents ont été disponibles par le passé sur le serveur d'un entrepreneur étranger pose la question de la sous-traitance en particulier à l'étranger et de ses risques pour la cybersécurité.

II. — **AUDITION DE MM. JAN BENS (DIRECTEUR GÉNÉRAL) ET RONY DRESSELAERS (DIRECTEUR SÉCURITÉ ET TRANSPORT), REPRÉSENTANTS DE L'AFCN, ET DE MMES ELS THOELEN (DIRECTOR HEALTH & SAFETY / NUCLEAR SAFETY / SECURITY) ET GRIET HEYVAERT (CHIEF REGULATORY AUTHORITIES AND PUBLIC AFFAIRS OFFICER), REPRÉSENTANTES D'ENGIE ELECTRABEL**

A. **Exposé de MM. Jan Bens (directeur général) et Rony Dresselaers (directeur sécurité et transport), représentants de l'AFCN**

M. Rony Dresselaers (AFCN) explique que la présentation comprend les parties suivantes:

1. Le cadre national

2. Procédure d'agrément

3. Habilitation des personnes morales et physiques

4. Inspection Engie – siège

5. Cyber security

Le 12 septembre 2001, au lendemain du 11 septembre, nous nous sommes réveillés dans un monde complètement différent. La manière de percevoir la sécurité a non seulement changé au niveau de la société, mais aussi dans le secteur nucléaire. Avant 2001, la sécurité nucléaire était essentiellement axée sur la non-prolifération, tant sur le plan des matières que des connaissances. Après 2001, la communauté internationale a pris conscience du fait que des actes malveillants, comme le sabotage d'installations ou de transports, pouvaient constituer un risque réel. Certains instruments contraignants au niveau international ont été modifiés, comme la CPPMN, la Convention sur la protection physique des matières nucléaires. Il a fallu près de 10 ans avant que

werking is getreden. Dit is mede te danken naar aanleiding van de *Nuclear Security Summit*.

Ook de nationale regelgevingen werden aangepast om deze nieuwe concepten op te nemen in de nationale regelgeving. In ons land is deze nieuwe regelgeving in 2011 in werking getreden.

Bij de wet van 30 maart 2011 "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 en tot wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen" werden:

— in de wet van 15 april 1994 nieuwe definities ingevoerd betreffende categorisering, beveiligingsniveau, nucleaire documenten en beveiligingszones; werd de categorisering van nucleair materiaal gedefinieerd, werd een beveiligingsniveau toegekend en werden er drie beveiligingsniveaus bepaald: Vertrouwelijk-NUC, Geheim-NUC en Zeer geheim-NUC;

— in de wet van 11 december 1998 het toepassingsgebied uitgebreid naar gecategoriseerde elementen (nucleair materiaal en documenten, veiligheidszones), bepaald dat een veiligheidsmachtiging moet worden afgeleverd aan personen die toegang hebben tot gecategoriseerd nucleair materiaal tot nucleaire documenten en tot beveiligingszones, nadere regels van aflevering van veiligheidsattesten en toegangsvergunningen en de introductie van bijkomende bescherming van technische, organisatorische of administratieve aard.

Het begrip "veiligheidszone" wordt als volgt bepaald: "Elke plaats van een installatie waar zich nucleaire materialen en /of nucleaire documenten bevinden of uitrustingen, systemen of voorzieningen of om het even welk ander element waarvan de sabotage een rechtstreekse of onrechtstreekse radiologische impact kan hebben die de internationaal erkende radiologische normen overschrijdt.

cette convention entre en vigueur, notamment grâce au Sommet Sécurité Nucléaire.

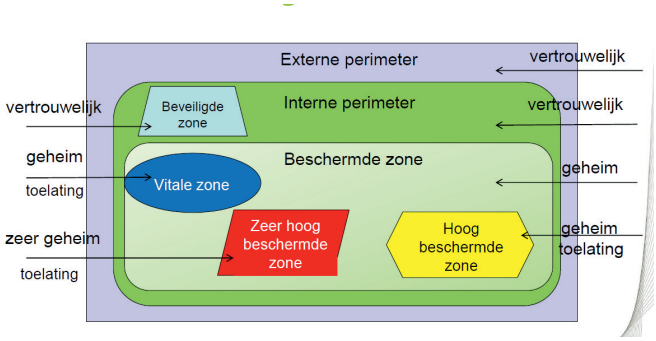
Les réglementations nationales ont également été adaptées de manière à intégrer ces nouveaux concepts. Dans notre pays, cette nouvelle réglementation est entrée en vigueur en 2011.

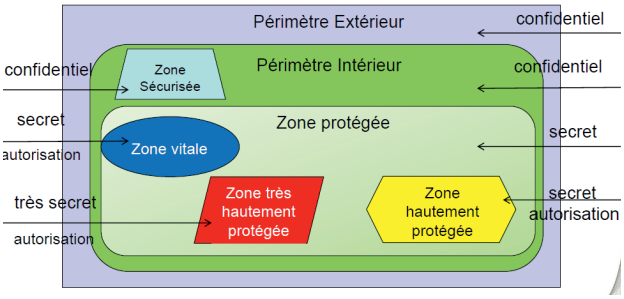
La loi du 30 mars 2011 modifiant la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire et modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité a apporté toute une série de modifications:

— dans la loi du 15 avril 1994, elle a introduit de nouvelles définitions relatives à la catégorisation, à l'échelon de sécurité, au document nucléaire et à la zone de sécurité; a défini la catégorisation du matériel nucléaire, a attribué un échelon de sécurité et a fixé trois échelons de sécurité: "CONFIDENTIEL – NUC"; "SECRET – NUC"; "TRÈS SECRET – NUC";

— dans la loi du 11 décembre 1998, elle a élargi le champ d'application aux éléments catégorisés (matières et documents nucléaires, zones de sécurité), a prévu qu'une habilitation de sécurité doit être délivrée aux personnes ayant accès à des matières nucléaires catégorisées, à des documents nucléaires et à des zones de sécurité, a fixé les modalités relatives à la délivrance d'attestations de sécurité et d'autorisations d'accès et a introduit des mesures de protection complémentaires de nature technique, organisationnelle ou administrative.

La notion de "zone de sécurité" est définie comme suit: tout endroit d'une installation où se trouvent des matières nucléaires ou des documents nucléaires; ou des équipements, des systèmes, des dispositifs ou tout autre élément dont le sabotage pourrait conduire directement ou indirectement à des conséquences radiologiques dépassant les normes radiologiques internationalement reconnues.





Het begrip “nucleair document” wordt als volgt gedefinieerd: Elke vorm van geregistreerde informatie met betrekking op nucleair materiaal, op uitrustingen en vitale zones of op de fysieke beveiligingsmaatregelen.

Deze nieuwe concepten werden vervolgens uitgewerkt en beschreven en geïmplementeerd binnen de bestaande installaties. De wetgever heeft hiervoor aan het FANC de opdracht gegeven een specifieke erkenningprocedure toe te passen voorzien in het koninklijk besluit van 17 oktober 2011 betreffende de “Fysieke beveiliging”. De beveiliging van de nucleaire documenten maakt hiervan ook deel uit. Deze erkenningprocedure is momenteel lopende voor alle nucleaire exploitanten en de transporten van nucleair materiaal. Deze procedure geldt echter niet voor onderaannemers of toeleveranciers, die werkzaamheden uitvoeren op de site: het KB is immers niet van toepassing buiten de nucleaire sector voor natuurlijke personen en personen van publiek of privaat recht.

De erkenningprocedure verloopt als volgt : na het in werkingtreden van de reglementering op 1 mei 2012 hadden de nucleaire exploitanten en transporteurs 6 maanden de tijd om hun erkenningdossier in te dienen bij het agentschap. Het FANC heeft vervolgens op 1 mei 2013 advies uitgebracht. Vanaf de ontvangst van dit advies, hadden de exploitanten en transporteurs 36 maanden de tijd om alle door het FANC voorgestelde veiligheidsmaatregelen tegen 1 mei 2016 door te voeren. Vervolgens heeft het FANC opnieuw het ingerichte fysieke beveiligingssysteem geëvalueerd en tegen 1 november 2016 een uitspraak gedaan. Dit is ondertussen gekend. In een gemotiveerd schrijven heeft het FANC uiteengezet waarom het beveiligingssysteem niet werd erkend. De exploitant heeft opnieuw drie maanden de tijd om antwoorden te formuleren en aanpassingen door te voeren. Tegen 1 mei 2017 zal het FANC opnieuw een beslissing moeten nemen. Indien het FANC het beveiligingssysteem niet erkent, zal het FANC bijkomende maatregelen opleggen, inclusief de handhaving, en zal het FANC de uitvoeringstermijnen bepalen. De nadruk wordt hierbij voornamelijk gelegd

La notion de “document nucléaire” se définit comme suit: toutes les sortes d’informations enregistrées relatives aux matières nucléaires, aux équipements en zone vitale ou aux mesures de protection physique.

Ces nouveaux concepts ont ensuite été développés, décrits et mis en œuvre dans les installations existantes. Pour ce faire, le législateur a chargé l’AFCN d’appliquer une méthode d’agrément spécifique prévue dans l’arrêté royal du 17 octobre 2011 sur la “protection physique”, qui couvre également la protection des documents nucléaires. Cette procédure d’agrément est en cours pour tous les exploitants nucléaires et pour les transports de matières nucléaires. Cette procédure ne vaut toutefois pas pour les sous-traitants ou les fournisseurs qui sont actifs sur le site: l’arrêté royal ne s’applique en effet pas aux personnes physiques ni aux personnes de droit public ou privé qui ne font pas partie du secteur nucléaire.

La procédure d’agrément se déroule de la manière suivante: après l’entrée en vigueur de la réglementation, le 1er mai 2012, les exploitants et transporteurs nucléaires ont eu six mois pour introduire leur demande d’agrément auprès de l’agence, et l’AFCN a rendu son avis le 1er mai 2013. À partir de la réception de cet avis, les exploitants et transporteurs ont eu 36 mois, soit jusqu’au 1er mai 2016, pour mettre en œuvre toutes les mesures de sécurité proposées par l’AFCN. Ensuite, l’AFCN a une nouvelle fois évalué le système de protection physique mis en place et a rendu son verdict le 1er novembre 2016. Entre-temps, les conclusions de l’évaluation sont connues. Dans une lettre motivée, l’AFCN a expliqué pourquoi le système de protection n’a pas été agréé. L’exploitant dispose d’un délai supplémentaire de trois mois pour formuler des réponses et procéder à des ajustements. L’AFCN devra à nouveau prendre une décision d’ici le 1er mai 2017. Si l’AFCN n’accorde pas son agrément au système de protection, elle imposera des mesures complémentaires, y compris en ce qui concerne contrôle de leur mise en œuvre, et elle fixera les délais d’exécution. L’accent sera mis

op *compliance* en erkenning komt dan op de tweede plaats. Tijdens de afgelopen periode werden er dossiers uitgewisseld en werden de erkenningdossiers geanalyseerd. Er werden dossier- en technische vergaderingen gehouden en plaatsbezoeken georganiseerd. Na controles wordt er, indien nodig, geheroriënteerd. Het is zeer belangrijk om een goed te beeld te krijgen tussen wat is beschreven in het dossier en hoe dit op het terrein wordt geïmplementeerd.

Het FANC heeft niet enkel de fysieke beveiliging van de nucleaire installaties en het transport bekeken, maar ook of de beveiligingsmaatregelen konden worden versterkt voor al diegenen die, om professionele redenen, toegang moesten hebben tot de Belgische sites. We denken hierbij aan onderaannemers die toegang moeten hebben tot de site en die soms in het bezit kunnen zijn van nucleaire documenten.

Situatieschets vóór 2011: de nucleaire exploitant vraagt veiligheidsattesten aan het FANC en machtigingen aan de NVO (Nationale VeiligheidsOverheid) voor het eigen personeel en het personeel van de onderaannemers, of ze nu resident of niet-resident in België waren. Het aantal machtigingen was beperkt, zowel van de natuurlijke personen als van de rechtspersonen.

Situatieschets na 2011: in het nieuwe systeem wordt de machtiging van natuurlijke personen en rechtspersonen standaard. Elke nucleaire exploitant heeft als natuurlijke en als rechtspersoon een machtiging moeten vragen. Voor alle onderaannemers geldt een identieke procedure.

Vanaf 2012 werd een volledige nieuwe regularisatieprocedure opgestart in samenwerking met de NVO. In bepaalde gevallen worden er nog veiligheidsattesten en toegangsvergunningen afgeleverd maar door de nieuwe regelgeving zijn de mogelijkheden hiervoor sterk beperkt. Voor de machtiging van rechtspersonen, geschiedt het onderzoek door de NVO, zowel voor de natuurlijke en de rechtspersonen en er wordt ook gekeken naar de installatie van de geclassificeerde en – sinds de wet van 2011 – gecategoriseerde documenten, die ook de nucleaire documenten worden genoemd. Het FANC heeft van de NVO de opdracht gekregen na te gaan hoe deze documenten specifiek worden aangemaakt, beheerd, bewaard en vernietigd in het kader van de procedure “machtiging rechtspersoon”. Het FANC heeft een specifieke reglementering uitgewerkt voor de nucleaire documenten in het KB “Nucleaire documenten”. Het basisprincipe dat wordt gehanteerd, is dat de primaire verantwoordelijkheid bij de nucleaire exploitant wordt gelegd. Het is de exploitant die beslist met wie de documenten moeten worden gedeeld.

principalement sur l’aspect de conformité (*compliance*), l’agrément venant en deuxième place. Au cours de la période écoulée, des dossiers ont été échangés et les dossiers d’agrément ont été analysés. Des délibérations sur les dossiers et des réunions techniques ont été organisées, de même que des visites *in situ*. Après plusieurs contrôles, des ajustements seront proposés si nécessaire. Il est très important d’avoir une vision claire de ce qui est décrit dans le dossier et de la façon dont ce contenu est mis en œuvre sur le terrain.

L’AFCN a vérifié la sécurisation physique des installations nucléaires et du transport, mais elle a aussi examiné si les mesures de sécurisation pouvaient être renforcées pour tous ceux qui, pour des raisons professionnelles, doivent avoir accès aux sites belges. Nous pensons à cet égard aux sous-traitants qui doivent avoir accès au site et qui peuvent parfois être en possession de documents nucléaires.

Situation avant 2011: l’exploitant nucléaire demande des attestations de sécurité à l’AFCN et des habilitations à l’Autorité nationale de sécurité (ANS) pour le personnel propre de l’entreprise et le personnel des sous-traitants, que ces derniers résident ou non en Belgique. Le nombre d’habilitations, tant des personnes physiques que morales, était limité.

Situation après 2011: l’habilitation des personnes physiques et morales devient standard dans le nouveau système. Chaque exploitant nucléaire a dû demander une habilitation en tant que personne physique et en tant que personne morale. Une procédure identique s’applique à tous les sous-traitants.

À partir de 2012, une procédure de régularisation entièrement nouvelle a été lancée en collaboration avec l’ANS. Dans certains cas, des attestations de sécurité et des autorisations d’accès sont encore délivrées mais la nouvelle réglementation en limite fortement les possibilités. C’est l’ANS qui réalise l’enquête en vue de l’habilitation des personnes morales, tant pour les personnes physiques que morales, et l’installation des documents classifiés et, depuis la loi de 2011, catégorisés, aussi appelés documents nucléaires, est également examinée. L’ANS a confié à l’AFCN la mission de contrôler comment ces documents sont spécifiquement produits, gérés, conservés et détruits dans le cadre de la procédure “habilitation des personnes morales”. L’AFCN a élaboré une réglementation spécifique pour les documents nucléaires dans l’arrêté royal portant sur la catégorisation et la protection des documents nucléaires. Le principe de base qui est appliqué est que la responsabilité primaire incombe à l’exploitant. Ce dernier décide avec qui les documents doivent être partagés.

De heer Dresselaers vat als volgt samen: nucleaire documenten en fysieke beveiliging maken onderdeel uit van de erkenningdossiers voor de nucleaire exploitanten en transporteurs. Voor alle onderaannemers zijn alle relevante maatregelen op het vlak van betrouwbaarheid en de nucleaire documenten opgenomen in de K.B.'s en de aanbevelingen van het FANC en wordt er een controle uitgeoefend op het niveau van de rechtspersoon. Maar de eerstelijnsverantwoordelijkheid blijft bij de nucleaire exploitant die beslist wat mogelijk is binnen het kader van de geldende regels.

Binnen het geschetste wettelijke kader heeft het FANC een inspectie doorgevoerd van de hoofdzetel van Engie Electrabel, waarvan documenten in de pers werden gelekt.

Tijdens de inspectie deed het FANC een onderzoek naar de volgende punten:

— is er een efficiënt en goed gedocumenteerd systeem voor het beheer van nucleaire documenten: het FANC heeft verbeteringen voorgesteld, een analyse doorgevoerd van de technische documentatie en een controle doorgevoerd over de samenhang van de procedures;

— het FANC heeft ook een onderzoek gevoerd naar de aanwezigheid van een minimale infrastructuur, dit samen met medewerkers van het ADIV, de militaire inlichtingen- en veiligheidsdienst; er werden voorstellen tot verbetering opgesteld;

— voor het FANC is de aanwezigheid van een beveiligingscultuur zeer belangrijk: op de hoofdzetel van Engie Electrabel is er ter zake een programma lopende en er zullen ook nog een aantal aandachtspunten moeten worden ontwikkeld naar de toekomst toe;

— na de meldingen dat er nucleaire documenten zouden zijn teruggevonden op het *Dark-net*, heeft het FANC onmiddellijk een onderzoek opgestart, in samenwerking met de personeelsleden van het Centrum Cyberveiligheid België (hierna: CCB). Dit onderzoek heeft niet geleid tot het terugvinden van nucleaire documenten op het *Dark-net*. Voor dit punt verwijst de spreker naar de uiteenzetting van de heer Miguel de Bruycker, hoofd van het CCB.

Cyber security is de laatste jaren zeer belangrijk geworden: de recentste dreigingen vinden er immers hun oorsprong en vormen een zeer dynamische dreiging die zeer snel evolueert. De risico's voor de nucleaire sector zijn:

M. Dresselaers résume les choses comme suit: les documents nucléaires et la protection physique font partie des dossiers d'agrément destinés aux exploitants et aux transporteurs nucléaires. Les arrêtés royaux et les recommandations de l'AFCN comprennent toutes les mesures pertinentes en matière de fiabilité et les documents nucléaires nécessaires à tous les sous-traitants. Un contrôle est également exercé au niveau de la personne morale. La responsabilité de première ligne continue toutefois à être assumée par l'exploitant nucléaire, qui décide de ce qui est possible dans le cadre des règles en vigueur.

Dans le respect du cadre légal esquissé, l'AFCN a procédé à une inspection du siège principal d'Engie Electrabel, dont des documents ont fuité dans la presse.

Lors de cette inspection, l'AFCN s'est concentrée sur les points suivants:

— existe-t-il un système efficace et bien documenté pour la gestion des documents nucléaires? L'AFCN a formulé des propositions d'amélioration et a procédé à une analyse de la documentation technique ainsi qu'à un contrôle de la cohérence des procédures;

— l'AFCN a également investigué la présence d'une infrastructure minimale, en collaboration avec des collaborateurs du SGRS et du service militaire de renseignement et de sécurité; des propositions d'amélioration ont été formulées;

— la présence d'une culture de sécurité revêt une importance primordiale pour l'AFCN: au sein du siège principal d'Engie Electrabel, un programme en la matière est en cours et il conviendra également de s'atteler à plusieurs points importants à l'avenir;

— après l'annonce que des documents nucléaires auraient été retrouvés sur le *Dark-net*, l'AFCN a immédiatement ouvert une enquête, en collaboration avec le personnel du Centre Cybersécurité Belgique (ci-après CCB). Aucun document nucléaire n'a été retrouvé sur le *Dark-net* lors de cette enquête. Concernant ce point, l'orateur renvoie à l'exposé de M. Miguel de Bruycker, directeur du CCB.

La cybersécurité a acquis une grande importance ces dernières années: les menaces les plus récentes, qui sont très dynamiques et évoluent très rapidement, y sont en effet liées. Les risques pour le secteur nucléaire sont les suivants:

— kwaadwillige handelingen die schade kunnen berokkenen aan kernmateriaal en nucleaire installaties (met mogelijk menselijke slachtoffers en/of gevolgen voor het milieu);

— diefstal van kernmateriaal;

— diefstal van nucleaire *know how*.

Het FANC zal in deze nieuwe partnerschappen afsluiten met het CCB om de huidige concepten van fysieke beveiliging op termijn te verbeteren. De installaties zullen in deze hun beveiligingsniveau zeker moeten opkrikken. Middelen en kennis zullen moeten worden gebundeld. Het is belangrijk om in dit verband samen te werken met nationale en internationale organisaties.

De risico's van een cyberaanval zijn algemeen gekend: mogelijkheid van *black out*, het niet beschikbaar zijn van een aantal installaties, het verlies van informatie en *know how.* Specifiek voor de nucleaire sector is daarenboven dat een mogelijke sabotage aanleiding zou kunnen geven tot radiologische risico's. Diefstal van nucleaire materialen die, misschien niet in België, maar wel daarbuiten, zouden kunnen worden gebruikt om een aanslag te plegen. Ook diefstal van kennis, *know how* en technieken die in de nucleaire sector worden toegepast.

De aanpak van het FANC en de toekomstige ontwikkelingen zijn als volgt:

— ontwikkeling van competenties, zowel in de schoot van het FANC als Bel V;

— in 2011 hebben stresstests plaatsgevonden: België heeft in deze ook aandacht gehad voor *man made events*: er is met andere woorden nagegaan wat de gevolgen van een cyberaanval kunnen zijn op systemen die de nucleaire veiligheid betreffen binnen een nucleaire installatie; de eerste analyses zijn gemaakt en er worden verdere acties genomen en opgevolgd;

— in hetzelfde jaar werd het koninklijk besluit van 17 oktober 2011 houdende de categorisering en de bescherming van nucleaire documenten uitgevaardigd: de richtlijnen zijn duidelijk: de nucleaire installatie/vervoerder moet de nucleaire documenten beschermen, deze die digitaal worden bewaard mee inbegrepen;

— het uitwerken van een nieuw aangepast kader betreffende *cyber security,* in nauw overleg met het CCB, het bevoegd orgaan voor de ontwikkeling van een nationaal beleid ter zake;

— des actes malveillants pouvant porter atteinte aux matières et installations nucléaires (avec potentiellement des conséquences en vies humaines et/ou sur l'environnement);

— le vol de matières nucléaires;

— le vol de savoir-faire technique nucléaire.

L'AFCN conclura de nouveaux partenariats en la matière avec le CCB, en vue d'améliorer, à terme, les concepts actuels de protection physique. Dans ce domaine, les installations devront certainement relever leur niveau de protection. Il conviendra de regrouper les moyens et les connaissances. La collaboration avec des organisations nationales et internationales est importante à cet égard.

Les risques d'une cyberattaque sont bien connus: la possibilité d'un *black out*, l'indisponibilité d'un certain nombre d'installations, la perte d'informations et de savoir-faire. Une spécificité du secteur nucléaire est en outre qu'un éventuel sabotage pourrait entraîner des risques sur le plan radiologique. Des matières nucléaires pourraient être volées en vue de perpétrer un attentat, peut-être pas en Belgique, mais bien à l'étranger. Le vol de connaissances, de savoir-faire et de techniques appliquées dans le secteur nucléaire est également possible.

L'approche de l'AFCN et les développements futurs portent sur les points suivants:

— le développement des compétences, tant au sein de l'AFCN que de Bel V;

— des tests de résistance ont eu lieu en 2011: en la matière, la Belgique a également accordé de l'attention aux *man made events*: autrement dit, on a vérifié quelles sont les conséquences possibles d'une cyberattaque sur des systèmes de sécurité nucléaire au sein d'une installation nucléaire; les premières analyses ont été effectuées, et d'autres actions seront entreprises et feront l'objet d'un suivi;

— la même année, l'arrêté royal du 17 octobre 2011 portant sur la catégorisation et la protection des documents nucléaires a été promulgué: les directives sont claires: l'installation/le transporteur nucléaire doit protéger les documents nucléaires, y compris ceux conservés sous forme numérique;

— l'élaboration d'un nouveau cadre adapté en matière de cybersécurité, en concertation étroite avec le CCB, l'organe compétent pour l'élaboration d'une politique nationale dans la matière;

— het opvolgen op internationaal niveau van de ontwikkelingen in de schoot van het IAEA;

— het regelmatig informatie uitwisselen met andere bevoegde buitenlandse autoriteiten;

— het wijzigen van het koninklijk besluit van 17 oktober 2011 houdende de categorisering en de bescherming van nucleaire documenten met het oog op het inschrijven van bepalingen betreffende de *cyber security*;

— het instellen van een *Cyber Design Basis Threat (Cyber-DBT): op deze wijze worden mogelijke dreigingen nauwgezet beschreven*;

— het uitwerken van bijkomende FANC-richtlijnen;

— het voorbereiden van een inspectieregime.

B. **Uiteenzetting van de dames Els Thoelen (*Director Health & Safety / Nuclear Safety / Security*) en Griet Heyvaert (*Chief Regulatory Authorities and Public Affairs Officer*), vertegenwoordigsters van Engie Electrabel;**

Mevrouw Els Thoelen is verantwoordelijk voor de dienst Fysische controle van Electrabel. Deze dienst waakt op onafhankelijke wijze over de nucleaire veiligheid binnen de installaties. De subcommissie heeft de wens geuit om een zicht te krijgen op het intern beheer van de nucleaire documenten en te weten te komen op welke wijze Electrabel de risico's inzake *cyber security* ter harte neemt.

Nucleaire veiligheid is binnen Engie Electrabel een absolute prioriteit. De ter zake geldende normen worden dan ook strikt nageleefd. Het nucleaire veiligheidsbeleid bestaat uit drie pijlers: het ontwerp van de installaties, de werkwijzen en het gedrag.

De installaties van Engie Electrabel zijn robuust, dank zij de redundantie en de diversiteit. In dit verband wordt verwezen naar de investeringen die worden doorgevoerd in het kader van de levensduurverlenging van de kerncentrales en de investeringen na de stresstests in 2012.

De werkwijzen en processen worden continu vergeleken met de beste standaarden wereldwijd en er wordt dan ook permanent bijgestuurd.

— le suivi au niveau international des développements au sein de l'IAEA;

— l'échange régulier d'informations avec d'autres autorités compétentes étrangères;

— la modification de l'arrêté royal du 17 octobre 2011 portant sur la catégorisation et la protection des documents nucléaires en vue d'y inscrire des dispositions relatives à la cybersécurité;

— la création du *Cyber Design Basis Threat (Cyber-DBT)* permettant de décrire précisément les menaces possibles;

— l'élaboration de directives supplémentaires au sein de l'AFCN;

— la préparation d'un régime d'inspection.

B. **Exposé de Mmes Els Thoelen (*Director Health & Safety / Nuclear Safety / Security*) et Griet Heyvaert (*Chief Regulatory Authorities and Public Affairs Officer*), représentantes d'Engie Electrabel;**

Mme Els Thoelen est responsable du service de contrôle physique d'Electrabel. Ce service veille, en toute indépendance, à la sûreté nucléaire au sein des installations. La sous-commission souhaite se faire une idée de la gestion interne des documents nucléaires et être informée de la manière dont Electrabel prend à cœur les risques en matière de c*yber sécurité*.

Chez Engie Electrabel, la sûreté nucléaire est une priorité absolue. Les normes applicables en la matière sont donc rigoureusement respectées. La politique de sûreté nucléaire s'articule autour de trois piliers: la conception des installations, les méthodes de travail et le comportement.

Les installations d'Engie Electrabel sont robustes, grâce à la redondance et à la diversité. À cet égard, l'oratrice évoque les investissements qui sont consentis dans le cadre de la prolongation de la durée de vie des centrales nucléaires et ceux réalisés après les tests de résistance de 2012.

Les méthodes de travail et les processus sont continuellement comparés avec les meilleures normes au monde et ajustés en permanence.

De derde pijler betreft het gedrag van de medewerkers: Electrabel heeft ongeveer tweeduizend personeelsleden die werken op de sites van de kerncentrales en er zijn op deze sites ook nog honderden *contractors* aan het werk. Bij de indiensttreding krijgen alle personeelsleden een gespecialiseerde opleiding en er worden geregeld vervolmakingcursussen aangeboden. Dit maakt deel uit van de integrale veiligheidscultuur. De verantwoordelijkheidszin van de medewerkers wordt continu aangescherpt.

Voor de *World Association of Nuclear Operators* (WANO) zijn de kenmerken van een sterken veiligheidscultuur:

— persoonlijk verantwoordelijkheid

— vragende houding

— veiligheidscommunicatie

— leiderschap

— beslissingen nemen

— respectvolle werkomgeving

— continu leren

— probleemidentificatie en oplossingen

— omgeving waarin bekommeringen kunnen geuit worden

— aangepaste werkprocessen.

Deze tien principes worden continu herhaald in de contacten met de medewerkers en de contractanten die actief zijn op de site van de kerncentrales. Daarenboven wordt er ook heel wat *know how* uitgewisseld op internationaal niveau en tussen de sites en de nucleaire exploitanten onderling. Er wordt met andere woorden ervaring uitgewisseld om de nucleaire veiligheid te versterken. WANO *peerreviews* maken hiervan deel uit.

Electrabel beschikt over een globaal S*ecurity Plan* 2015-2020. Nucleaire veiligheid maakt immers integraal deel uit van de nucleaire veiligheidscultuur. De zes principes van het Globaal Security Plan 2015-2020 zijn:

— identificeren en analyseren van vijandige, kwaadwillige en criminele bedreigingen gericht tegen de onderneming: er wordt op een proactieve wijze aan risicoanalyse gedaan;

Le troisième pilier concerne le comportement des collaborateurs: Electrabel occupe environ deux mille membres du personnel sur les sites des centrales nucléaires auxquels s'ajoutent encore des centaines de contractants. À leur entrée en fonction, tous les membres du personnel reçoivent une formation spécialisée et des cours de perfectionnement leur sont régulièrement proposés. Ces éléments font partie intégrante de la culture de sûreté nucléaire. Le sens des responsabilités des collaborateurs est affiné en permanence.

Selon l'association mondiale des exploitants nucléaires (WANO), une culture de sûreté solide présente les caractéristiques suivantes:

— responsabilité personnelle

— attitude interrogative

— communication sur la sûreté

— responsabilisation du leadership

— prise de décision

— environnement de travail respectueux

— apprentissage continu

— identification et résolution des problèmes

— environnement permettant de remonter ses préoccupations

— processus d'intervention.

Ces dix principes sont répétés en permanence lors des contacts avec les collaborateurs et les contractants qui travaillent sur le site des centrales nucléaires. On observe en outre un important échange de savoir-faire au niveau international et entre les sites et les exploitants nucléaires. Autrement dit, les expériences sont échangées dans le but de renforcer la sûreté nucléaire. Les *peer reviews* de WANO en font partie.

Electrabel s'est dotée d'un Plan *Global Security* 2015-2020. La sécurité nucléaire fait en effet partie intégrante de la culture de sûreté nucléaire. Les six principes du Plan *Global Security* 2015-2020 sont les suivants:

— Identification et analyse des menaces hostiles, malveillantes et criminelles à l'encontre de l'entreprise: analyse proactive des risques;

— streven naar uitmuntendheid en het voortdurend verbeteren van de maturiteit op het vlak van beveiliging: de regelgeving wordt strikt opgevolgd en omgezet in interne richtlijnen, die ook steeds worden afgetoetst met de internationaal geldende *best practises*;

— ondersteunen van onze beveiligingsstrategie door een efficiënte organisatie en toepassing van efficiënte beveiligingstechnieken: zo zijn er sinds 19 maart 2016 *Fast Respons Teams* aanwezig op de nucleaire sites. Deze teams, ter beschikking gesteld door de minister van Binnenlandse Zaken, wordt gefinancierd door Electrabel;

— investeren in de menselijke factor als sterkste schakel voor de preventie: verplicht dragen van de badge; *clean desk* principe, principe van *follow me printing,…*;

— uitwerken van inspanningen op het vlak van informatiebeveiliging, met de nadruk op *cyber* dreigingen;

— continu raadplegen van interne en externe partners: Electrabel maakt deel uit van verscheidene netwerken die actief zijn in de preventie tegen cyberbeveiliging en er wordt continu overlegd met de autoriteiten.

Essentieel in de nucleaire sector is het continu verbeteren van de werkwijzen: er wordt permanent toezicht uitgeoefend op de werkwijzen door het FANC, die over de nodige expertise beschikt. Als de nucleaire veiligheid in het geding is, bestaat er ook geen concurrentie. Er bestaat een vrijwillige, intensieve internationale *benchmarking* om de werkwijzen af te toetsen aan de beste praktijken en de hoogste standaarden door middel van internationale *audits*, zowel van het WANO als van het Internationaal Atoomagentschap. Om continue verbetering toe te laten, organiseert Electrabel daarenboven zelf op permanente wijze interne *audits* zowel vanuit Engie-Electrabel als vanuit de Groep Engie. Elke interne en externe audit wordt opgevolgd met een actieplan dat vervolgens een *follow up* kent. Binnen Electrabel bestaat er een departement dat de naam *Quality Assurance* draagt. Deze dienst heeft medewerkers, zowel op de sites (7) als op het niveau van de Hoofdzetel (5) en zij auditeren de werkprocessen. Deze medewerkers genoten hiervoor een specifieke opleiding en hebben ook elk een eigen specialiteit. Binnen de nucleaire centrales zijn 140 werkprocessen en deze worden over een periode van drie jaar telkens weer geauditeerd, waarna actieplannen voor continue verbetering worden opgesteld.

— recherche de l'excellence et amélioration continue du degré de maturité de l'entreprise en matière de sécurité: la réglementation est strictement respectée et traduite en consignes internes, qui sont par ailleurs constamment évaluées à la lumière des "meilleures pratiques" au niveau international;

— soutien de la politique de sécurité de l'entreprise par une organisation performante et par la mise en œuvre de techniques de sécurisation efficaces: des équipes d'intervention rapide sont présentes sur les sites nucléaires depuis le 19 mars 2016. Ces équipes, mises à disposition par le ministre de l'Intérieur, sont financées par Electrabel;

— investissement dans le facteur humain en tant que maillon le plus fort de la prévention: port obligatoire du badge, principe du *clean desk*, principe du *follow me printing*, etc.;

— intensification des efforts de l'entreprise en matière de protection de l'information, avec un accent sur les cyber-menaces;

— consultation permanentes des partenaires internes et externes: Electrabel fait partie de différents réseaux actifs dans le domaine de la prévention des cyberattaques et est constamment en concertation avec les autorités.

Dans le secteur nucléaire, l'amélioration continue est un élément essentiel: l'AFCN, qui dispose de l'expertise nécessaire, exerce un contrôle permanent sur les procédures d'Electrabel. Il est vrai qu'en matière de sûreté nucléaire, il n'y a pas de concurrence. Il existe au niveau international un *benchmarking* intensif qui permet, sur une base volontaire, d'évaluer les procédures à l'aune des meilleures pratiques et des standards les plus stricts par le biais d'audits internationaux, effectués tant par la WANO que par l'Agence internationale de l'énergie atomique. Afin de permettre une amélioration continue, Electrabel organise en outre elle-même des audits internes permanents réalisés tant par Engie-Electrabel que par le Groupe Engie. Chaque audit interne et externe est suivi d'un plan d'action qui fait lui-même l'objet d'un suivi. Il existe au sein d'Electrabel un département dénommé "*Quality Assurance*". Ce service compte des collaborateurs déployés tant sur les différents sites (7) qu'au niveau du siège central (5), et leur mission est d'analyser les processus de travail. Ces collaborateurs ont été spécifiquement formés à cet effet et ont en outre chacun leur propre spécialité. Il existe 140 processus différents dans les centrales nucléaires, et ces processus sont soumis à un nouvel audit tous les trois ans. Ces audits servent ensuite à élaborer des plans d'action d'amélioration continue.

Het intern werkdocument van Electrabel, dat in de pers is verschenen, en dat mede aanleiding is van de heden georganiseerde hoorzitting, betreft een intern auditdocument dat nagaat wat de prestatie van Electrabel is op het niveau van document management van de geclassificeerde of gecategoriseerde documenten, met name de wettelijk beschermde documenten.

Voor wat het document management in het algemeen betreft, zijn de werkprocessen met betrekking tot de nucleaire veiligheid zeer belangrijk. Alles wordt zo goed mogelijk beheerd en opgeslagen en er moet voor worden gezorgd dat de medewerkers te allen tijde op een betrouwbare wijze toegang hebben tot de vereiste documenten. Elk kwaliteitsdocument doorloopt verschillende fases: opmaken, controleren, goedkeuren, valideren, verdelen en eventueel beschikt het document over een einddatum in geldigheid. Voor de nucleaire centrales zijn er op vandaag 1,7 miljoen documenten gearchiveerd in SAP. Jaarlijks worden er 55 000 documenten toegevoegd en 32 000 versieverhogingen voorzien. De toegang tot deze documenten zijn geregistreerd per doelgroep en meer dan 300 personen werken dagelijks voor het Document Management. Al deze medewerkers beschikken over een veiligheidsmachtiging. De wettelijk gereglementeerde documenten in de categorie “Vertrouwelijk en Geheim” worden niet bewaard op SAP servers.

Naargelang van het classificatieniveau zijn er verschillende archiveringsmethodes:

— het beleid van de Groep Engie in verband met de bescherming van het Patrimonium voor wat interne documenten betreft, is als volgt:

+ alle documenten worden verondersteld intern te zijn;

+ interne documenten mogen enkel publiek gemaakt worden na goedkeuring van de hiërarchie;

+ er zijn interne documenten met beperkte verspreiding: daarvoor geldt het niveau “Beperkt” en zij hebben een oranje label; het is een document met dergelijk label dat in de pers is terecht gekomen en mee aanleiding is voor de hoorzitting in de subcommissie;

+ er zijn interne documenten met confidentieel karakter: daarvoor geldt het niveau “Geheim” en zij hebben een rood label;

— specifiek voor de wettelijk gereglementeerde documenten: hierbij wordt een onderscheid gemaakt tussen de toepasselijke wetgeving:

Le document de travail interne d’Electrabel qui a été publié dans la presse, et qui est en partie à l’origine de la présente audition, provient d’un audit interne dont le but était de vérifier les performances d’Electrabel au niveau de la gestion des documents classifiés ou catégorisés, et notamment les documents légalement protégés.

Pour ce qui est de la gestion des documents en général, les processus de travail relatifs à la sûreté nucléaire sont très importants. Tout est géré et archivé le mieux possible et il faut veiller à ce que les collaborateurs puissent, à tout moment et de façon fiable, accéder aux documents requis. Chaque document de qualité passe par différentes phases: élaboration, contrôle, approbation, validation, diffusion et, éventuellement, le document est assorti d’une date de fin de validité. Pour les centrales nucléaires, il y a aujourd’hui 1,7 million de documents qui sont stockés en SAP. Chaque année, quelque 55 000 documents sont ajoutés et 32 000 sont mis à jour. L’accès à ces documents est enregistré par groupes cibles et plus de 300 personnes travaillent quotidiennement pour le Document Management. Tous ces collaborateurs ont une habilitation de sécurité. Les documents réglementés par la loi dans la catégorie “Confidentiel et Secret” ne sont pas stockés sur les serveurs.

En fonction de la classification, il y a différentes méthodes d’archivage:

— la politique du Groupe ENGIE au sujet de la protection du patrimoine au niveau des documents internes est la suivante:

+ tous les documents sont présumés internes;

+ les documents internes ne peuvent être rendus publics qu’avec l’accord de la hiérarchie;

+ il y a des documents internes à diffusion restreinte: le niveau “restreint” leur est appliqué et ils ont une étiquette orange; c’est un document muni d’une telle étiquette qui s’est retrouvé dans la presse et est l’une des raisons de cette audition en sous-commission;

+ il y a des documents internes revêtant un caractère confidentiel: le niveau “secret” leur est appliqué et ils ont une étiquette rouge;

— spécifique pour les documents réglementés: une distinction est établie entre les différentes législations en vigueur:

+ de wet van 11 december 1998 voorziet drie niveaus: beperkte verspreiding, vertrouwelijk en geheim;

+ de wet van 15 april 1994 voorziet eveneens drie niveaus voor de nucleaire documenten: beperkte verspreiding – NUC, vertrouwelijk – NUC en geheim – NUC.

De vertrouwelijke en geheime documenten zijn op geen enkele server terug te vinden, maar worden in brandkoffers bewaard.

Voor wat de *Cybersecurity* bij de Belgische kerncentrales betreft, wijst mevrouw Thoelen erop dat er in 2011 *stress tests* werden uitgevoerd in lidstaten van de Europese Unie en dat eind 2011 de robuustheid van de Belgische kerncentrales in extreme omstandigheden werd aangetoond: *"the assessments show that the facilities are robust enough to face extreme conditions, considering the numerous Lines of defence and the additionnel mobile services that were deployed and implemented soon after the accident in Fukushima."*

Bovenop de Europese *stress tests* heeft België het toepassingsgebied van deze evaluaties uitgebreid tot andere mogelijke bedreigingen die verband houden met menselijke activiteiten en tot andere kwaadwillige handelingen waaronder vliegtuigcrashes en *cyberattack*.

Uit deze tests blijkt dat de Belgische kerncentrales tot de meest robuuste van de wereld behoren.

Dit werd ook bevestigd in het verslag van het FANC van januari 2012:

"een cyberaanval kan niet leiden tot een verlies van de veiligheidsfuncties; de informaticabeveiligingsstrategie is vergelijkbaar met die van andere bedrijven die zich bewust zijn van de gebruikelijke risico's voor de gevoelige systemen: segmentatie van netwerken volgens toegang via *firewalls*, *monitoring, hardening* van de systemen, preventie van de malware, procedures, opleidingen,…."

De cyberbeveiligingsaspecten worden voortdurend opgevolgd. Er worden met dit doel regelmatig *meetings* met het FANC georganiseerd.

Tot slot onderlijnt de spreekster dat de Belgische kerncentrales niet worden bestuurd met informaticasystemen. De aansturing van de kringen gebeurt niet door informaticasystemen.

Mevrouw Thoelen besluit dat bij Electrabel de nucleaire veiligheid prioritair is en centraal staat:

+ la loi du 11 décembre 1998 prévoit trois niveaux: diffusion restreinte, confidentiel et secret;

+ la loi du 15 avril 1994 prévoit également trois niveaux pour les documents nucléaires: diffusion restreinte – NUC, confidentiel – NUC et secret – NUC.

Les documents confidentiels et secrets ne sont pas stockés sur un serveur, ils sont conservés dans des coffres-forts.

S'agissant de la cybersécurité dans les centrales nucléaires belges, Mme Thoelen souligne qu'en 2011, des tests de résistance ont été réalisés dans les États membres de l'Union européenne et que fin 2011, la robustesse des centrales nucléaires belges lors d'évènements externes exceptionnels a été démontrée: "*the assessments show that the facilities are robust enough to face extreme conditions, considering the numerous Lines of defence and the additionnel mobile services that were deployed and implemented soon after the accident in Fukushima*.".

Outre les tests de résistance européens, la Belgique a étendu le champ d'application de ces évaluations à d'autres menaces potentielles d'origine humaine et à d'autres actes de malveillance, dont les avions suicides et les cyberattaques.

Il ressort de ces tests que les centrales nucléaires belges font partie des plus robustes au monde.

Cela a également été confirmé dans le compte rendu de l'AFCN de janvier 2012:

"la perte des fonctions de sûreté des centrales nucléaires résultant d'une attaque informatique est impossible; l'exploitant a une stratégie de sécurité informatique comparable à celles de toute société consciente des risques habituels sur des systèmes sensibles (segmentation des réseaux en fonction des accès via firewalls, monitoring, hardening des systèmes, prévention des malwares, procédures, formations…)".

Les aspects de la cybersécurité font l'objet d'un suivi permanent. Dans cette optique, des réunions sont organisées régulièrement avec l'AFCN.

Enfin, l'oratrice souligne que les centrales nucléaires belges ne sont pas gérées par le biais de systèmes informatiques. La gestion des circuits ne se fait pas via les systèmes informatiques.

Mme Thoelen conclut que pour Electrabel, la sûreté nucléaire est la priorité absolue:

— de nucleaire sector is de meest gecontroleerde industriële sector ter wereld;

— de nucleaire veiligheid staat centraal in de activiteiten van het bedrijf en is ingebed in de bedrijfscultuur;

— de informatiebeveiliging maakt integraal deel uit van de nucleaire veiligheid;

— in de nucleaire activiteiten geldt een cultuur van continue verbetering.

Electrabel is zich wel bewust van de vragen die leven bij de publieke opinie en verklaart in alle transparantie te zullen communiceren en inspanningen te zullen doen opdat eenieder zich een eigen mening kan vormen over de Belgische kerncentrales.

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

De heer Eric Thiébaut (PS) wenst in de eerste plaats in te gaan op het in de pers gelekte document. Meer algemeen merkt de spreker op dat het feit dat er een interne audit werd doorgevoerd op zich een positief feit betekent. Maar uit deze audit blijken toch duidelijk een aantal tekortkomingen in het documenten beheer van Electrabel. Deze tekortkomingen werden daarenboven reeds vastgesteld in de zomer 2015. Maar in een persbericht van het FANC van 6 oktober 2016 leest de spreker het volgende: “Het Koninklijk Besluit van 17 oktober 2011 houdende de categorisering en bescherming van nucleaire documenten bepaalt dat alle exploitanten van nucleaire installaties moeten beschikken over een systeem voor het veilige beheer van gecategoriseerde documenten en gevoelige informatie. Sinds de publicatie van dit K.B. hebben de exploitanten de nodige acties opgestart om zich te conformeren aan de wettelijke vereisten. Het is in deze context dat Electrabel in 2014 en 2015 een interne audit heeft uitgevoerd. Doel van de audit was om het beheer van gecategoriseerde documenten binnen het bedrijf in kaart te brengen. Daarbij werd een reeks aandachtspunten geïdentificeerd. Het rapport van deze audit dateert van juni 2015 en beschrijft de situatie zoals die anderhalf jaar geleden door Electrabel zelf werd opgetekend. Volgens het bedrijf is sindsdien een reeks verbeteringsacties ondernomen. Het FANC waakt erover dat de exploitanten van nucleaire installaties hun wettelijke verplichtingen op het vlak van de veiligheid en beveiliging nakomen. Die controle gebeurt door middel van regelmatige inspecties. De volgende inspecties rond het thema van de beveiliging van gevoelige informatie staan gepland in 2017. Indien er op dat moment effectief nog tekortkomingen zijn, zal het FANC erop toezien dat de exploitant die zo snel mogelijk wegwerkt.”

— le secteur nucléaire est le secteur industriel le plus contrôlé dans le monde;

— la sûreté nucléaire est centrale dans les activités de l’entreprise et est inscrite au plus profond de sa culture;

— la protection de l’information fait partie intégrante de la sûreté nucléaire;

— La culture de l’amélioration continue prévaut dans les activités nucléaires.

Electrabel est consciente des interrogations présentes dans l’opinion publique et indique qu’elle communiquera en toute transparence et fera des efforts pour que tout un chacun puisse se forger sa propre opinion sur les centrales nucléaires belges.

C. **Questions et observations des membres**

M. Éric Thiébaut (PS) souhaite tout d’abord aborder la question du document qui a fuité dans la presse. De manière plus générale, l’intervenant observe que le fait qu’un audit interne ait été réalisé est en soi un élément positif. Cet audit a toutefois mis distinctement en lumière plusieurs manquements dans la gestion des documents d’Electrabel. Ces manquements avaient de surcroît déjà été constatés à l’été 2015. Pourtant, dans un communiqué de presse publié le 6 octobre 2016 par l’AFCN, l’intervenant a pu lire ce qui suit: “L’arrêté royal du 17 octobre 2011 portant sur la catégorisation et la protection des documents nucléaires stipule que tous les exploitants d’installations nucléaires doivent disposer d’un système garantissant la gestion sûre des documents catégorisés et des renseignements sensibles. Depuis la publication de cet arrêté, les exploitants ont entamé les actions nécessaires pour se conformer aux exigences légales. C’est dans ce contexte qu’Electrabel a réalisé un audit interne en 2014 et 2015. Le but de cet audit était d’évaluer la gestion des documents catégorisés au sein de l’entreprise. Cet exercice a permis d’identifier certains aspects à surveiller. Le rapport d’audit date de juin 2015 et décrit la situation telle que l’a constatée Electrabel voici 18 mois. Selon l’entreprise, une série d’actions d’amélioration ont été entreprises depuis lors. L’AFCN vérifie que les exploitants d’installations nucléaires respectent leurs obligations légales sur le plan de la sûreté et de la sécurité. Ce contrôle s’exerce sous forme d’inspections régulières. Les prochaines inspections portant sur le thème de la sécurité des renseignements sensibles sont prévues en 2017. Si des manquements sont observés à cette occasion, l’AFCN veillera alors à ce que l’exploitant les corrige dans les meilleurs délais.”

De heer Thiébaut wijst er bovendien op dat hij de uiteenzetting van mevrouw Thoelen duidelijk en geruststellend vindt. Maar hij is bekommerd over het feit dat er zo'n groot verschil is in de helderheid van het betoog van mevrouw Thoelen en alle in de pers verschenen berichten over dit dossier. Voorts wenst de spreker te vernemen of de in de audit vastgestelde tekortkomingen ondertussen werden rechtgezet. Het feit dat het FANC nog geen erkenning verstrekte, baart het lid toch zorgen. Waarom werd deze erkenning nog niet verstrekt? Welke tekortkomingen moeten nog worden weggewerkt?

De heer Michel de Lamotte (cdH) wenst in eerste instantie te vernemen hoeveel deskundigen in *cybersecurity* op dit ogenblik werkzaam zijn bij het FANC. Vervolgens herinnert de heer de Lamotte eraan dat mevrouw Thoelen in haar uiteenzetting onderlijnde dat *cybersecurity* op de sites van de kerncentrales een absolute prioriteit is voor Electrabel. Maar de spreker stelt, zoals de heer Thiébaut vast, dat Electrabel over haar beleid inzake deze prioriteit van het FANC geen erkenning kreeg. Dit feit is toch verontrustend. Waarom heeft het FANC tot op vandaag zijn goedkeuring geweigerd? Wat zijn de exacte redenen?

Welke grote uitdagingen op het vlak van *cybersecurity* dienen zich de komende zes maanden aan? Welke mogelijke *cyberattacks* zijn het meest waarschijnlijk?

Van het FANC wenst de spreker te vernemen hoe het Agentschap de houding van de kernexploitant ten aanzien van *cybersecurity* inschat. Heeft het FANC de volle bevoegdheid om Electrabel in deze aangelegenheid te controleren?

De heer Jean-Marc Nollet (Ecolo-Groen) onthoudt uit de uiteenzetting van mevrouw Thoelen dat Electrabel één van de meest solide bedrijven zou zijn voor wat betreft *cybersecurity*. De heer Nollet stelt zich bij deze bewering toch heel wat vragen gezien het feit dat het FANC tot nog toe zijn erkenning niet heeft willen verstrekken. Is mevrouw Thoelen wel heel zeker van haar zaak? De spreker heeft vernomen dat er door Engie Electrabel een penetratietest werd afgenomen. Wat was het resultaat van deze test? Welke waren de positieve punten, welke de negatieve punten? Aan welke punten zal concreet worden verder gewerkt? Voorts wenst de heer Nollet van mevrouw Thoelen zelf te vernemen waarom het FANC tot nog toe de erkenning weigerde.

Vervolgens citeert de heer Nollet een aantal zinnen uit de interne audit van Electrabel om aan te tonen dat er toch problemen waren: zo zou een onderaannemer in het bezit zijn van alle veiligheidsplannen van de nucleaire sites, zonder dat Electrabel hiervan zelf op de

M. Thiébaut signale par ailleurs qu'il a trouvé clair et rassurant l'exposé de Mme Thoelen. Il se dit cependant préoccupé par le fait qu'il existe un tel contraste entre l'exposé limpide de Mme Thoelen et toutes les informations relatives à ce dossier qui ont été publiées dans la presse. Ensuite, l'intervenant souhaite savoir si les manquements constatés dans l'audit ont entretemps été corrigés. Le fait que l'AFCN n'ait pas encore confirmé la correction des manquements inquiète le membre. Pourquoi cette confirmation n'a-t-elle pas encore été apportée? Quels manquements doivent encore être corrigés?

M. Michel de Lamotte (cdH) souhaiterait d'abord savoir combien d'experts en cybersécurité travaillent actuellement à l'AFCN. Ensuite, M. de Lamotte rappelle que Mme Thoelen a souligné dans son exposé que la cybersécurité sur les sites des centrales nucléaires est une priorité absolue pour Electrabel. Cependant, l'intervenant constate, tout comme M. Thiébaut, que la politique menée par Electrabel concernant cette priorité n'a pas été agréée par l'AFCN. Ce fait est tout de même préoccupant. Pourquoi l'AFCN a-t-elle refusé jusqu'à présent de donner son approbation? Quelles en sont les raisons exactes?

Quels sont les grands défis à relever en matière de cybersécurité au cours des six prochains mois? Quels types de cyberattaques sont les plus vraisemblables?

L'intervenant demande à l'AFCN comment elle évalue l'attitude de l'exploitant nucléaire à l'égard de la cybersécurité. L'AFCN est-elle pleinement compétente pour contrôler Electrabel en la matière?

M. Jean-Marc Nollet (Ecolo-Groen) retient de l'exposé de Mme Thoelen qu'Electrabel serait l'une des entreprises les plus solides en matière de cybersécurité. M. Nollet se pose tout de même de nombreuses questions concernant cette affirmation, vu que l'AFCN n'a pas voulu, jusqu'à présent, agréer la politique d'Electrabel en la matière. Mme Thoelen est-elle bien sûre de son fait? L'intervenant a appris qu'Engie Electrabel a réalisé un test de pénétration. Quel en a été le résultat? Quels étaient les points positifs et négatifs? À quels points travaillera-t-on encore concrètement? M. Nollet demande ensuite à Mme Thoelen elle-même pourquoi l'AFCN a refusé, jusqu'à présent, d'agréer la politique d'Electrabel en matière de cybersécurité.

Ensuite, M. Nollet cite quelques phrases de l'audit interne d'Electrabel en vue de prouver qu'il y a tout de même eu des problèmes: ainsi, un sous-traitant aurait été en possession de tous les plans de sécurité des sites nucléaires, sans qu'Electrabel soit au courant.

hoogte was. Hoe rijmt mevrouw Thoelen dit met haar eerdere verklaringen? Ook werden in de interne audit 26 tekortkomingen vastgesteld waaraan Electrabel moest remediëren.

In de pers verklaarde de heer Bens, directeur-generaal van het FANC, dat Electrabel nog drie maanden de tijd kreeg om zich in regel te stellen. Wanneer zullen deze drie maanden zijn verstreken?

De heer de Bruycker (CCB) verduidelijkte het begrip "*Information exchange gateway"*. Hoe zal dit concept door Electrabel worden geïmplementeerd? Of kiest Electrabel voor andere beveiligingssystemen? Mevrouw Thoelen verklaarde dat alle niet geheime of niet vertrouwelijke documenten bewaard worden op SAP servers. Kan zij aangeven welke personen binnen Electrabel toegang hebben tot de veiligheidsplannen die op het Internet zouden hebben gecirculeerd?

Vervolgens gaat de heer Nollet nader in op de berichtgeving vanwege Electrabel: na het in de pers verschijnen van de interne audit, verklaarde Electrabel dat het om een document met verouderde gegevens ging. Inderdaad, de audit dateert van 2015. Maar moest Electrabel zich ondertussen volledig geconformeerd hebben naar de toepasselijke wetgeving, dan zou het FANC toch zijn goedkeuring niet weigeren, zo oordeelt de heer Nollet. Er kan in deze dan ook geen sprake zijn van eerlijke communicatie vanwege Electrabel. De heer Nollet vraagt dan ook dat zowel het FANC als Electrabel op een eerlijke, open manier zouden communiceren. Heeft het FANC de goedkeuring geweigerd omwille van belangrijke tekortkomingen of betreft het veeleer minder belangrijke elementen?

Kan mevrouw Thoelen garanderen dat de *back ups* voor de elektronische data nooit het Belgisch territorium hebben verlaten? Zijn er nooit *back ups* geplaatst in India of Frankrijk?

Welk veiligheidsbeleid hanteert Electrabel ten aanzien van onderaannemers? Hoeveel personen zijn vandaag via onderaanneming in de kerncentrales en op het hoofdkantoor van Electrabel te werk gesteld? Hoeveel personen werken in onderaanneming in de IT of in de IT-beveiliging? Wat zijn de evoluties in dit verband gedurende de laatste 10 jaren: aantal onderaannemers en op het totaal, het aandeel dat de IT-ers hierin innemen? Ook wenst de spreker een zicht te krijgen op de evolutie van het aantal IT-ers voor dezelfde periode, namelijk "*in house*" en "in onderaanneming". Immers, bij een merkelijke verhoging van het aantal onderaannemers zal ook het aantal documenten dat circuleert onvermijdelijk

Comment Mme Thoelen concilie-t-elle cela avec ses déclarations antérieures? L'audit interne a également permis de constater 26 problèmes auxquels Electrabel devait remédier.

M. Bens, le directeur général de l'AFCN, a déclaré dans la presse qu'Electrabel avait encore trois mois pour se mettre en règle. Quand ces trois mois seront-ils écoulés?

M. de Bruycker (CCB) a précisé la notion d'"*Information exchange gateway*". Comment ce concept sera-t-il mis en œuvre par Electrabel? Ou bien la société Electrabel optera-t-elle pour d'autres systèmes de sécurisation? Mme Thoelen a déclaré que tous les documents non secrets ou non confidentiels sont stockés sur des serveurs SAP. Pourrait-elle indiquer qui, au sein d'Electrabel, a accès aux plans de sécurité qui auraient circulé sur l'internet?

M. Nollet se penche ensuite sur la communication faite par Electrabel: après la publication de l'audit interne dans la presse, Electrabel a déclaré que ce document contenait des données obsolètes. Cet audit date en effet de 2015. Mais l'intervenant considère que si Electrabel s'était entièrement conformée dans l'intervalle à la législation applicable, l'AFCN n'aurait pas refusé de donner son aval. Il n'y a donc pas eu de communication honnête de la part d'Electrabel. M. Nollet souhaiterait que l'AFCN et Electrabel communiquent de façon honnête et ouverte. L'AFCN a-t-elle refusé son approbation en raison de manquements conséquents, ou s'agit-il plutôt d'éléments de moindre importance?

Mme Thoelen peut-elle garantir que les *back ups* des données électroniques n'ont jamais quitté le territoire belge? N'a-t-on jamais placé de *back ups* en Inde ou en France?

Quelle est la politique menée par Electrabel en matière de sécurité à l'égard de ses sous-traitants? Quel est le nombre de personnes travaillant actuellement en sous-traitance dans les centrales nucléaires et au siège principal d'Electrabel? Quel est le nombre de personnes travaillant en sous-traitance dans le domaine de l'informatique ou de la sécurité informatique? Quelles sont les évolutions observées au cours de ces dix dernières années au niveau du nombre de sous-traitants et en particulier de la part qu'occupent les spécialistes en *IT*? L'intervenant demande également de quelle façon le nombre de spécialistes en *IT* a évolué pour la même période – "*in house*" et "en sous-traitance". En effet, une

toenemen, met alle veiligheidsrisico's van dien. Zijn er hiervoor voldoende veiligheidsmaatregelen voorzien?

In een antwoord op een mondelinge vraag aan de minister bevoegd voor Veiligheid, leest de heer Nollet dat het FANC zijn eerste specialist inzake cyberveiligheid heeft aangeworven in 2010. Dit bleek achteraf echter niet juist te zijn want in 2015 heeft het FANC nog verklaard dat het Agentschap het niet nodig vond onder de eigen personeelsleden medewerkers te rekruteren met een specialisatie "cyberveiligheid". Kan het FANC deze ongerijmdheid verklaren?

Tot slot wijst de heer Nollet erop dat er verscheidene getuigenissen zijn vanuit de sector die op hetzelfde neerkomen: indien er tien jaar geleden veiligheidsproblemen werden gemeld van welke aard ook, dan werden onmiddellijk voldoende middelen vrijgemaakt om hieraan ter remediëren. Dit is vandaag niet meer het geval, terwijl de veiligheidsproblemen groter zijn. Rentabiliteit gaat blijkbaar boven veiligheid, zo stelt de heer Nollet vast en hij betreurt dit.

Een laatste vraag voor mevrouw Thoelen, Electrabel: mag het document betreffende de interne audit, dat bestemd is voor beperkte verspreiding en het label oranje draagt, verspreid worden onder de leden van de subcommissie?

De heer Egbert Lachaert (Open Vld) wijst erop dat het moeilijk debatteren is in een vergadering waar er een onevenwicht in voorkennis bestaat bij de leden over de interne audit van Electrabel. De spreker hoopt dan ook dat er een manier kan worden gevonden om aan alle leden van de subcommissie inzagerecht te verlenen van de interne audit van Electrabel.

Omwille ook van de vele tegengestelde signalen die er uitgestuurd worden over de juiste staat van de cyberveiligheid van de kerncentrales, verklaart de spreker nog niet gerustgesteld te zijn. Dit blijkt ook uit de uiteenzettingen van de sprekers: het FANC en de exploitant zitten duidelijk nog niet op dezelfde golflengte. Het FANC heeft recent nog publiek verklaard dat er zich op bepaalde nucleaire sites hardnekkige problemen inzake veiligheidscultuur stellen. De boodschap van mevrouw Thoelen beweert dan weer het tegendeel. Niemand heeft een boodschap aan een zwart-wit verhaal in deze aangelegenheid. Hoe kan dit dossier verder worden geobjectiveerd zodat de publieke opinie kan worden gerustgesteld? Het is duidelijk dat de menselijke factor in de veiligheidscultuur cruciaal is. Hoe wordt eraan

augmentation importante du nombre de sous-traitants s'accompagne inévitablement d'une augmentation du nombre de documents en circulation, avec tous les risques que cela implique en termes de sécurité. Des mesures de sécurité suffisantes ont-elles été prévues à cet égard?

Dans une réponse à une question orale adressée au ministre en charge de la Sécurité, M. Nollet lit que l'AFCN a engagé son premier expert en cybersécurité en 2010, ce qui s'est toutefois révélé faux *a posteriori*, car l'AFCN déclarait encore en 2015 qu'elle n'estimait pas nécessaire le recrutement de collaborateurs spécialisés en cybersécurité parmi son personnel. L'AFCN peut-elle expliquer cette ineptie?

Enfin, M. Nollet indique que différents témoignages livrés au sein du secteur convergent vers la même conclusion: si des problèmes de sécurité, de quelque nature qu'ils soient, avaient été signalés il y a dix ans de cela, des moyens suffisants auraient immédiatement été dégagés pour y remédier. Ce n'est plus le cas à l'heure actuelle, alors que les problèmes de sécurité sont encore plus graves. M. Nollet constate et regrette que la rentabilité prime manifestement la sécurité.

Une dernière question pour Mme Thoelen d'Electrabel: est-il possible de distribuer le document relatif à l'audit interne, qui revêt un caractère restreint et porte l'étiquette orange, aux membres de la sous-commission?

M. Egbert Lachaert (Open Vld) observe qu'il est difficile de débattre de ce sujet lors d'une réunion où tous les membres ne disposent pas des mêmes connaissances préalables sur l'audit interne d'Electrabel. Par conséquent, l'intervenant espère qu'une solution pourra être trouvée pour permettre à tous les membres de la sous-commission de consulter l'audit interne d'Electrabel.

L'intervenant déclare ne pas encore être rassuré, en raison aussi des nombreux signaux contraires émis concernant l'état réel de la cybersécurité dans les centrales nucléaires. Comme le prouvent les exposés des orateurs, l'AFCN et l'exploitant ne sont clairement pas sur la même longueur d'onde. Récemment, l'AFCN a encore déclaré publiquement que sur certains sites nucléaires, des problèmes persistants relatifs à la culture de sécurité se posaient. L'exposé de Mme Thoelen prétend le contraire. Il faut probablement chercher la vérité entre ces deux versions. Comment peut-on objectiver davantage ce dossier afin de rassurer l'opinion publique? Il est évident que le facteur humain est crucial dans la culture de sécurité. Quelles sont les mesures prises pour prévenir, par exemple, les

gewerkt om bijvoorbeeld sabotages door eigen personeelsleden of onderaannemers te vermijden?

Van het FANC wenst de heer Lachaert een duidelijk overzicht van de belangrijke incidenten en wat de reactie van het FANC is en de uiteindelijke remedies die de exploitant doorvoert. Indien nodig zou een dergelijke informatievergadering achter gesloten deuren kunnen worden gevoerd. Het is de taak van de subcommissie om elk mogelijk veiligheidsrisico uit te klaren.

De heer Bert Wollants (N-VA), voorzitter a.i., wenst van mevrouw Thoelen te vernemen wat de juridische status is van de interne audit waarnaar de heer Nollet verwees en onder welke voorwaarden de leden van de subcommissie eventueel kennis zouden kunnen nemen van dit document.

Eenzelfde vraag heeft de heer Wollants over de twee brieven van het FANC, gericht aan de bedrijfsleiding van Engie Electrabel, in verband met de problemen inzake de veiligheidscultuur.

Vervolgens verwijst de spreker naar de stress tests die in 2011 hebben plaatsgevonden, alsook naar het verslag van januari 2012 betreffende de"*man made events*": uit deze verslagen bleek duidelijk dat het grootste deel van de systemen van de kerncentrales niet verbonden is met het Internet. Maar er wordt wel verwezen naar uitrusting die gebruik maakt van digitale en computergebaseerde technologie in het verslag zelf, gevalideerd door het FANC. Is het verbeteringsprogramma ter verhoging van het veiligheidsniveau ondertussen volledig uitgevoerd?

Eerder werd gesteld dat er aan het luik "referentiedreiging" wordt gewerkt. Hoe moet men dit concreet interpreteren? De referentiedreiging waaraan moet worden getoetst, wordt nog verder uitgewerkt. Bestaan er internationale referenties die zouden kunnen worden gebruikt? Of kan er geleerd worden van referenties die gehanteerd worden door de ons omringende landen? Indien dit niet geval is: wat was dan het toetsingskader dat werd gehanteerd bij het opstellen van het verslag *"man made events"* , zo wenst de heer Wollants te vernemen. Werd er enkel nagegaan wat het niveau van de dreiging was? Welke stappen worden nog voorbereid ter verzekering van de cyberveiligheid? Hoe gaat Electrabel daarmee om? Welke garanties zijn er dat de dataservers en *back ups* in België blijven? Worden de *back ups* ook op de nucleaire sites bewaard?

Voor wat het aanwezig zijn van deskundigen "cyberveiligheid" in het FANC betreft, heeft de heer Wollants op de website van het Agentschap een in

sabotages perpétrés par le personnel lui-même ou par des sous-traitants?

M. Lachaert souhaite que l'AFCN présente un relevé clair des incidents graves, de ses réactions à la suite desdits incidents et des mesures finales que l'exploitant a mises en œuvre. Une telle réunion d'information pourrait au besoin se dérouler à huis clos. La sous-commission a la tâche d'expliciter tout risque potentiel pour la sécurité.

M. Bert Wollants (N-VA), président ad interim, souhaite que M. Thoelen lui dise quel est le statut juridique de l'audit interne évoqué par M. Nollet et à quelles conditions les membres de la sous-commission pourraient éventuellement prendre connaissance de ce document.

M. Wollants pose la même question concernant les deux courriers que l'AFCN a adressés à la direction de l'entreprise Engie Electrabel au sujet des problèmes en matière de culture de sécurité.

L'intervenant renvoie ensuite aux *stress tests* qui ont eu lieu en 2011, ainsi qu'au rapport de janvier 2012 concernant les "*man made events*". Il en était clairement ressorti que la plus grande partie des systèmes des centrales nucléaires n'est pas connectée à l'Internet. Il est en revanche question d'équipement qui recourt à la technologie numérique et informatique dans le rapport même validé par l'AFCN. Le programme d'amélioration en vue du relèvement du niveau de sécurité a-t-il été entièrement mis en œuvre dans l'intervalle?

Il avait été affirmé précédemment que le volet "menace de référence" était en cours d'élaboration. Comment faut-il l'interpréter concrètement? La menace de référence, sur la base de laquelle s'effectueront les contrôles, doit encore être affinée. Existe-t-il des références internationales qui pourraient être utilisées? Ou peut-on tirer des enseignements des références employées dans les pays voisins? Si tel n'est pas le cas, M. Wollants souhaite savoir quel était le cadre de contrôle appliqué lors de la rédaction du rapport *"man made events"*. A-t-on uniquement contrôlé quel était le niveau de la menace? Quelles mesures sont encore préparées en vue d'assurer la cybersécurité? Quelle est l'approche d'Electrabel en la matière? Quelles sont les garanties quant au maintien en Belgique des serveurs et des *back ups*? Les *back ups* sont-ils également conservés sur les sites nucléaires?

Concernant la présence d'experts en cybersécurité au sein de l'AFCN, M. Wollants a retrouvé une offre d'emploi publiée en 2010 sur le site web de l'Agence.

2010 gepubliceerde vacature teruggevonden. Bij de aanwervingsvereisten werd zowel kennis van cyberveiligheid als kennis van nucleaire installaties verondersteld. Hoe wordt deze kennis getoetst bij aanwerving?

D. **Antwoorden van de sprekers**

Electrabel

Mevrouw Els Thoelen wenst in de eerste plaats het belang te onderstrepen van "agrément – erkenning" en "habilitation – veiligheidsmachtiging".

Bij de erkenning gaat het om de fysieke beveiliging van de kerncentrales. Deze fysieke beveiliging wordt gecontroleerd door het FANC. Op dit ogenblik bevindt men zich in de eindfase van de beoordeling van de nucleaire sites: fysieke controle behelst: hoe zit het met het alarmbeheer, hoe worden de fysieke bewakingsdiensten gecontroleerd, worden de voertuigen gecontroleerd, hoe worden bezoekers van de centrales gescreend,… Er is met andere woorden op dit ogenblik nog geen erkenning geweigerd. Maar dit dossier bevindt zich in de finale toekenningfase. Het FANC moet zich met andere woorden nog uitspreken.

Een veiligheidsmachtiging wordt toegekend door de Nationale Veiligheidsoverheid, en niet door het FANC. Alle personen die werkzaam zijn op de kerncentrales hebben een veiligheidsmachtiging en bepaalde personen die toegang hebben tot bepaalde informatie hebben ook een veiligheidsmachtiging. Electrabel heeft als onderneming ook een veiligheidsmachtiging bekomen in 2015. De NVO doet wel een beroep op het FANC om het gedeelte te bekijken van de wettelijk gereglementeerde documenten binnen Electrabel. Eind oktober heeft er hierover een audit door het FANC plaatsgevonden om dit specifiek onderdeel te evalueren. Op dit ogenblik worden er met het FANC gegevens uitgewisseld, die het Agentschap nader onderzoekt.

Het reeds veelvuldig aangehaalde document betreffende de interne audit, is een intern document van Electrabel. Dit document was bedoeld om de controle door het FANC voor te bereiden betreffende het documentenbeheer. De 26 opmerkingen die in de audit werden weerhouden, zijn op dit ogenblik allemaal beantwoord en opgelost. Aangezien het een intern document betrof, werd dit document ook nooit overgemaakt aan het FANC.

Dit document betrof een interne audit die als kompas fungeerde voor de eigen personeelsleden. Alle verbeterpunten zijn ondertussen opgelost. Stilstaan bij het resultaat van die acties is belangrijker dan het raadplegen

Les conditions de recrutement comprenaient une connaissance tant de la cybersécurité que des installations nucléaires. Comment ces connaissances sont-elles évaluées lors du recrutement?

D. **Réponses des orateurs**

Electrabel

Mme Els Toelen souhaiterait tout d'abord souligner l'importance de l'"agrément – erkenning" et de l'"habilitation – veiligheidsmachtiging".

L'agrément concerne la protection physique des centrales nucléaires, qui est contrôlée par l'AFCN. On se trouve actuellement dans la phase finale de l'évaluation des sites nucléaires. Le contrôle physique porte sur les points suivants: la manière dont l'alarme est gérée, dont les services de gardiennage physiques, dont les véhicules et les visiteurs des centrales sont contrôlés, etc. Autrement dit, aucun agrément n'a encore été refusé pour l'instant. Ce dossier se trouve dans sa phase finale d'attribution. En d'autres termes, l'AFCN doit encore se prononcer en la matière.

Les habilitations sont octroyées par l'Autorité nationale de sécurité, et non par l'AFCN. Toutes les personnes travaillant dans les centrales nucléaires possèdent une habilitation, de même que certaines personnes ayant accès à certaines informations. En tant qu'entreprise, Electrabel a également obtenu une habilitation en 2015. L'ANS fait cependant appel à l'AFCN en vue d'examiner la partie des documents réglementés par la loi détenus par Electrabel. Fin octobre, l'AFCN a organisé un audit en vue d'évaluer cet élément spécifique. Des données sont actuellement échangées avec l'AFCN, qui est en train d'examiner ces dernières.

Le document maintes fois évoqué relatif à l'audit interne est un document interne d'Électrabel qui visait à préparer le contrôle par l'AFCN de la gestion des documents. Les 26 observations figurant dans l'audit ont toutes obtenu une réponse et été solutionnées. Comme il s'agissait d'un document interne, il n'a jamais été transmis à l'AFCN.

Ce document était donc un audit interne qui servait de boussole aux membres du personnel d'Électrabel. Il a entre-temps été remédié à tous les problèmes mentionnés. Il importe davantage d'examiner le résultat de ces

van het interne kompas. Enkel het eindresultaat en de analyse van het FANC van dit eindresultaat zijn relevant.

Mevrouw Thoelen suggereert dat zij eventueel bereid is om de vergelijkende tabel met actiepunten en stand van zaken aan de leden van de subcommissie te bezorgen.

Op de vragen wat de reële gevaren voor de kerncentrales zijn met betrekking tot cyberbeveiliging, antwoordt mevrouw Thoelen nogmaals dat de kerncentrales niet worden aangestuurd door een digitaal platform. De procesaansturing van de nucleaire delen van de kerncentrales gebeurt analoog en niet digitaal en is dus op geen enkele wijze verbonden met het Internet. De personeelsleden op de sites zelf zijn via een afzonderlijk Intranet verbonden met de server. De server zelf is verbonden met het Internet via *fire walls*. De centrales staan met andere woorden niet rechtstreeks in verbinding met het Internet.

Voor wat de toegang tot de grondplannen van de kerncentrales betreft, antwoordt mevrouw Thoelen dat het voor de medewerkers nodig is om over deze informatie te beschikken. Ook de brandweer en de gemeentelijke overheden van de gemeenten waar de centrales zijn gevestigd, hebben toegang tot deze grondplannen. Dit is nodig omwille van evidente veiligheidsredenen. Er is wel een hiërarchie in de openbaarheid van de plannen voorzien. Er bestaan ook verschillende niveaus van plannen met verschillende niveaus van informatie. Sommige plannen zullen kunnen worden uitgestuurd via het SAP-systeem, maar de wettelijk beschermde plannen worden niet op de SAP-servers bewaard en bevinden zich in brandkoffers.

Het informaticasysteem wordt voornamelijk beheerd door Engie Electrabel zelf. Het enige wat wordt uitbesteed, is het onderhoud van bepaalde servers. Maar de personeelsleden van de onderaannemers hebben geen toegang tot de inhoud van de servers, die geïncrypteerd zijn.

De bewering als zou Electrabel winstoptimalisatie nastreven ten koste van nucleaire veiligheid, houdt geen steek, zo stelt mevrouw Thoelen formeel. Er is vanwege de hiërarchie geen enkele vraag om te besparen op veiligheid in de nucleaire centrales.

actions que de consulter la boussole interne. Seuls le résultat final et son analyse par l'AFCN sont pertinents.

Mme Thoelen indique qu'elle est éventuellement disposée à transmettre aux membres de la sous-commission le tableau comparatif avec les actions et leur état d'avancement.

En réponse aux questions portant sur les dangers réels que représentent les cyberattaques pour les centrales nucléaires, Mme Thoelen souligne encore une fois que les centrales nucléaires ne sont pas commandées par le biais d'une plateforme numérique. Le pilotage des parties nucléaires des centrales est de type analogique et non numérique, et n'est donc relié d'aucune manière à l'internet. Les membres du personnel occupés sur les sites sont quant à eux connectés au serveur par le biais d'un intranet distinct. Le serveur lui-même est relié à l'internet mais protégé par des pare-feu. Autrement dit, les centrales ne sont pas directement raccordées à l'internet.

En ce qui concerne l'accès aux plans des centrales nucléaires, Mme Thoelen répond que les collaborateurs doivent pouvoir avoir accès à cette information. Les services d'incendie et les autorités communales des communes sur le territoire desquelles se trouvent les centrales ont également accès à ces plans, ce qui est nécessaire pour d'évidentes raisons de sécurité. Il existe toutefois une hiérarchie dans le caractère public des plans. Ceux-ci sont en outre organisés en différents niveaux associés à différents niveaux d'information. Certains plans pourront être envoyés par le biais du système SAP, mais les plans légalement protégés ne sont pas conservés sur les serveurs SAP et se trouvent dans des coffres-forts.

Le système informatique est principalement géré par la société Engie Electrabel elle-même. La seule partie qui est sous-traitée est la maintenance de certains serveurs. Mais le personnel des sous-traitants n'a pas accès au contenu des serveurs, qui est crypté.

À propos de l'idée selon laquelle Electrabel tenterait d'optimiser ses bénéfices au détriment de la sûreté nucléaire, Mme Thoelen est formelle: cette affirmation est dénuée de tout fondement. Il n'y a pas la moindre demande, de la part de la hiérarchie, de faire des économies dans le domaine de la sécurité des centrales nucléaires.

FANC

De heer Jan Bens (directeur-generaal van het FANC) sluit zich volledig aan bij de analyse van mevrouw Thoelen met betrekking tot “erkenning-agrément” en “veiligheidsmachtiging – habilitation”.

“Erkenning” betreft het volledige fysieke beveiligingssysteem van de nucleaire installatie. Het bewustzijn van het belang van een verhoging van het fysieke beveiligingssysteem werd geactiveerd na de terroristische aanslagen van 9-11. Tien jaar later werd een wettelijk kader goedgekeurd, met name de koninklijke besluiten van 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties. Deze KB’s voorziet een stappenplan om de nucleaire installaties op het vereiste veiligheidsniveau te brengen. Op 1 november 2016 werd de balans opgemaakt van één van de stappen van dit plan en oordeelde het FANC dat er vooruitgang is gemaakt maar dat het stappenplan nog niet is voleindigd. Dit dossier is met andere woorden nog in evolutie, maar er worden steeds stappen in de goede richting gezet.

Op de vraag van de heer Nollet of het FANC het intern document ooit heeft opgevraagd bij Electrabel, wordt ontkennend geantwoord. De heer Jan Bens, directeur-generaal, verduidelijkt dat het FANC zijn eigen inspectieprogramma opmaakt en niet werkt op basis van interne nota’s van de exploitant.

Het FANC volgt niet alle interne audits van de exploitant op. Het FANC gaat wel na of de exploitant een deugdelijk auditsysteem heeft. Voorts heeft het FANC zijn eigen controle-agenda en aandachtspunten. Als de inspecteurs van Bel-V en FANC specifieke probleempunten op de sites vaststellen, kunnen hierover ook punctuele inspecties worden doorgevoerd. Dit is bijvoorbeeld gebeurd naar aanleiding van de tumultueuze berichtgeving over het documentenbeheer bij de exploitant.

Het FANC beschikt niet over één alleswetende expert inzake cyberbeveiliging. Het gaat om een expertise die verdeeld is over verscheidene FANC-medewerkers. In elk geval beschikt het FANC minstens over één deskundige, ook Bel-V beschikt over minstens één of twee specialisten inzake informaticabeveiliging. Bovendien werkt het FANC, als sectoriële overheid, nauw samen met de specialisten van het CCB. Het criminele luik wordt door de Justitiële overheden opgevolgd.

De analyse van het FANC is dat Electrabel op aanvaardbare wijze de problematiek van cyberbeveiliging

AFCN

M. Jan Bens (directeur général de l’AFCN) souscrit entièrement à l’analyse de Mme Thoelen concernant l’“agrément” et l’“habilitation”.

L’“agrément” porte sur le système intégral de protection physique de l’installation nucléaire. C’est à la suite des attentats terroristes du 11 septembre qu’on s’est rendu compte qu’il était important de renforcer le système de protection physique. Dix ans plus tard, un cadre légal a été adopté: les arrêtés royaux du 17 octobre 2011 relatif à la protection physique des matières nucléaires et des installations nucléaires. Ces arrêtés royaux prévoit un plan phasé visant à garantir que les installations nucléaires atteindront le niveau de sécurité requis. L’une des étapes de ce plan a fait l’objet d’une évaluation en date du 1er novembre 2016. L’AFCN a estimé à cette occasion que des progrès avaient été enregistrés mais que la mise en œuvre du plan n’était pas encore terminée. En d’autres termes, ce dossier est encore en évolution, mais il évolue dans la bonne direction.

M. Jan Bens, directeur général, indique en réponse à la question de M. Nollet que l’AFCN n’a jamais réclamé le document interne à Electrabel. L’orateur précise que l’AFCN établit son propre programme d’inspection et qu’elle ne travaille pas sur la base de notes internes de l’exploitant.

L’AFCN n’assure pas le suivi de l’ensemble des audits internes de l’exploitant. Elle vérifie par contre si ce dernier dispose d’un bon système d’audit. L’AFCN a par ailleurs son propre agenda de contrôle et ses propres points d’attention. Si les inspecteurs de Bel-V et de l’AFCN constatent des problèmes spécifiques sur les sites, des inspections ponctuelles peuvent également être effectuées. Cela a été le cas, par exemple, à la suite de la communication tumultueuse relative à la gestion des documents par l’exploitant.

L’AFCN ne dispose pas d’un expert omniscient en matière de cybersécurité. Il s’agit d’une expertise partagée entre différents collaborateurs de l’agence. L’AFCN dispose en tout état de cause d’au moins un expert et Bel-V, d’au moins un ou deux spécialistes dans le domaine de la protection informatique. De plus, en tant qu’autorité sectorielle, l’AFCN travaille en étroite collaboration avec les spécialistes du CCB. Le suivi du volet criminel est assuré par les autorités judiciaires.

Selon l’analyse de l’AFCN, Electrabel s’attaque à la problématique de la cybersécurité de manière

aanpakt, maar dat er zwakke punten zijn die te maken hebben met de veiligheidscultuur. Hieraan moet nog verder worden gewerkt.

Het FANC zal een gedeklassificeerde versie van de twee brieven van het FANC, waarnaar werd verwezen, aan de leden van de subcommissie overmaken.

Voorts moet er een systeem ontwikkeld worden voor de verschillende mogelijke dreigingscenario's waartegen het fysiek beveiligingssysteem moet bestand zijn. Bij nadere analyse werd vastgesteld dat de dreigingscenario's waarmee de nucleaire sector wordt geconfronteerd, ook gelden voor andere strategische sectoren. Daarom is beslist de krachten te bundelen over de verschillende sectoren heen.

E. **Replieken**

De heer Jean-Marc Nollet (Ecolo-Groen) wenst toch beter te begrijpen waarom het FANC het niet nodig acht om zelf een expert inzake cyberbeveiliging te rekruteren.

De heer Rony Dresselaers (FANC) verduidelijkt dat men een onderscheid moet maken tussen cyberveiligheid en cybercrime: voor het eerste, dat betrekking heeft op de fysieke beveiliging van de nucleaire sites, is het FANC bevoegd en is er expertise aanwezig; voor het tweede, dat tot het bevoegdheidsdomein van de Justitiële overheden behoort, is er in het FANC geen expertise aanwezig.

Op de vraag van de heer Jean-Marc Nollet of Electrabel bereid is om de resultaten van de penetratietests aan de leden van de subcommissie over te maken, antwoordt *mevrouw Thoelen (Electrabel)* positief.

De heer Michel de Lamotte (cdH) vraagt of het FANC de brief van november 2016 betreffende de stand van zaken betreffende de erkenningprocedure aan de leden van de subcommissie kan bezorgen.

De heer Jan Bens, directeur-generaal van het FANC, antwoordt dat het om een document met veiligheidsniveau "Vertrouwelijk-NUC" gaat en bijgevolg niet mag worden verspreid.

De heer Bens verklaarde dat het niveau van Electrabel inzake cyberbeveiliging voldoende is. Moet er veeleer naar excellentie gestreefd worden, zo vraagt *de heer Michel de Lamotte (cdH)* nog. Zal het FANC niet strenger en kordater optreden? Heeft het FANC zelf voldoende middelen om zich te bekwamen in cyberbeveiliging?

acceptable. L'Agence identifie néanmoins des faiblesses liées à la culture de la sûreté. Il faudra encore travailler davantage sur ces points.

L'AFCN transmettra aux membres de la sous-commission une version déclassifiée des deux lettres en question.

En outre, il faut développer un système pour faire face aux différents scénarios de menace potentiels auxquels le système de protection physique doit être capable de résister. Une analyse plus poussée a établi que les scénarios de menace auxquels le secteur nucléaire est confronté s'appliquent également à d'autres secteurs stratégiques. C'est pourquoi il a été décidé de conjuguer les forces, par-delà les différents secteurs.

E. **Répliques**

M. Jean-Marc Nollet (Ecolo-Groen) aimerait tout de même mieux comprendre pourquoi l'AFCN n'a pas jugé nécessaire de recruter elle-même un expert en cybersécurité.

M. Rony Dresselaers (AFCN) précise qu'il faut opérer une distinction entre la cybersécurité et la cybercriminalité: en ce qui concerne la première, qui porte sur la protection physique des sites nucléaires, l'AFCN est compétente et dispose d'experts mais pour la seconde, qui est du ressort des autorités judiciaires, l'AFCN ne dispose d'aucune expertise.

Interrogée par M. Jean-Marc Nollet sur la disposition d'Electrabel à transmettre les résultats des tests de pénétration aux membres de la sous-commission, *Mme Thoelen (Electrabel)* répond par l'affirmative.

M. Michel de Lamotte (cdH) demande si l'AFCN peut fournir aux membres de la sous-commission la lettre de novembre 2016 ayant pour objet l'état d'avancement de la procédure d'agrément.

M. Jan Bens, directeur-général de l'AFCN, répond qu'il s'agit d'un document classé "CONFIDENTIEL – NUC", qui ne peut dès lors être divulgué.

M. Bens déclare que le niveau d'Electrabel en matière de cybersécurité est suffisant. M. de Lamotte lui demande s'il ne faudrait pas plutôt viser l'excellence en la matière. L'AFCN ne devrait-elle pas intervenir plus sévèrement et fermement? L'AFCN dispose-t-elle de moyens suffisants en vue de se former en cybersécurité?

De heer Jan Bens (directeur-generaal FANC) antwoordt dat er wel degelijk gestreefd wordt naar excellentie, maar dat men steeds te maken heeft met evolutieve processen. De missie van het FANC gaat bovendien veel ruimer dan louter de cyberveiligheid. Ook de globale fysieke beveiliging en het correcte informatiebeheer behoort tot de opdracht van het FANC. In dit verband worden de medewerkers van het FANC bijgeschoold inzake cyberbeveiliging. De gespecialiseerde informatie inzake *cybercrime* vindt men terug bij het CCB.

De heer Jean-Marc Nollet (Ecolo-Groen) wenst van Electrabel nog duidelijke cijfers over het aantal personeelsleden van onderaannemers dat werkzaam is in het onderhoud van de ICT-infrastructuur. Hebben deze personen voor het uitoefenen van hun onderhoudsopdracht kennis nodig van de grondplannen van de nucleaire sites? Dit verwondert de spreker ten zeerste.

Mevrouw Griet Heyvaert (Electabel) wenst te weten waarom de heer Nollet deze vraag stelt. Heeft hij de indruk dat er voor deze personen andere veiligheidsregels zouden gelden dan voor de eigen personeelsleden? Dit is immers niet het geval, zo verzekert mevrouw Griet Heyvaert. Zij zal nagaan welke cijfers aan de subcommissie kunnen worden bezorgd.

De heer Jean-Marc Nollet (Ecolo-Groen) verduidelijkt dat hij een vergelijking wenst van het aantal personen, werknemers van Electrabel, dat in het verleden het onderhoud verzekerde en vandaag en dezelfde vergelijking voor de personen die dit werk verrichten in onderaanneming. Hij wenst de evolutie te zien. De spreker vermoedt immers dat uit de cijfers zal blijken dat voor dit specifiek punt Electrabel wel heeft bespaard om rentabiliteitsredenen. Hij vermoedt dat dit een invloed kan hebben op de veiligheidsrisico's. De spreker wenst ook duidelijk te weten wat "onderhoudswerkzaamheden" juist inhouden.

De rapporteur, *De voorzitter a.i.,*

ERIC THIÉBAUT BERT WOLLANTS

M. Jan Bens (directeur général de l'AFCN) répond que l'on tend bel et bien vers l'excellence, mais qu'il s'agit toujours de processus évolutifs. De plus, la mission de l'AFCN va bien au-delà de la simple cybersécurité. La protection physique globale et la gestion correcte de l'information relèvent, elles aussi, de la mission de l'AFCN. À cet effet, les collaborateurs de l'AFCN bénéficient de formations de recyclage en matière de cybersécurité. L'information spécialisée en matière de cybercriminalité se trouve au CCB.

M. Jean-Marc Nollet (Ecolo-Groen) demande à Electrabel de fournir des chiffres précis concernant le nombre de membres de personnel de sous-traitants s'occupant de la maintenance de l'infrastructure ICT. Ces personnes doivent-elles avoir connaissance des plans des sites nucléaires pour effectuer leur mission de maintenance? L'intervenant s'en étonne vivement.

Mme Griet Heyvaert (Electrabel) demande pourquoi M. Nollet pose cette question. A-t-il l'impression que ces personnes sont soumises à d'autres règles en matière de sécurité que les membres du personnel des centrales? Mme Griet Heyvaert assure que tel n'est pas le cas. Elle vérifiera quels chiffres peuvent être transmis à la sous-commission.

M. Jean-Marc Nollet (Ecolo-Groen) précise qu'il souhaite obtenir une comparaison entre le nombre de personnes, travailleurs d'Electrabel, qui assuraient la maintenance par le passé et actuellement et une même comparaison concernant les personnes qui assurent ce travail en sous-traitance. Il souhaite constater l'évolution. L'intervenant présume en effet que les chiffres feront apparaître que, sur ce point précis, Electrabel a effectivement fait des économies pour des raisons de rentabilité. Il présume que cela peut avoir une influence sur les risques de sécurité. L'intervenant s'enquiert également de la teneur exacte des "travaux de maintenance".

Le rapporteur, *Le président a.i.,*

Eric THIÉBAUT Bert WOLLANTS

Centrale drukkerij – Imprimerie centrale