DOC 54 **1744/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

6 april 2016

GEDACHTEWISSELING

met de heer met de heer Miguel De Bruycker, directeur van het Centrum voor Cybersecurity België

VERSLAG

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

INHOUD Blz.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

6 avril 2016

ÉCHANGE DE VUES

avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique

RAPPORT

FAIT AU NOM DE LA COMMISSION DE L'INTÉRIEUR, DES AFFAIRES GÉNÉRALES ET DE LA FONCTION PUBLIQUE 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: Brecht Vermeulen

A. — Vaste leden / Titulaires:

N-VA	Christoph D'Haese, Koenraad Degroote, Koen Metsu, Brecht Vermeulen
PS	Nawal Ben Hamou, Willy Demeyer, Eric Thiébaut
MR	Denis Ducarme, Philippe Pivin, Françoise Schepmans
CD&V	Franky Demon, Veerle Heeren
Open Vld	Katja Gabriëls, Sabien Lahaye-Battheu
sp.a	Monica De Coninck
Ecolo-Groen	Gilles Vanden Burre
cdH	Vanessa Matz

B. — Plaatsvervangers / Suppléants:

Peter Buysrogge, Renate Hufkens, Sarah Smeyers, Valerie Van Peel, Hendrik Vuye
Laurent Devin, André Frédéric, Emir Kir, Laurette Onkelinx
Sybille de Coster-Bauchau, Emmanuel Burton, Caroline Cassart-Mailleux, Stéphanie Thoron
Leen Dierick, Nahima Lanjri, Veli Yüksel
Patrick Dewael, Vincent Van Quickenborne, Frank Wilrycx
Hans Bonte, Alain Top
Wouter De Vriendt, Stefaan Van Hecke
Christian Brotcorne, Isabelle Poncelet

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

VB	Filip Dewinter
DéFI	Olivier Maingain
PP	Aldo Carcaci

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

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Abréviations dans la numérotation des publications:

DOC 54 0000/000:	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
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:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

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

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

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

Les publications sont imprimées exclusivement sur du papier certifié FSC

Dames en Heren,

Uw commissie heeft haar vergadering van 3 februari 2016 gewijd aan een gedachtewisseling met de heer met de heer Miguel De Bruycker, directeur van het Centrum voor Cybersecurity België.

I. — **INLEIDENDE UITEENZETTING**

De heer Miguel De Bruycker, directeur van het Centrum voor Cybersecurity licht toe dat het Centrum is opgericht door het koninklijk besluit van 10 oktober 2014, met als doel bij te dragen aan een veilig en betrouwbaar internet, alsook een nationaal beleid in te voeren met de bestaande actoren. Het gaat bijgevolg om een coördinerende opdracht tussen de verschillende overheidsdiensten.

1. **Organisatie**

Het Centrum hangt rechtstreeks af van de eerste minister. Het is ondergebracht bij de Kanselarij van de eerste minister, waarop een beroep kan worden gedaan voor de administratieve ondersteuning. Bij koninklijk besluit van 2 juni 2015 werd ook twee comités opgericht. Het strategisch comité heeft vertegenwoordigers van de regeringsleden die lid zijn van de Nationale Veiligheidsraad. Daarnaast is er het coördinatiecomité, waarvan de spreker een niet-permanent lid is. Dat houdt in dat hij wordt uitgenodigd om aan de vergadering van het comité deel te nemen telkens wanneer er een thema wordt behandeld dat verband houdt met cyberveiligheid. Hij kan tevens vragen een dergelijk punt te agenderen. De hoofden van de verschillende operationele diensten komen er samen om concrete zaken te bespreken. Dat zorgt ervoor dat een geest van samenwerking en vertrouwen tussen de verschillende diensten kan worden opgebouwd. De eerste ervaringen met het coördinatiecomité zijn alvast zeer positief.

Concreet werkt de heer De Bruycker dus wat betreft de rapportering aan de politieke verantwoordelijken hoofdzakelijk via het coördinatiecomité. Tegelijk wordt ook rechtstreeks gerapporteerd aan de eerste minister, waarbij ook andere punten kunnen worden besproken die moeilijk aan bod kunnen komen tijdens de comitévergaderingen.

2. **Opdrachten**

De opdrachten van het Centrum zijn gedefinieerd in het koninklijk besluit van 10 oktober 2014. Eerst en vooral gaat het om de invoering van een Belgische strategie op het vlak van de cyberveiligheid, en het

Mesdames, Messieurs,

Votre commission a, au cours de sa réunion du 3 février 2016, procédé à un échange de vues avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique.

I. — **EXPOSÉ INTRODUCTIF**

M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique, indique que le Centre a été créé par l'arrêté royal du 10 octobre 2014, dans le but de contribuer à un internet sûr et fiable, et d'instaurer une politique nationale en collaboration avec les acteurs existants. Il s'agit par conséquent d'une mission de coordination entre les différents services publics.

1. **Organisation**

Le Centre dépend directement du premier ministre. Il a été créé auprès de la Chancellerie du premier ministre, à laquelle il peut être fait appel pour l'appui administratif. Deux comités ont également été créés par l'arrêté royal du 2 juin 2015. Le comité stratégique est composé de représentants des autres membres du gouvernement qui sont membres du Conseil national de sécurité. Il y a par ailleurs le comité de coordination, dont l'orateur est un membre non permanent. Cela implique qu'il est invité à participer à la réunion du comité chaque fois que celui-ci examine un thème lié à la cybersécurité. Il peut également demander qu'un tel point soit inscrit à l'ordre du jour. Les responsables des différents services opérationnels s'y réunissent pour examiner des points concrets. Un esprit de collaboration et de confiance peut ainsi être créé entre les différents services. Les premières expériences faites avec le comité de coordination sont déjà très positives.

Concrètement, pour ce qui est du rapportage aux responsables politiques, M. De Bruycker opère essentiellement par le biais du comité de coordination. Il est également fait directement rapport au premier ministre, d'autres points, difficiles à aborder lors des réunions du comité, pouvant alors également être examinés.

2. **Missions**

Les missions du Centre sont définies par l'arrêté royal du 10 octobre 2014. Il s'agit avant tout de l'élaboration d'une stratégie belge en matière de cybersécurité et de la gestion intégrée et centralisée – c'est-à-dire par-delà

geïntegreerd en gecentraliseerd beheer — en dus over de verschillende diensten heen — van de verschillende projecten binnen datzelfde domein. Het gaat dus om de coördinatie van de taken, opdrachten, capaciteiten en verantwoordelijkheden van de verschillende bestaande diensten in België. Het gaat daarbij zowel om de publieke als de private sector, en om de academische wereld.

Het Centrum zal ook voorstellen formuleren tot aanpassing van het wettelijk kader rond de cyberveiligheid. Bij crisissen zal het samen met het Crisiscentrum de beheerscel binnen dat Centrum sturen met het oog op het behandelen en het nemen van de nodige maatregelen.

Tevens zal worden gezorgd voor de verspreiding van richtlijnen en standaarden, en dat voornamelijk ten behoeve van de administraties en de publieke organisaties.

Het Centrum coördineert ook de Belgische vertegenwoordiging op de internationale fora, alsook de evaluatie en eventueel de certificatie van veiligheidssystemen en —componenten die gebruikt worden bij de uitbouw van netwerken.

Een laatste maar niet minder belangrijke opdracht is het sensibiliseren van de gebruikers, zodat zij op de hoogte zijn van de voornaamste dreigingen, kwetsbaarheden en het eventueel gevaarlijk gedrag bij het gebruik van systemen die verbonden zijn met het internet.

3. ***Strategisch plan***

Op basis van het wettelijk kader en de opdrachten die door de eerste minister worden toegewezen heeft het Centrum een strategisch plan opgesteld. Daarin wordt de functionering van het Centrum beschreven voor de komende vijf jaar. Het plan steunt op de visie dat samenwerken aan een veilig internet zal leiden tot meer welvaart. Dat betekent dat er voor gezorgd moet worden dat België geldt als een digitale *safe haven* voor nationale en internationale organisaties en bedrijven, en dat dus tegen 2020.

Vertrekkend vanuit die visie en dat *mission statement* heeft het Centrum een reeks strategische doelstellingen bepaald. Tijdens de opstartfase van het Centrum heeft een brainstormsessie plaatsgevonden om na te gaan wie de klanten zijn van het Centrum, en wie de klanten zijn van België in het domein van de cyberveiligheid. Tegelijk was er de vraag welke diensten aan die klanten verleend moeten worden. In dat verband gaat het om diensten op het vlak van:

les différents services - des différents projets dans ce domaine. Il s'agit donc de coordonner les tâches, missions, capacités et responsabilités des différents services existants en Belgique. En l'occurrence, cela concerne tant le secteur public et privé que le monde académique.

Le Centre formulera également des propositions afin d'adapter la cadre légal en matière de cybersécurité. En cas de crise liée à un cyberincident, il dirigera la cellule de gestion du Centre de Crise en collaboration avec ce dernier en vue d'assurer la gestion de la crise et de prendre les mesures nécessaires.

Le Centre veillera également à diffuser des directives et des normes de sécurité, principalement auprès des administrations et des organismes publics.

Le Centre coordonne également la représentation belge aux forums internationaux sur la cybersécurité, ainsi que l'évaluation et éventuellement la certification des systèmes et composants de sécurité utilisés lors du développement de réseaux informatiques.

Une de ses dernières missions, mais non des moindres, est la sensibilisation des utilisateurs afin de les informer des principales menaces et vulnérabilités informatiques ainsi que des comportements potentiellement dangereux à éviter lors de l'utilisation de systèmes reliés à Internet.

3. **Plan stratégique**

Sur la base du cadre légal et des missions assignées par le Premier ministre, le Centre a élaboré un plan stratégique décrivant son fonctionnement pour les cinq prochaines années. Ce plan part du principe que la collaboration visant à sécuriser Internet créera davantage de prospérité. Le Centre dispose dès lors de cinq ans pour faire de la Belgique un havre de sécurité numérique pour les organismes nationaux et internationaux ainsi que pour les entreprises.

Le Centre a fixé une série d'objectifs stratégiques en tenant compte du principe fondamental de son plan et de son *mission statement*. Lors de la phase de lancement du Centre, une session de brainstorming avait été organisée en vue de déterminer le profil des clients du Centre ainsi que le profil des clients de la Belgique en matière de cybersécurité. Il a également été demandé quels services il convenait de fournir à ces clients. Il s'agit de services concernant:

— *governance*,

— preventie (bescherming van de systemen),

— detectie (monitoring, kennis van de dreigingen) en

— respons wanneer het fout loopt (zorg voor de nodige capaciteit die een gepaste reactie mogelijk maakt).

4. **Doelgroepen**

In functie van de lijsten met de klanten en de diensten werd het doelpubliek opgesplitst in drie groepen:

— de bevolking (“*at home”*);

— de Belgische bedrijven (“*at work”*);

— de groep die gebundeld werd tot de “vitale sectoren”.

Bij de zorg voor het opstellen van de strategische doelstellingen voor de verschillende doelpublieken, stelt men vast dat ten aanzien van de bevolking het belangrijkste element de sensibilisering is, doch zonder een sfeer van wantrouwen of angst ten aanzien van het internet te creëren. Wel moet duidelijk worden gemaakt wat de mogelijke risico’s zijn bij het gebruik van het internet, en hoe het op een veilige manier kan gebeuren.

a. ***Bevolking***

Bij de bescherming van de systemen en de zorg voor veilige netwerken in België moet enerzijds worden ingezet op de veiligheid van die systemen en netwerken (technische veiligheidsmaatregelen), maar anderzijds ook op het gedrag van de gebruiker. De heer De Bruycker trekt de parallel met de verkeersveiligheid: het heeft geen zin om veilige autowegen of wagens te bouwen indien de bestuurders geen veilig rijgedrag vertonen. Beide elementen zijn belangrijk.

Naast de sensibilisering moet gezorgd worden voor ondersteunende informatie. Zonder een angstklimaat in het leven te roepen, moet worden gewezen op dreigingen die actueel en accuraat zijn. Tegelijk moet informatie worden geboden over hoe de burger thuis zijn informatiesysteem kan beveiligen, hoe hij de mogelijke kwetsbaarheid van dat systeem kan nagaan, en wat hij kan doen om dat te verhelpen.

— la gouvernance,

— la prévention (protection des systèmes),

— la détection (monitoring, connaissance des menaces) et

— les réponses à donner en cas d’erreur (veiller à disposer de la capacité nécessaire pour permettre une réaction adéquate).

4. **Groupes cibles**

Le public cible a été divisé en trois en fonction des listes de clients et des listes de services:

— population (“à domicile”),

— entreprises belges (“au travail”),

— groupe réunissant les “secteurs vitaux”.

Lorsqu’on prend soin d’établir les objectifs stratégiques pour les différents publics cibles, on constate que la sensibilisation est l’élément le plus important à l’égard de la population, mais qu’il ne s’agit toutefois pas de créer un climat de méfiance ou de peur face à l’internet. Il convient néanmoins d’indiquer clairement quels sont les risques potentiels liés à son utilisation et comment l’internet peut être utilisé d’une manière sûre.

a. ***Population***

Pour la protection des systèmes et la mise en place de réseaux sûrs en Belgique, il conviendra, d’une part, d’investir dans la sécurité des systèmes et des réseaux (mesures de sécurité techniques) mais aussi, d’autre part, de miser sur les comportements des utilisateurs. M. De Bruycker établit un parallèle avec la sécurité routière: il est inutile de construire des autoroutes ou des voitures sûres si les conducteurs n’adoptent pas une conduite sûre. Ces deux éléments sont importants.

Outre la sensibilisation, il faut également fournir des informations de soutien. Sans susciter un climat d’angoisse, il convient d’attirer l’attention sur les menaces qui sont actuelles et réelles. Il faut également offrir des informations sur la façon dont le citoyen peut sécuriser son système informatique à son domicile, sur la façon de détecter les failles éventuelles de ce système, et sur la manière d’y remédier.

b. ***Bedrijven***

Voor de bedrijven ligt de focus enigszins anders. Via het platform *Cyber Security Coalition Belgium* werden heel wat bedrijven in België bevraagd over hun behoeften: wat verlangen zij van de Belgische overheid op het vlak van de cyberveiligheid? Uit de bevraging is gebleken dat die bedrijven moeite hebben om te bepalen welke veiligheidsmaatregelen zij moeten nemen binnen hun eigen bedrijf. Zij zijn met andere woorden vragende partij voor een standaardraamwerk met richtlijnen, goede praktijken en adviezen die toelaten de cyberveiligheid te implementeren.

Het spreekt voor zich dat met de bedrijven partnerschappen zullen worden gesloten die de samenwerking rond cyberveiligheid mogelijk maakt. Tegelijk zal waar mogelijk gezorgd worden voor de beschikbaarheid van veilige technologieën.

c. ***Vitale sectoren***

De wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren bepaalt dat er in België vier sectoren van kritieke infrastructuur zijn. België heeft aan de Europees vastgelegde sectoren transport en energie ook de financiële sector en de telecommunicatie toegevoegd.

De wet bepaalt tevens een mechanisme met een sectoriële overheid voor elk van die vier sectoren. Het gaat daarbij telkens om een entiteit die expertise heeft in het domein en die de kritieke punten in kaart brengt, de operatoren identificeert, een risicoanalyse uitvoert, een veiligheidsplan laat opstellen en dat plan laat auditeren.

Het Centrum wil datzelfde mechanisme in het domein van de cyberveiligheid toepassen voor een aantal andere sectoren, zoals de overheid. Er werd dus nagegaan of binnen dat domein een entiteit te vinden is die bijvoorbeeld de identificatie van de belangrijkste kritieke punten van de overheid — en niet enkel federaal — in kaart kan brengen, om vervolgens de operatoren te identificeren, een risicoanalyse uit te voeren, enz. Fedict heeft zich geëngageerd om die rol op zich te nemen. Het gaat om een voorlopig engagement dat in het nog goed te keuren plan zal worden opgenomen.

Op basis van de zo goed als goedgekeurde Europese NIS-richtlijn (*Network Information Security*) zal bijvoorbeeld ook de sector van het drinkbaar water worden toegevoegd.

b. ***Entreprises***

L'accent est mis ailleurs pour les entreprises. Par le biais de la plate-forme *Cyber Security Coalition Belgium*, de nombreuses entreprises en Belgique ont été questionnées sur leurs besoins: qu'attendent-elles des autorités belges en matière de cybersécurité? Il ressort de cette enquête que ces entreprises ont des difficultés à déterminer les mesures de sécurité qu'elles doivent prendre dans leurs propres murs. Elles sont, en d'autres termes, demandeuses d'un cadre standard de directives, de bonnes pratiques et d'avis qui leur permettraient de mettre en œuvre la cybersécurité.

Il va sans dire que des partenariats seront conclus avec les entreprises, ce qui permettra une coopération en matière de cybersécurité. De même, là où c'est possible, des technologies sûres seront mises à disposition.

c. ***Secteurs vitaux***

La loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques dispose qu'il y a, en Belgique, quatre secteurs d'infrastructures critiques. La Belgique a ajouté le secteur financier et les télécommunications aux secteurs des transports et de l'énergie retenus par l'Europe.

La loi fixe également un mécanisme avec une autorité sectorielle pour chacun des quatre secteurs. Il s'agit chaque fois d'une entité qui dispose d'une expertise dans le domaine et qui cartographie les points critiques, identifie les opérateurs, exécute une analyse de risques, fait établir un plan de sécurité et fait soumettre ce plan à un audit.

Le Centre veut appliquer ce même mécanisme du domaine de la cybersécurité dans une série d'autres secteurs, tels que le secteur public. On a dès lors examiné s'il existe, dans ce domaine, une entité en mesure, par exemple, de faire l'inventaire des principaux points critiques du secteur public – et pas seulement fédéral –, afin d'identifier ensuite les opérateurs, de réaliser une analyse du risque, etc. Le Fedict s'est engagé à assumer ce rôle. Il s'agit d'un engagement provisoire qui sera repris dans le plan qui reste encore à adopter.

Sur la base de la directive européenne relative à la sécurité des réseaux et des informations (NIS, *Network Information Security*), qui est pour ainsi dire adoptée, le secteur de l'eau potable, par exemple, sera également ajouté.

Voor de vitale sectoren wil het Centrum echter nog een stap verder gaan. Zo zal er bijvoorbeeld voor gezorgd worden dat er een nationale technische ploeg beschikbaar is die bij een belangrijke crisis op een vitaal punt in België — en met een belangrijke impact op het functioneren van België — in staat is tussen te komen aan de hand van een op voorhand vastgelegd noodplan en volgens welomschreven procedures. Het spreekt voor zich dat die ploeg essentieel zal werken binnen het domein van de vitale sectoren of bij specifieke crisissen, en dus niet ten behoeve van de mensen thuis.

Naast deze *incident response*, die gericht is op de vitale sectoren, wordt nog een andere stap gezet: binnen het domein van de preventie zal ervoor gezorgd worden dat de inkomende informatie over dreigingen op een efficiënte manier terechtkomt bij de betrokken doelgroepen binnen de vitale sectoren. De bedoeling is te komen tot een systeem van *early warning*. Dat systeem wordt momenteel verfijnd op basis van de analyse van de behoeften en de actuele capaciteiten, en moet ervoor zorgen dat in het geval van een dreiging — bijvoorbeeld ten aanzien van de energiesector — de informatie onmiddellijk, efficiënt en op een gepaste wijze terechtkomt bij die punten die op dat ogenblik de nodige maatregelen kunnen nemen om te zorgen voor een bijkomende bescherming.

Naast de ondersteuning met richtlijnen en adviezen onderzoekt het Centrum momenteel de ontwikkeling van normen. Dat betekent dat wordt nagegaan of het mogelijk is om globaal of per sector een basis- of minimumnorm (*base line*) te bepalen waaraan de vitale sectoren moeten voldoen.

De heer De Bruycker geeft aan veeleer voorzichtig om te gaan met normering, audit en accreditatie, en persoonlijk meer gewonnen te zijn voor de piste van de responsabilisering. Dat zou kunnen betekenen dat ervoor gekozen wordt om weliswaar een basisnorm op te leggen, maar toch de hoofdverantwoordelijkheid bij de sectoren zelf te laten. Dat zal nog verder worden onderzocht met het oog op een concreet voorstel.

5. ***Pijlers van een cyberveiligheidsbeleid***

a. *Expertise*

Naast de drie hierboven geschetste doelgroepen, wijst de spreker er voorts op dat ook het deeldomein "*at school*" werd gedefinieerd.

Eén van de kritieke punten bij het uitbouwen van een capaciteit rond cyberveiligheid is de technische expertise. Welk beleid men ook vooropstelt, steeds is het noodzakelijk dat het steunt op de beschikbaarheid

Le Centre veut toutefois encore aller plus loin en ce qui concerne les secteurs vitaux. On veillera par exemple à la disponibilité d'une équipe technique nationale qui sera à même d'intervenir selon un plan d'urgence fixé préalablement et selon des procédures bien définies, en cas de crise majeure sur un point vital en Belgique ayant un impact considérable sur le fonctionnement du pays. Il va de soi que cette équipe travaillera essentiellement dans le domaine des secteurs vitaux ou dans le cadre de crises spécifiques, et non pour les particuliers à domicile.

Outre cette *incident response*, qui est axée sur les secteurs vitaux, une autre mesure est encore prévue: dans le domaine de la prévention on veillera à ce que les informations entrantes parviennent efficacement aux groupes cibles dans les secteurs vitaux. Le but est d'arriver à un système d'*early warning*. Ce système est actuellement affiné sur la base de l'analyse des besoins et des capacités actuelles, et doit assurer que, dans le cas d'une menace – par exemple envers le secteur de l'énergie – l'information parvienne immédiatement, efficacement et de manière adéquate aux points qui à ce moment-là sont en mesure de prendre les mesures nécessaires afin de fournir une protection supplémentaire.

Outre le soutien sur la base de directives et d'avis, le Centre examine actuellement le développement de normes. Cela signifie qu'il vérifie s'il est possible de définir, de manière globale ou par secteur, une norme minimale ou de base (*base line*) à laquelle doivent satisfaire les secteurs vitaux.

M. De Bruycker estime qu'il convient d'être prudent avec les normes, les audits et les accréditations et est personnellement plus favorable à la piste de la responsabilisation. On pourrait décider d'imposer une norme de base tout en laissant la responsabilité première aux secteurs. Cette piste sera examinée plus avant en vue de la formulation d'une proposition concrète.

5. ***Piliers d'une politique de cybersécurité***

a. *Expertise*

Outre les trois groupes-cibles esquissés ci-dessus, l'orateur souligne que le sous-domaine "*at school*" a également été défini.

Lors de l'élaboration d'une capacité en matière de cybersécurité, l'un des points critiques est l'expertise technique. Quelle que soit la politique préconisée, il est toujours nécessaire qu'elle repose sur la disponibilité

van deskundigen met de gepaste kennis. Daaruit volgt dat het Centrum de scholen zal stimuleren om jongeren ertoe aan te zetten kennis te verwerven rond cyberveiligheid. Tegelijk zal het in samenwerking met de universiteiten en de hogescholen streven naar de ontwikkeling van opleidingen tot bachelor of master binnen dat expertisegebied. Bijzondere aandacht zal daarbij gaan naar de "*quick wins*" in de vorm van de gespecialiseerde opleidingen. Dat komt erop neer dat mensen die reeds een ICT-opleiding achter de rug hebben over het beheer en de beveiliging van netwerken een bijkomende specifieke opleiding kunnen volgen. Daarnaast zal ook het Centrum zelf de eigen capaciteiten verder oefenen en eventueel evalueren aan de hand van de reeds bestaande internationale trainingen.

Dat betekent ook dat binnen de overheid de mogelijkheid tot het bestaan van aangepaste statuten moet worden bekeken. De overheid dient er immers voor te zorgen dat zij in staat is deskundige personen aan te trekken en gedurende een nuttige periode in dienst te houden.

b. *Situational awareness*

Een tweede belangrijke pijler, naast de deskundigheid, is de zogenaamde "*situational awareness*". Dat komt erop neer dat het van belang is om een algemeen beeld te krijgen van enerzijds de cyberdreiging, en anderzijds van het huidige niveau van veiligheid en kwetsbaarheid van de vitale punten in België.

Indien men een gepast niveau van cyberveiligheid wil bereiken, is het essentieel de dreiging op een correcte wijze in kaart te brengen. Dat moet vermijden om een te hoge veiligheidgraad in te bouwen, wat ertoe zou leiden dat enerzijds de flexibiliteit van de systemen te veel wordt ingeperkt en dat anderzijds middelen worden verspild. Indien de risico's te laag worden ingeschat, bestaat de kans dat zich incidenten zullen voordoen waar men niet op voorbereid is en waarvoor onvoldoende capaciteit beschikbaar is.

Het is dus van kapitaal belang om een duidelijk beeld te krijgen van de actuele dreigingsituatie en van de actoren en hun intenties, alsook van de kwetsbaarheid van de systemen.

c. *Efficiënte informatie-uitwisseling*

Een derde pijler is een efficiënte informatie-uitwisseling. De ervaring leert immers dat bij de meeste incidenten heel wat informatie wel ergens — meestal in het buitenland — beschikbaar was en die er had kunnen voor zorgen dat de anomalieën vroeger gedetecteerd werden.

d'experts disposant des connaissances adéquates. Il en découle que le Centre stimulera les écoles à inciter les jeunes à acquérir des connaissances en matière de cybersécurité. En même temps, il s'emploiera, en coopération avec les universités et les hautes écoles, à développer des formations bachelor ou master dans ce domaine d'expertise. À cet égard, une attention particulière sera accordée aux "*quick wins*" sous la forme de formations spécialisées. Autrement dit, les personnes qui ont déjà suivi une formation ICT pourront suivre une formation spécialisée supplémentaire en gestion et en sécurisation des réseaux. Par ailleurs, le Centre lui-même continuera à exercer ses propres capacités et les évaluera éventuellement sur la base des formations internationales existantes.

Cela implique que la possibilité de l'existence de statuts adaptés doit également être examinée au sein de l'autorité. Celle-ci doit en effet veiller à être en mesure d'attirer des personnes expertes et de les garder en service pendant une période utile.

b. *Situational awareness*

Outre l'expertise, un deuxième pilier important concerne la *situational awareness*. Cela revient à dire qu'il importe d'avoir une image générale de la cybermenace, d'une part, et du niveau actuel de sécurité et de vulnérabilité des points vitaux en Belgique, d'autre part.

Si l'on tient à atteindre un niveau approprié de cybersécurité, il est essentiel d'identifier correctement la menace. Cela doit éviter de prévoir un niveau de sécurité trop élevé, pouvant conduire à ce que, d'une part, la flexibilité des systèmes soit trop limitée et, d'autre part, des moyens soient gaspillés. Si les risques sont sous-évalués, des incidents auxquels on n'est pas préparé et pour lesquels la capacité disponible est insuffisante peuvent survenir.

Il est donc crucial d'avoir une idée précise de la situation actuelle de la menace et des acteurs et de leurs intentions, ainsi que de la vulnérabilité des systèmes.

c. *Échange d'informations efficient*

Un troisième pilier a trait à un échange d'informations efficient. L'expérience apprend que lors de la plupart des incidents, de nombreuses informations étaient disponibles quelque part – généralement à l'étranger – et auraient pu permettre de détecter plus tôt les anomalies.

Die vaststelling leidt ertoe dat gezorgd zal worden voor een informatieportaal voor de burgers en de bedrijven (*awareness*) met duidelijke richtlijnen, en voor een beveiligd netwerk voor de vitale sectoren waarop de meer gevoelige informatie ter beschikking wordt gesteld.

6. ***Aanpak***

Zoals eerder aangeduid heeft het Centrum vooral een coördinerende rol. Dat houdt in dat optimaal gebruik zal worden gemaakt van de bestaande middelen en diensten (CERT.be, de federale politie, Justitie, Defensie, Veiligheid van de Staat, enz.).

Er zullen dus partnerschappen en coalities tot stand worden gebracht met de publieke, de private en de academische sector. Ook de internationale samenwerking zal van groot belang zijn. Het Centrum heeft er in dat verband voor gekozen om tijdens zijn opstartfase (de eerste zes maanden) te focussen op de Benelux en Frankrijk. Er werden inmiddels al contacten gelegd met de buurlanden. Uit dat overleg zijn al concrete afspraken voortgekomen die verder uitgewerkt zullen worden.

Daarnaast is het zo dat het Centrum kiest voor een stapsgewijze implementatie, en dus niet voor een "*big bang*". Het gaat immers ook om een kleine entiteit met 10 personen. Ter vergelijking, het Nederlandse NCSC (*Nationaal Cyber Security Centrum*), dat de taken van het CCB en CERT.be uitoefent, telt 88 personeelsleden, waarvan 53 voor het luik beleid (vergelijkbaar met het CCB), en 35 voor het meer technische luik (vergelijkbaar met het CERT.be).

Het is niet de bedoeling om in België de capaciteit op een zelfde wijze te centraliseren, maar wel om meer gebruik te maken van de bestaande capaciteiten en te zorgen voor een gelijkaardig en evenwaardig effect aan de hand van de optimalisatie van de samenwerking. Uit de voorbije jaren is reeds gebleken dat in België zeer goed wordt samengewerkt tussen de verschillende diensten op het ogenblik dat zich een incident voordoet.

7. ***Timing***

Er is een opstartfase voorzien van zes maanden. Dat betekent concreet dat in maart 2016 wordt overgegaan naar de "*build-up*" fase van drie jaar. Tijdens deze periode zullen de verschillende capaciteiten worden uitgebouwd in functie van de projecten die thans worden gedefinieerd. Over drie jaar zullen de verschillende capaciteiten en middelen dus beschikbaar zijn, waarna wordt overgegaan naar de laatste fase binnen het mandaat van vijf jaar, en dat is de maturiteitsfase. Tijdens die

Partant de cette constatation, on veillera à créer un portail d'information pour les citoyens et les entreprises (*awareness*), avec des consignes claires, ainsi qu'un réseau sécurisé pour les secteurs vitaux où les informations plus sensibles pourront être consultées.

6. ***Méthode***

Comme indiqué précédemment, le Centre a surtout un rôle de coordinateur, ce qui signifie notamment qu'il sera fait un usage optimal des moyens et des services existants (CERT.be, police fédérale, Justice, Sûreté de l'État, etc.).

Des partenariats et des synergies seront donc mis en place avec le secteur public, le secteur privé et les universités. La coopération internationale revêtira également une grande importance. À cet égard, le Centre a choisi de se focaliser, au cours de la phase de démarrage (les six premiers mois) sur le Benelux et la France. Entre-temps, des contacts ont déjà été pris avec les pays voisins. Cette concertation a déjà permis de dégager des accords concrets dont les modalités seront davantage précisées.

Par ailleurs, le Centre a choisi de déployer ses activités par étapes et n'a donc pas opté pour le *"big bang"*. Il s'agit d'ailleurs d'une petite entité composée de 10 personnes. À titre de comparaison, aux Pays-Bas, le personnel du NCSC (*Nationaal Cyber Security Centrum*), qui remplit les missions du CCB et de CERT.be, compte 88 membres, dont 53 sont affectés au volet politique (mission comparable à celle du CCB) et 34 au volet technique (mission comparable à celle de CERT.be).

L'idée n'est pas, en Belgique, de centraliser les capacités de la même manière, mais plutôt d'utiliser davantage les capacités existantes et de veiller à avoir un impact similaire et équivalent en optimisant la collaboration. Ces dernières années, on a déjà pu constater que l'on était capable, en Belgique, de faire en sorte que les différents services coopèrent efficacement lorsqu'un incident se produit.

7. ***Timing***

Une phase de démarrage de six mois a été prévue. Concrètement, cela signifie que le passage à la phase "*build-up*" qui durera trois ans aura lieu en mars 2016. Au cours de cette période, les différentes capacités seront développées en fonction des projets qui sont actuellement définis. Par conséquent, d'ici trois ans, les différentes capacités et moyens seront disponibles, après quoi, pendant le mandat de cinq ans, on passera à la dernière phase, qui est la phase de maturité. Au cours

fase zullen de capaciteiten ten volle worden gebruikt, en tegelijk ook geëvalueerd, met een eventueel voorstel tot bijsturing aan het einde van het mandaat.

Tijdens de eerste zes maanden was de hoofdbekommernis de aanwerving van het personeel en de verhuis naar de nieuwe kantoren. Er werd ook gewerkt aan de overname van het beheer van het CERT.be, en aan het beheer van enkele platformen (bv. het coördinatiecomité).

Intussen werden ook alle betrokken diensten geconsulteerd. Het is immers de bedoeling om niet op een onbezonnen wijze de projecten op te starten, maar om te vertrekken op basis van een duidelijke kennis over het actuele landschap (situatie "*as is*"). Op basis daarvan kunnen de doelstellingen worden bepaald (situatie "*to be*") na drie jaar. Daarna kunnen de projecten zeer gericht worden opgestart.

Zoals reeds gesteld, zal op internationaal niveau aanvankelijk worden samengewerkt met de Benelux en Frankrijk. Tegelijk is er ook ondersteuning vanwege ENISA (*European Union Agency for Network and Information Security*), met hoofdzetel in Griekenland, dat heel wat expertise en analysecapaciteit heeft op het vlak van de oprichting van nationale capaciteit rond cyberveiligheid en certificatie. Het Europese agentschap heeft het CCB al uitvoerig bijgestaan bij de oprichting en de uitwerking van de strategie van het Centrum.

Een andere belangrijke prioriteit tijdens de opstartfase was het uitschrijven van een noodplan voor de cyberveiligheid. Het is immers de bedoeling dat er een basisplan klaarligt op het ogenblik dat zich een incident voordoet. Dat plan is momenteel bijna klaar, en wordt in samenwerking met de betrokken diensten verder verfijnd. In maart of april 2016 zal het klaar zijn. Medio maart zal het alvast worden geëvalueerd in het kader van een *crisis management exercise* van de NAVO die op dat ogenblik plaatsvindt. Dan zal de procedure dus een eerste keer worden getest in het Crisiscentrum aan de hand van een *table top exercise*. Daarbij zal het scenario worden overlopen om te zien waar zich eventueel nog problemen voordoen, en zullen de platformen voor informatiedeling worden geïdentificeerd.

8. ***Rekrutering***

De directeur en de adjunct-directeur werden inmiddels bij koninklijk besluit aangewezen. Sedert oktober 2015 telt het Centrum ook een communicatieattaché, en dat in het kader van een jongerenbanenplan. Begin

de celle-ci, les capacités seront pleinement utilisées et elles feront simultanément l'objet d'une évaluation, puis , éventuellement, d'une proposition d'adaptation à la fin du mandat.

Au cours des six premiers mois, les principaux soucis furent le recrutement du personnel et le déménagement dans les nouveaux bureaux. Il a également été travaillé à la reprise de la gestion de la CERT.be et à la gestion de quelques plateformes (par ex. le comité de coordination).

Entre-temps, tous les services concernés ont également été consultés, l'objectif étant de ne pas démarrer les projets de manière inconsidérée mais de s'appuyer sur une connaissance claire du paysage actuel (situation "telle qu'elle est") qui pourra servir de base pour définir les objectifs après trois ans (situation "telle qu'elle sera"). Les projets pourront ensuite être lancés de manière très ciblée.

Ainsi qu'il a déjà été précisé, au cours de la phase initiale, une collaboration avec le Benelux et la France sera mise en place au niveau international. Un soutien sera également apporté simultanément par l'ENISA (*European Union Agency for Network and Information Security*), dont le siège principal se trouve en Grèce et qui possède une très grande expertise et une capacité d'analyse en matière de développement de capacité nationale en matière de cybersécurité et de certification. Lors de la création et de la mise au point de la stratégie du Centre, cette Agence européenne a déjà amplement assisté le CCB.

Une autre priorité importante durant la phase de lancement a consisté en l'élaboration d'un plan d'urgence pour la cybersécurité. L'objectif est en effet de disposer d'un plan de base au moment où un incident se produit. Ce plan est aujourd'hui pratiquement prêt, on continue à l'affiner en collaboration avec les services concernés. Il sera fin prêt en mars ou avril 2016. À la mi-mars, il fera en tout état de cause l'objet d'une évaluation dans le cadre d'un *crisis management exercise* de l'OTAN prévu à ce moment-là. La procédure sera donc ainsi testée une première fois dans le Centre de crise à l'occasion d'un *table top exercise.* On y passera en revue le scénario afin de voir où des problèmes se posent encore éventuellement, et les plates-formes de partage de l'information seront identifiées.

8. ***Recrutement***

Le directeur et le directeur-adjoint ont dans l'intervalle été désignés par arrêté royal. Depuis octobre 2015, le Centre compte également un attaché chargé de la communication et ce, dans le cadre d'un plan

februari 2016 is ook een jurist aan de slag gegaan, alsook de eerste project manager. Begin maart starten de tweede project manager en de eerste eGov-expert met een expertise in cyberveiligheid.

De procedures voor de office managers zijn lopende, en moeten ten laatste in mei of juni 2016 tot resultaten leiden. Het Centrum is ook nog op zoek naar een tweede eGov-expert met een expertise rond *policies* en richtlijnen.

Begin maart zijn dus zeven van de tien voorziene personeelsleden aan de slag, en in mei-juni zal het Centrum voltallig zijn.

9. ***Quick wins***

De heer De Bruycker wijst tot slot op enkele *quick wins*. Zo was er begin september 2015 een specifieke dreiging. Na analyse daarvan bleek dat aanvallen die het normaal functioneren van hoofdzakelijk websites ("*distributed denial of service attacks*") in gevaar brengen de voornaamste dreiging vormden. Aan CERT.be werd bijgevolg gevraagd een technisch verslag op te stellen over de te nemen proactieve en reactieve maatregelen. Begin oktober 2015 werd dat verslag gepubliceerd en verspreid onder de overheidsdiensten en de operatoren van de vitale sectoren ("*DDoS — Proactive and Reactive measures*", https://www.cert.be/files/DDoS-proactive-reactive.pdf).

In samenwerking met de *Cyber Security Coalition Belgium* (een coalitie van ongeveer 40 entiteiten uit de publieke, de private en de academische sector) werd ook een gids uitgebracht over hoe een onderneming zich kan voorbereiden en reageren op incidenten. De gids is reeds beschikbaar in het Engels, en binnenkort zal ook een versie in het Nederlands en in het Frans klaar zijn.

II. — **VRAGEN EN OPMERKINGEN VAN DE LEDEN**

De heer Philippe Pivin (MR) merkt op dat cybercriminaliteit een verontrustend verschijnsel is dat de komende jaren dreigt uit te dijen. In die context vormt het CCB — waarvan moet worden erkend dat het een bescheiden omvang heeft — een kostbaar instrument dat inzake coördinatie en internationale samenwerking een rol zal moeten spelen. Die internationale samenwerking neemt een belangrijke plaats in, gelet op de aard van de dreigingen. Kan de heer De Bruycker in enkele woorden zeggen wat er op het gebied van cybersecurity in het buitenland bestaat?

d'embauche des jeunes. Début février 2016, un juriste ainsi que le premier *project manager* ont commencé à y travailler. Début mars, ce sera au tour du deuxième *project manager* et du premier *eGov-expert* ayant une expertise dans la cybersécurité.

Les procédures de recrutement des *office managers* sont en cours et doivent aboutir au plus tard en mai ou juin 2016. Le Centre est également encore à la recherche d'un deuxième *eGov-expert* ayant une expertise en *policies* et directives.

Début mars, ce sont donc sept des dix membres du personnel prévus qui sont au travail, et le cadre du Centre sera complet en mai-juin.

9. ***Quick wins***

M. De Bruycker évoque enfin quelques *quick wins*. Ainsi, il y a eu une menace spécifique au début du mois de septembre 2015. Il s'est avéré après analyse que les attaques compromettant essentiellement le fonctionnement normal de sites internet ("*distributed denial of service attacks*") constituaient la principale menace. CERT.be a en conséquence été invité à rédiger un rapport technique sur les mesures proactives et réactives à prendre. Ce rapport a été publié et distribué aux services publics et aux opérateurs des secteurs vitaux au début du mois d'octobre 2015 ("*DDoS – Proactive and Reactive measures*", https://www.cert.be/files/DDoS-proactive-reactive.pdf).

Par ailleurs, un guide expliquant comment une entreprise peut se préparer et réagir à des incidents a également été publié en collaboration avec la *Cyber Security Coalition Belgium* (qui regroupe environ 40 entités des secteurs public et privé et du monde universitaire). Ce guide est déjà disponible en anglais et il le sera prochainement en français et en néerlandais.

II. — **QUESTIONS ET OBSERVATIONS DES MEMBRES**

M. Philippe Pivin (MR) observe que la cybercriminalité est un phénomène inquiétant qui risque de prendre de l'ampleur dans les années à venir. Dans ce cadre, le CCB dont il faut reconnaître que la taille est modeste constitue un outil précieux appelé à jouer un rôle en matière de coordination et de coopération internationale. Celle-ci revêt une dimension importante compte de la nature des menaces. M. De Bruycker peut-il dire quelques mots sur ce qui existe à l'étranger dans le domaine de la cybersécurité?

Uit de uiteenzetting van de heer De Bruycker blijkt dat het CCB zich op drie doelgroepen richt: de particulieren, de wereld van het werk en bepaalde vitale sectoren. Wat zijn die vitale sectoren? Maakt de banksector er deel van uit?

De heer Eric Thiébaut (PS) herinnert eraan dat al lang op de start van het CCB werd gewacht. Het door de heer De Bruycker meegedeelde tijdschema toont aan dat er nog veel werk voor de boeg blijft.

Hoe verhouden het CCB en het Cert zich? Zullen de werkzaamheden van laatstgenoemde worden overgenomen door het CCB? Of stevenen beide instanties veeleer af op meer samenwerking? Is voorts samenwerking gepland met Defensie, dat onlangs een twintigtal specialisten in digitale defensie in dienst heeft genomen, of met de politie-eenheid ter bestrijding van de cybercriminaliteit?

Tijdens zijn uiteenzetting heeft de directeur van het CCB ook een publiek-private samenwerking ter sprake gebracht. Kan hij daarover meer precieze informatie geven? Is men, gelet op de geringe omvang van het CCB, van plan belangrijke taken aan de privésector toe te vertrouwen?

De heer Roel Deseyn (CD&V) stelt verheugd vast dat het Centrum eindelijk van start kan gaan. Hij is al tien jaar vragende partij voor de oprichting van een dergelijk orgaan. Het gaat om een zeer belangrijke en ambitieuze opdracht, die met een team met een beperkte omvang vervuld moet worden. Bovendien gaat het deels om omkaderend personeel.

Is het, gelet op de hoge specialisatiegraad van deze opdracht, sowieso mogelijk om het nodige personeel te vinden aan de hand van de klassieke Selor-rekruteringsmethode? Ook binnen andere entiteiten (bv. Fedict) heeft men op het vlak van de rekrutering al enige creativiteit aan de dag moeten leggen. Hetzelfde geldt voor het aantrekken van bepaalde internationale profielen. Ziet de heer De Bruycker bepaalde wettelijke beperkingen die een vlotte rekrutering belemmeren? Wat zou voor hem het optimale personeelskader zijn, indien er geen budgettaire beperkingen waren?

De heer Deseyn is ook tevreden dat de certificering van de apparatuur één van de ambities is. Het gaat dan concreet om apparatuur waarin software is geïntegreerd die het mogelijk maakt bepaalde informatie weg te schrijven. Men moet vaststellen dat ten aanzien van dergelijke praktijken in het bedrijfsleven enige naïviteit heerst. Met welke onafhankelijke deskundigen zal hierover worden samengewerkt, niet enkel ten behoeve van de overheid maar ook voor het bedrijfsleven?

De l'exposé de M. De Bruycker, il ressort que le CCB s'adresse à trois publics cibles: les particuliers, le monde du travail et certains secteurs vitaux. Quels sont ces secteurs vitaux? Le secteur bancaire en fait-il partie?

M. Eric Thiébaut (PS) rappelle que la mise en route du CCB était attendue de longue date. Le calendrier communiqué par M. De Bruycker démontre qu'il reste beaucoup à faire.

Qu'en est-il des relations du CCB avec le Cert? Les activités de ce dernier seront-elles reprises par le CCB? Ou s'oriente-t-on plutôt vers une collaboration renforcée? Des collaborations sont-elles par ailleurs prévues avec la Défense nationale qui a récemment embauché une vingtaine de spécialistes en défense numérique ou encore avec l'unité policière de lutte contre la cybercriminalité?

Au cours de son exposé, le directeur du CCB a également évoqué un partenariat public – privé. Peut-il donner quelques précisions à ce sujet? Compte tenu de la taille modeste du CCB, envisage-t-on de confier des missions importantes au secteur privé?

M. Roel Deseyn (CD&V) se réjouit de constater que le Centre peut enfin entamer ses activités. Cela fait déjà dix ans que l'intervenant demande la création d'un tel organe. La mission capitale et ambitieuse qui lui est confiée devra être réalisée par une équipe aux effectifs réduits, dont certains membres relèvent en outre du personnel d'encadrement.

L'intervenant se demande du reste si la méthode classique de recrutement par le Selor est bien adaptée en l'espèce pour trouver le personnel nécessaire, eu égard au degré élevé de spécialisation requis pour cette mission. D'autres entités (comme Fedict) ont déjà dû faire preuve de créativité au niveau du recrutement de personnel. Il en va de même pour l'engagement de certains profils internationaux. M. De Bruycker estime-t-il que le recrutement risque d'être ralenti par certaines limitations légales? Quel serait à ses yeux le cadre organique idéal s'il n'y avait pas de restrictions budgétaires?

M. Deseyn se réjouit également que la certification du matériel fasse partie des objectifs. Il s'agit en l'espèce du matériel dans lequel sont intégrés des logiciels qui permettent d'effacer certaines informations. L'intervenant constate que les entreprises font preuve d'une certaine naïveté à l'égard de ce type de pratiques. Avec quels experts indépendants une collaboration sera-t-elle mise en place en la matière, non seulement au bénéfice des pouvoirs publics, mais aussi des entreprises?

De heer Deseyn wijst vervolgens op het belang van de afstemming van de regelgeving. Er werd gewezen op de vitale sectoren die in België zijn aangewezen. Er dient voor die sectoren nog heel wat uitvoerende regelgeving te worden uitgevaardigd. De spreker nodigt het CCB uit om het Parlement in te lichten wanneer het dergelijk hiaten vaststelt in de regelgeving.

In dat verband kan worden gewezen op de telecomwetgeving, waarin bepaald wordt dat de providers op het vlak van veiligheid een zekere verantwoordelijkheid hebben bij het aanbieden van hardware- en softwarepakketten. Het is goed dat het CCB daaromtrent bepaalde minimumstandaarden zal opleggen. Dat is vandaag de dag meer dan nodig, gelet op het vrij zwakke veiligheidsniveau dat heel wat websites kenmerkt. Er is met andere woorden heel wat roekeloos rijgedrag merkbaar op de huidige internetsnelweg. Hoe zal de samenwerking met de Privacycommissie verlopen in verband met deze opdracht?

Binnen de vitale sectoren geldt doorgaans ook een meldplicht. Het is voor de exploitanten echter vaak niet eenvoudig om na te gaan aan wie of wat gemeld moet worden. Ook op dat punt is dus een belangrijke coördinatietaak weggelegd voor het CCB. Daarnaast is er nog heel wat werk aan de winkel rond de uitbouw van een meldingsplicht voor de burger. Het is van essentieel belang dat er voor de burger een laagdrempelig aanspreekpunt komt.

De heer De Bruycker heeft gesproken over de overname van het beheer van het CERT. Gaat het dan om een verdwijn- of overnamescenario voor de organisatie?

Op internationaal niveau zet het CCB aanvankelijk in op overleg met de buurlanden. De heer Deseyn wenst er in dat verband op te wijzen dat ook de OVSE over een bijzondere expertise beschikt op het vlak van de cyberveiligheid. Zal vanuit het CCB input worden geboden aan de verschillende administratieve en technische werkgroepen van de OVSE?

De heer De Bruycker heeft eerder al gecommuniceerd over het internetrijbewijs binnen de cluster "*at school*". Dat houdt onder meer in dat er een minimale basisvorming moet zijn rond cyberveiligheid, aangezien de "*awareness*" van jongeren daarover vaak niet voldoende is. In hoeverre zal het CCB de bevoegdheid rond de structuren overstijgen, en ook verantwoordelijkheid opnemen over het gedrag rond content? In het Parlement werd recent ook gedebatteerd over het te grabbel gooien van bepaalde gegevens in het kader van de procedure rond overheidsopdrachten. Zal het

M. Deseyn souligne ensuite qu'il est capital d'harmoniser la réglementation. L'accent a déjà été mis ci-avant sur les secteurs vitaux identifiés en Belgique. De nombreuses dispositions d'exécution doivent encore être édictées pour ces secteurs. L'intervenant invite le CCB à informer le Parlement lorsqu'il constatera de telles lacunes dans la réglementation.

On peut renvoyer à cet égard à la législation relative aux télécommunications, en vertu de laquelle les fournisseurs assument une certaine responsabilité en matière de sécurité lorsqu'ils proposent des paquets de *hardware* et de logiciels. L'intervenant se félicite que le CCB ait l'intention d'imposer certaines normes minimales en la matière, ce qui est absolument indispensable au jour d'aujourd'hui, eu égard au niveau de sécurité relativement bas qui caractérise beaucoup de sites internet. En d'autres termes, les chauffards sont aujourd'hui très nombreux sur les autoroutes de l'internet. Comment la collaboration avec la Commission de la protection de la vie privée se déroulera-t-elle dans le cadre de cette mission?

Une obligation de signalement est en général également imposée au sein des secteurs vitaux. Mais il est souvent difficile pour les exploitants d'identifier ce qui doit être signalé, et à qui. Sur ce point également, le CCB pourrait jouer un rôle de coordination important. Par ailleurs, il y a encore beaucoup à faire au niveau du développement d'une obligation de signalement dans le chef du citoyen. Il est essentiel de mettre en place un point de contact aisément accessible pour les citoyens.

M. De Bruycker a évoqué la reprise de la gestion du CERT. L'organisation va-t-elle disparaître ou s'agira-t-il d'une reprise?

Au niveau international, le CCB mise avant tout sur la concertation avec les pays voisins. M. Deseyn souligne à cet égard que le l'OSCE dispose, elle aussi, d'une expertise particulière dans le domaine de la cybersécurité. Le CCB fournira-t-il une contribution aux différents groupes de travail administratifs et techniques de l'OSCE?

M. De Bruycker avait déjà communiqué au sujet du "permis de surfer" dans le cluster "*at school*". Cette initiative insiste notamment sur la nécessité de mettre en place une formation de base minimale en matière de cybersécurité, étant donné que les jeunes ne sont pas suffisamment conscients de l'importance de cet aspect. Dans quelle mesure le CCB dépassera-t-il la compétence relative aux structures et assumera-t-il aussi des responsabilités à l'égard du comportement en matière de contenu? Le Parlement a récemment aussi débattu sur le fait de jeter certaines données en pâture dans le

CCB naast de sensibilisering ook mee ondersteuning bieden aan een contentbeleid?

Zal het CCB aandacht schenken aan de situatie van de digitale klokkenluiders, gelet op de relatieve onveiligheid van de huidige systemen? Binnen een degelijk beleid van "*responsible disclosure*" is er bijvoorbeeld nood aan een voorafgaande toestemming om de veiligheid van een bepaald systeem te testen. Nederland heeft in dat verband een aantal goede praktijken, zoals de organisatie van "*hackatons*". Dergelijke praktijken steunen op de visie dat iemand die te goeder trouw veiligheidsproblemen signaleert een maatschappelijke verantwoordelijkheid op zich neemt. Op welke termijn acht de heer De Bruycker het bestaan van een onthaalinfrastructuur voor dergelijke meldingen haalbaar in België? Binnen een kennismaatschappij is de bescherming van de knowhow immers van het allergrootste belang.

De heer De Bruycker heeft in zijn inleiding een aantal partners van het CCB vermeld: CERT.be, de federale politie, Justitie, Defensie, Veiligheid van de Staat, enz. Werd reeds met alle partners overleg gepleegd, of moeten sommige contacten nog worden gelegd?

De heer Jean-Marc Nollet (Ecolo-Groen) verwijst naar de zopas door NTI bekendgemaakte nucleaireveiligheidsindex en stipt aan dat de Belgische nucleaire installaties bijzonder zwak scoren op het vlak van cyberveiligheid: ons land deelt de laatste plaats immers met Kazachstan.

Het is duidelijk dat ons land niet klaar is om een cyberaanval op onze nucleaire installaties te weren. Die vaststelling is des te zorgwekkender omdat een dergelijke aanval op een nucleaire site dramatische gevolgen kan hebben. De toegangscontrolesystemen kunnen worden gekraakt, de productie van niet-toegelaten nucleair materiaal kan veel schade berokkenen, de boekhoudkundige systemen kunnen worden gemanipuleerd en de koelsystemen van de reactoren kunnen met opzet onklaar worden gemaakt. De spreker geeft dan ook uiting aan zijn verwondering over de manier waarop de resultaten van dat rapport werden geminimaliseerd, terwijl men ze net als een alarmsignaal hadden moeten opvatten. Hij wenst dan ook te weten of de nucleaire sector wel degelijk een kwetsbare sector is zoals de heer De Bruycker heeft aangegeven. Voorts vraagt hij hoe het CCB denkt lering uit dat rapport te zullen trekken. Beschikt België over een urgentieplan in geval van een cyberaanval?

cadre de la procédure relative aux marchés publics. En plus de ses actions de sensibilisation, le CCB soutiendra-t-il aussi une politique du contenu?

Le CCB accordera-t-il de l'attention à la situation des lanceurs d'alerte dans le secteur numérique, compte tenu de l'insécurité relative des systèmes actuels? Dans le cadre d'une telle politique de divulgation responsable, il est par exemple nécessaire de mette en place un système d'autorisation préalable pour tester la sécurité d'un système donné. Les Pays-Bas disposent à cet égard d'une série de bonnes pratiques, comme l'organisation de "*hackatons*". Ces pratiques se fondent sur l'idée qu'une personne qui signale de bonne foi des problèmes de sécurité assume une responsabilité sociale. À quelle échéance M. De Bruycker estime-t-il qu'une infrastructure d'accueil pour ce type de signalements serait réalisable en Belgique? Dans une société de la connaissance, la protection du savoir-faire est en effet capitale.

M. De Bruycker a mentionné dans son exposé un certain nombre de partenaires du CCB: CERT.be, la police fédérale, la Justice, la Défense, la Sûreté de l'État, etc. Une concertation a-t-elle déjà été organisée avec tous les partenaires, ou certains contacts doivent-ils encore être pris?

M. Jean-Marc Nollet (Ecolo-Groen) se réfère à l'index de sécurité nucléaire que vient de publier NTI et qui pointe du doigt la faiblesse absolue des installations nucléaires belges en matière de cybersécurité. La Belgique arrive en effet en fin de classement, au même niveau que le Kazachstan.

Manifestement, notre pays n'est pas prêt à faire face à une cyberattaque de ses installations nucléaires. Ce constat est d'autant plus préoccupant eu égard aux conséquences potentiellement catastrophiques d'une telle attaque contre un site nucléaire. Les systèmes de contrôle d'accès peuvent être "crackés", la fabrication de matériaux nucléaires non autorisée peut causer de nombreux dégâts; les systèmes comptables peuvent être manipulés, les systèmes de refroidissement des réacteurs peuvent être délibérément estropiés. L'intervenant se dit dès lors surpris de la manière dont les résultats de ce rapport ont été minimisés alors qu'il aurait du servir de signaux d'alarme. Il demande dès lors si le secteur nucléaire est bien un des secteurs vulnérables évoqués par M. De Bruycker et comment le CCB compte-t-il tirer les leçons de ce rapport. La Belgique possède-t-elle un plan d'urgence en cas de cyberattaque?

De heer Alain Top (sp.a) hoopt dat met de opstart van het CCB het thema van de cyberveiligheid voortaan de aandacht zal krijgen die het verdient, en dat zowel ten behoeve van de overheid en de bedrijven als van de burgers.

Het internet is in oorsprong een militair netwerk waarbinnen de gebruikers elkaar vertrouwden. Misschien verklaart die oorsprong de nonchalance in verband met de veiligheid van het internet. Men moet bijvoorbeeld vaststellen dat iemand vrij snel persoonlijke gegevens prijsgeeft op het internet. De opdracht die op het CCB rust om binnen die problematiek voor verandering te zorgen is dan ook enorm. Kan het CCB het verschil maken met een ploeg van 10 werknemers? Zal het orgaan meer kunnen doen dan brandjes blussen in geval van incidenten? Zal het CCB de taak rond sensibilisering en samenwerking met de partners naar behoren kunnen vervullen? Op welke taken zal het tijdens de komende maanden en jaren de nadruk leggen?

Tijdens de voorbije jaren werd een aanzienlijke lijst met veiligheidsincidenten opgebouwd, en dat zowel bij de ondernemingen als bij de overheid. Op welke wijze zal het Centrum de bedrijven en de overheid begeleiden naar een betere beveiliging van hun websites?

In een aantal gevallen is het zelfs zo dat bepaalde gevoelige informatie (bv. op sommige overheidswebsites) gewoon raadpleegbaar is. Zal het Centrum ook meewerken rond het bepalen van de regels rond content? Zo ja, met wie zal het Centrum samenwerken?

Hoe ziet de heer De Bruycker de omgang met de te goeder trouw handelende elektronische klokkenluiders? Hoe ziet hij de uitbouw van een portaal voor veiligheidsmeldingen, met de nodige bescherming voor de melders?

De heer Top is overtuigd van het belang van sensibilisering rond cyberveiligheid ten aanzien van de overheid, de bedrijven en de burgers (bv. de schoolkinderen) op de langere termijn. Zal het Centrum die ambitie kunnen waarmaken in het licht van de beperkte middelen waarover het beschikt? Welke hefbomen denkt de heer De Bruycker te kunnen aanwenden opdat bijvoorbeeld de scholen er de nodige aandacht aan besteden?

De spreker wijst er tot slot op dat heel wat overheidsdiensten en bedrijven werken met verouderde hard- en software. De heer De Bruycker heeft verwezen naar de mogelijkheden rond certificering. Hoe kunnen dergelijke normen worden opgelegd? Is het mogelijk om een minimumnorm te bepalen waaraan een gebruiker

M. Alain Top (sp.a) espère que le lancement du CCB permettra désormais au thème de la cybersécurité de bénéficier de l'attention qu'il mérite, dans l'intérêt tant des autorités et des entreprises que des citoyens.

L'internet était, à la base, un réseau militaire, au sein duquel les utilisateurs se faisaient confiance. Peut-être que cette origine explique la nonchalance qui caractérise la sécurité relative à l'internet. L'on constate, par exemple, que les gens tendent à révéler plutôt rapidement leurs données personnelles sur internet. La mission assignée au CCB, qui est de faire évoluer la chose quant à cette problématique, est donc énorme. Le CCB peut-il faire la différence avec une équipe de dix travailleurs? L'organe pourra-t-il faire davantage qu'éteindre des feux de paille en cas d'incident? Le CCB pourra-t-il s'acquitter correctement de sa mission de sensibilisation et de collaboration avec les partenaires? Sur quelles tâches l'accent sera-t-il mis au cours des prochains mois et des prochaines années?

Ces dernières années, les incidents de sécurité se sont succédé, que ce soit dans les entreprises ou dans les pouvoirs publics. Comment le Centre encadrera-t-il les entreprises et les autorités pour mieux sécuriser leurs sites internet?

Dans un certain nombre de cas, certaines données sensibles (par exemple, sur certains sites des autorités) sont simplement consultables. Le Centre collaborera-t-il aussi à la fixation de règles en matière de contenu? Dans l'affirmative, avec qui?

Comment M. De Bruycker conçoit-il l'attitude à adopter vis-à-vis des lanceurs d'alertes électroniques qui agissent de bonne foi? Comment envisage-t-il l'élaboration d'un portail pour signaler les problèmes de sécurité, offrant la protection requise aux auteurs des signalements?

M. Top est convaincu de l'importance de la sensibilisation en matière de cybersécurité à l'égard des pouvoirs publics, des entreprises et des citoyens (par exemple, les écoliers) sur le long terme. Le Centre pourra-t-il concrétiser cette ambition, à la lumière des moyens limités qui lui sont alloués? Quels leviers M. De Bruycker pense-t-il pouvoir utiliser pour que les écoles, par exemple, y consacrent l'attention nécessaire?

L'intervenant souligne enfin que de nombreux services publics et entreprises utilisent du matériel et des logiciels obsolètes. M. De Bruycker a renvoyé aux possibilités liées à la certification. Comment de telles normes peuvent-elles être imposées? Est-il possible de définir une norme minimale à laquelle doit satisfaire un

moet voldoen alvorens hij mag worden verbonden met het internet? Zo ja, welke vormen van samenwerking (met private of publieke organisaties) zijn er nodig om dat mogelijk te maken?

De heer Georges Dallemagne (cdH) onderstreept dat het CCB een vrij bescheiden instantie is in vergelijking met de middelen waarover men beschikt in het buitenland of bij andere Belgische instellingen (bijvoorbeeld de ADIV of de Veiligheid van de Staat). Zal het, gelet op het beperkte aantal specialisten bij het CCB, niet bijzonder moeilijk zijn de acties van al die kenniscentra op elkaar af te stemmen?

Moet overigens niet worden overwogen de wettelijke grondslag van het CCB te versterken? Momenteel wordt het CCB immers geregeld bij een gewoon koninklijk besluit. Vallen dan ook geen moeilijkheden te vrezen, meer bepaald wanneer delicate en soms geclassificeerde informatie moet worden gedeeld? Het is nauwelijks voor te stellen dat de ADIV bijvoorbeeld zijn informatie zou delen.

De spreker legt uit dat heel wat deskundigen België verlaten omdat ze hier niet de middelen vinden om hun knowhow inzake cyberveiligheid te ontwikkelen. Moet een van de taken van het CCB er niet in bestaan een beleid uit te stippelen waarmee de openbare en private middelen kunnen worden gevonden om een dergelijke knowhow tot ontwikkeling te brengen?

Op het vlak van de cyberveiligheid is internationale samenwerking essentieel. Welke rol speelt het CCB op dat vlak? Is de strijd tegen het terrorisme een prioriteit en zal worden voorzien in specifieke knowhow inzake cyberveiligheid om de daders van aanslagen op te sporen of rekruteringsnetwerken te ontmantelen?

Een van de basistaken van het CCB is advies uit te brengen over de ontwikkeling van het wettelijk raamwerk. Gaat het daarbij bijvoorbeeld om de manier waarop cyberaanvallen moeten worden beantwoord, om de eventuele neutralisering van computers of bronnen van waaruit een onderneming of een strategische sector werd aangevallen, om de opheffing van de anonimiteit op het internet of om het wissen van gegevens?

Dienen tot de vitale sectoren ook niet de regeringskabinetten te worden gerekend, die immers al het doelwit van cyberaanvallen zijn geweest?

Ten slotte verwijst de spreker naar het in Kreta gehuisveste Agentschap van de Europese Unie voor netwerken informatiebeveiliging (ENISA), waar tot voor kort niemand van had gehoord. Is dat Agentschap, waarvan

utilisateur avant de pouvoir être connecté à Internet? Le cas échéant, quelles sont les formes de coopération (avec des organisations privées ou publiques) nécessaires à cet effet?

M. Georges Dallemagne (cdH) souligne que le CCB est un organe relativement modeste en comparaison des moyens déployés à l'étranger et de ceux mis en œuvre par d'autres institutions belges (par exemple le SGRS ou la Sûreté de l'État). Compte tenu du nombre réduit de spécialistes que compte le CCB, ne sera-t-il pas particulièrement difficile de coordonner l'action de tous ces lieux d'expertises?

Par ailleurs, ne devrait-on pas envisager de renforcer la base légale du CCB? A l'heure actuelle, en effet, le CCB est régi par un simple arrêté royal. Ne doit-on dès lors pas craindre que surviennent des difficultés notamment en cas de nécessité de partager des informations sensibles, parfois classifiées? On imagine mal, par exemple, le SGRS partager ses informations.

L'intervenant explique que de nombreux experts quittent la Belgique car ils n'y trouvent pas les moyens de développer leur expertise en matière de cybersécurité. L'un des rôles du CCB ne devrait-il pas être de déployer une politique permettant de trouver les moyens publics et privés nécessaires au développement d'une telle expertise?

Dans le domaine de la cybersécurité, la coopération internationale est essentielle. Quel rôle le CCB joue-t-il en la matière? La lutte contre le terrorisme est-elle une priorité et va-t-on déployer dans ce domaine une expertise particulière en matière de cybersécurité afin de rechercher les auteurs d'attentats ou de démanteler des filières de recrutement?

Une des missions de base du CCB est de rendre un avis sur le développement du cadre légal. Les domaines concernent-ils par exemple la manière de répondre à des cyberattaques et la neutralisation éventuelle d'ordinateurs ou de sources à l'origine d'une attaque à l'encontre d'une entreprise ou d'un secteur stratégique, à la levée de l'anonymat sur Internet ou encore à l'effacement des données?

Parmi les secteurs vitaux, ne devrait-on pas également inclure les départements gouvernementaux qui, faut-il le rappeler ont déjà été la cible de cyberattaques?

Enfin, l'intervenant évoque l'Agence européenne chargée de la sécurité des réseaux et de l'information (AESRI), basée en Crète dont jusqu'à récemment personne n'avait entendu parler. Cette Agence dont la

de wettelijke grondslag en de middelen onlangs werden versterkt, opgewassen tegen de huidige uitdagingen?

De heer Brecht Vermeulen (N-VA) stelt verheugd vast dat de huidige federale regering eindelijk werk heeft gemaakt van de opstart en de operationalisering van een Centrum voor Cyberveiligheid. De spreker heeft tijdens een bezoek aan de *The Hague Security Delta (HSD)* in Den Haag vastgesteld dat heel wat te leren valt van de Nederlandse aanpak. In dat netwerk zit een aantal private en publieke spelers samen en zorgt er aldus voor een kruisbestuiving. In België stelt men daarentegen op dit ogenblik een vrij versnipperd werkveld vast. Hoe zal het CCB in België de geïntegreerde samenwerking rond onderzoek en ontwikkeling bevorderen?

De eerste minister heeft op 24 november 2015 in antwoord op een parlementaire vraag gesteld dat het CCB ook de sectoren van de overheid en de volksgezondheid heeft aangeduid als kritieke infrastructuren (CRIV 54 COM 274, blz. 9). De recente hacking van patiëntengegevens toont aan dat die stellig meer dan terecht is. Welke stappen zal het Centrum zetten om de instellingen van volksgezondheid onder te brengen bij de kritieke infrastructuren, of om er minstens een verhoogde aandacht aan te schenken?

De eerste minister heeft tevens laten optekenen dat het Centrum samenwerkt met het Crisiscentrum voor de opstelling van een procedure voor het beheer van nationale cyberincidenten en —crisissen. Tevens zou werk worden gemaakt van een noodplan (CRIV 54 COM 317, blz. 7). Wat is de stand van zaken?

Ook heeft de eerste minister er al op gewezen dat het CCB gebruik zou kunnen maken van de enveloppe van 200 miljoen euro voor investeringen (CRIV 54 COM 159, blz. 14). Concreet zou het Centrum een budget van 7 miljoen euro ter beschikking krijgen voor projectinvesteringen. Om welke projecten gaat het en wat is de timing? Die investeringen zijn hoe dan ook noodzakelijk om de achterstand op het vlak van het beheer van de cyberveiligheid ten overstaan van de buurlanden in te halen.

Recent heeft professor Bart Preneel in een opiniestuk uiteengezet dat de Belgische informatiesystemen erg kwetsbaar zijn, en dat in de eerste plaats omdat de technologie uit het buitenland komt, en de producenten doelbewust voor zwakke updates van de systemen zouden zorgen. Hoe geloofwaardig is die stelling? Zal het CCB — eventueel in samenwerking met andere partners — initiatieven ontwikkelen om dat te onderzoeken?

base légale et les moyens ont récemment été renforcés est-elle à la hauteur des défis actuels?

M. Brecht Vermeulen (N-VA) se réjouit de constater que le gouvernement fédéral s'est enfin attelé au lancement et à l'opérationnalisation d'un Centre de Cybersécurité. Lors d'une visite au *The Hague Security Delta (HSD)* à La Haye, l'intervenant a constaté qu'il y a beaucoup à apprendre de l'approche néerlandaise. Ce réseau réunit un certain nombre d'acteurs publics et privés, ce qui permet d'échanger les expériences. En Belgique, force est par contre de constater un certain morcellement dans ce domaine. Comment le CCB favorisera-t-il, en Belgique, la coopération intégrée en matière de recherche et de développement?

En réponse à une question parlementaire, le premier ministre a indiqué, le 24 novembre 2015, que le CCB a également désigné les secteurs des pouvoirs publics et de la santé publique comme étant des infrastructures critiques (CRIV 54 COM 274, p. 9). Le piratage récent de données de patients montre que ce point de vue est parfaitement justifié. Quelles démarches le Centre entreprendra-t-il pour faire figurer les institutions de santé publique parmi les infrastructures critiques, ou du moins pour y accorder une attention accrue?

Le premier ministre a déclaré que le Centre collabore avec le Centre de crise en vue de l'élaboration d'une procédure de gestion des cyberincidents et cybercrises nationaux. On s'attèlerait également à l'élaboration d'un plan d'urgence (CRIV 54 COM 317, p. 7). Où en est-on?

Le premier ministre a également déjà souligné que le CCB pourrait utiliser une enveloppe de 200 millions d'euros destinée aux investissements (CRIV 54 COM 159, p. 14). Le Centre disposerait concrètement d'un budget de 7 millions d'euros pour les investissements dans des projets. De quels projets s'agit-il et quel est le calendrier prévu? Ces investissements sont de toute façon indispensables pour rattraper le retard pris en matière de gestion de la cybersécurité par rapport aux pays limitrophes.

Le professeur Bart Preneel a récemment expliqué, dans un article d'opinion, que les systèmes informatiques belges sont très vulnérables, et ce, essentiellement parce que technologie vient de l'étranger et que les producteurs veilleraient sciemment à proposer des mises à jour mineures des systèmes. À quel point ces propos sont-ils crédibles? Le CCB développera-t-il – éventuellement en collaboration avec d'autres partenaires - des initiatives afin d'analyser ce point?

De heer De Bruycker heeft eerder al gewezen op het nut van een internetdiploma of —rijbewijs. De enige opleiding in België in verband met cyberveiligheid wordt thans aangeboden door Howest (Hogeschool West-Vlaanderen) in Brugge.

De docenten binnen die opleiding hebben er op gewezen dat studenten informatica veelal leren programmeren op een snel uitvoerbare, maar tegelijk ook vrij onveilige manier. Zal het CCB via het platform *Cyber Security Coalition Belgium* in de toekomst zorgen voor de ruimere verspreiding van een dergelijke ICT-opleiding rond cyberveiligheid?

Er werd ook al gewezen op het feit dat nog veel gebruik gemaakt wordt van verouderde hard- en software. Dat is zeker het geval binnen de overheidsdiensten, waar toch vaak met gevoelige informatie wordt gewerkt. Hoe zal het Centrum de ICT-verantwoordelijken binnen de overheid sensibiliseren over het thema?

III. — **ANTWOORDEN**

De heer De Bruycker benadrukt dat hij akkoord gaat met heel wat stellingen van de leden.

Het klopt dat de uitbouw van een Centrum rond cyberveiligheid in België relatief laat komt. In heel wat landen is dat al veel eerder gebeurd. Tegelijk moet men vaststellen dat er ook landen zijn die nog niet op het punt staan waar België zich nu bevindt. Tevens moet men vaststellen dat er binnen de verschillende overheidsdiensten veel aandacht en goodwill is ten aanzien van het thema.

A. **Organisatie en coördinerende rol**

In vergelijking met enkele andere landen is de personeelscapaciteit van het Centrum inderdaad beperkt. In een aantal landen is die capaciteit hoger, maar doorgaans is dan ook het takenpakket ruimer. In Frankrijk rusten op het Centrum bijvoorbeeld ook taken rond cryptografie of de behandeling van geclassificeerde informatie. In België hoort die taak bij het Nationale Veiligheidsoverheid (NVO), met wie het CCB daarover samenwerkt. Het Centrum heeft dus een coördinerende rol, en moet dus niet beschikken over personeel dat inhoudelijke antwoorden moet bieden. Het moet wel de taken verdelen van de diensten die in het geval van een

M. De Bruycker a déjà relevé l'utilité d'un diplôme ou d'un permis pour surfer sur internet. La haute école Howest (*Hogeschool West-Vlaanderen*) à Bruges est actuellement la seule en Belgique à dispenser une formation en matière de cybersécurité.

Les enseignants de cette filière ont fait observer que les étudiants en informatique apprennent généralement à programmer de manière rapide, mais aussi relativement peu sûre. Le CCB veillera-t-il à l'avenir, via la plateforme *Cyber Security Coalition Belgium*, à élargir la diffusion d'une telle formation ICT en matière de cybersécurité?

Il a également déjà été indiqué que l'on utilise encore beaucoup de matériel et de logiciel obsolète. Il en est certainement ainsi au sein des services publics, qui traitent pourtant souvent des informations sensibles. Comment le Centre sensibilisera-t-il les responsables ICT au sein des autorités à ce thème?

III. — **RÉPONSES**

M. De Bruycker souligne qu'il souscrit à un grand nombre de déclarations des membres.

Il est exact que la mise en place d'un Centre de cybersécurité arrive assez tard en Belgique et que de nombreux pays s'y sont pris beaucoup plus tôt. D'autre part, force est de constater qu'il existe aussi des pays qui n'en sont pas encore au stade où la Belgique se trouve actuellement et que cette thématique suscite par ailleurs un grand intérêt et bénéficie de beaucoup de bonne volonté de la part des différentes instances officielles concernées.

A. **Organisation et rôle de coordination**

En comparaison avec plusieurs autres pays, les effectifs du Centre sont en effet limités. Dans un certain nombre de pays, les centres disposent d'une plus grande capacité, mais, en général, leurs missions sont aussi plus étendues. En France, par exemple, le Centre doit également assumer des missions en rapport avec la cryptographie ou le traitement d'informations classifiées. En Belgique, cette mission incombe à l'Autorité nationale de Sécurité (ANS), avec laquelle le CCB collabore dans ce domaine. Le Centre a donc un rôle de coordination, et ne doit dès lors pas disposer d'un personnel capable d'apporter des réponses sur

incident in actie moeten komen. Bovendien komen cybercrisissen die een 24/7 crisisbeheer vereisen slechts vrij zelden voor.

Het Centrum kan dus een beroep doen op honderden deskundigen die zijn tewerkgesteld in de organisaties met wie het samenwerkt.

Het CCB werkt bovendien zeer goed samen met zijn buitenlandse tegenhangers. Heel wat zaken zullen immers ook in samenwerking met de buitenlandse partners moeten worden ontwikkeld.

De spreker heeft reeds gewezen op de vier sectoren van kritieke infrastructuren in België (transport, energie, telecommunicatie en financiën). Voor wat betreft de financiële sector onderhoudt het Centrum als coördinator directe contacten met enerzijds de Nationale Bank van België als wettelijke sectoriële autoriteit, en anderzijds met Febelfin.

CERT.be heeft momenteel slechts een zevental personen in dienst. Om de verschillende taken en bevoegdheden naar behoren te kunnen uitvoeren, zou de organisatie op langere termijn echter moeten beschikken over enkele tientallen personeelsleden. Met slechts een handvol personen is het immers zeer moeilijk om op gepaste wijze als "*computer emergency response team*" op te treden bij incidenten binnen de verschillende kritieke infrastructuren.

Het CCB bepaalt ten aanzien van het CERT.be momenteel de prioriteiten en de opdrachten, en heeft samen met Belnet een beheersplan opgesteld, en dat in directe coördinatie met de verantwoordelijke van CERT.be. Het Centrum vergadert daarover wekelijks met CERT.be. Of die laatste ook in de toekomst onder de Belnet-structuur zal vallen, kan op dit ogenblik nog niet worden gezegd. Alle elementen liggen nog niet op tafel om daarover een voorstel te formuleren.

Het is geenszins de bedoeling om een krimpscenario uit te rollen voor het CERT.be. Integendeel, het zal een belangrijke pijler zijn bij het beheer van incidenten in de vitale sectoren. Op dat punt zal het CERT.be de komende tijd stapsgewijze moeten groeien.

België kent reeds geruime tijd een degelijk overleg tussen verschillende betrokken actoren (Defensie, Justitie, Veiligheid van de Staat, CERT.be, enz.), waarbij er steeds een bereidheid bestaat om essentiële informatie uit te wisselen. De heer De Bruycker zou thans graag die uitstekende samenwerking willen formaliseren. Totnogtoe is die goede wisselwerking gesteund op het

le fond. Il doit en revanche répartir les tâches entre les différents services qui doivent entrer en action lorsqu'un incident se produit. De plus, les crises en matière de cybersécurité nécessitent assez rarement une gestion de crise 24 heures sur 24 et 7 jours sur 7.

Le Centre peut donc faire appel à des centaines d'experts qui sont employés par des organisations avec lesquelles il collabore.

De plus, il y a une très bonne coopération entre le CCB et ses homologues étrangers. De nombreux projets devront en effet être développés en collaboration avec les partenaires étrangers.

L'orateur a déjà évoqué les quatre secteurs d'infrastructures critiques en Belgique (le transport, l'énergie, les télécommunications et les finances). En ce qui concerne le secteur financier, le Centre entretient, en tant que coordinateur, des contacts directs, d'une part, avec la Banque nationale de Belgique en tant qu'autorité sectorielle légale, et, d'autre part, avec Febelfin.

CERT.be n'emploie actuellement que sept personnes. Pour pouvoir exécuter correctement ses différentes tâches et compétences, l'organisation devrait cependant pouvoir disposer, à long terme, de quelques dizaines de membres du personnel. Avec seulement quelques personnes, il est en effet très difficile d'intervenir de manière appropriée en tant qu'équipe d'intervention d'urgence en sécurité informatique lors d'incidents au sein des différentes infrastructures critiques.

Le CCB fixe actuellement les priorités et les missions de CERT.be, et a établi un plan de gestion avec Belnet, en coordination directe avec le responsable de CERT.be. Le Centre se réunit chaque semaine avec CERT.be à ce sujet. Il est encore impossible de dire si cette organisation relèvera, à l'avenir, de la structure de Belnet. On ne dispose pas encore de tous les éléments permettant de formuler une proposition à ce sujet.

L'objectif n'est pas du tout d'imposer une cure d'amincissement à CERT.be. Au contraire, il constituera un pilier important dans la gestion d'incidents dans les secteurs vitaux. Sur ce point, CERT.be devra croître de manière progressive à l'avenir.

En Belgique, il existe depuis un certain temps déjà une bonne concertation entre plusieurs acteurs concernés (la Défense, la Justice, la Sûreté de l'État, CERT.be, etc.), qui sont toujours disposés à échanger les informations essentielles. M. De Bruycker aimerait maintenant formaliser cette excellente collaboration. Jusqu'à présent, cette interaction de qualité repose sur

feit dat de verantwoordelijken elkaar kennen, en is zij dus gebaseerd op goede persoonlijke verstandhoudingen. De formalisering van die goede samenwerking zou voor de nodige continuïteit zorgen en zelfs de informatie-uitwisseling nog verder kunnen stimuleren. Eén van de taken van het CCB is immers het zorgen voor platformen voor informatie-uitwisseling, en dat niet enkel tussen de inlichtingen- en veiligheidsdiensten, maar ook met de private sectoren.

Voor de heer De Bruycker zijn de ondernemingen enerzijds klanten van normen, richtlijnen en goede praktijken, en anderzijds partners. Het Centrum onderhoudt daartoe contacten met het VBO (Verbond van Belgische Ondernemingen), maar ook met andere organisaties.

B. ***Scope van de verantwoordelijkheid***

Bij de opstart van het Centrum gingen sommigen ervan uit dat het CCB een rol zou gaan spelen bij de aanpak van een aantal criminele activiteiten op het internet, zoals de aanpak van de verspreiding van illegale muziek- of beeldbestanden, de bestrijding van pedopornografie of het tegengaan van online IS-propaganda.

Het is dus bij aanvang zeer belangrijk gebleken om de opdracht van het Centrum goed te beschrijven en af te bakenen. Die opdracht is te zorgen voor de beveiliging van systemen en netwerken in België, en dat voor de vitale sectoren, de ondernemingen en de burger. Het Centrum zal dus bijvoorbeeld proberen in kaart te brengen hoeveel systemen in België nog werken op niet langer ondersteunde Windows-versies, en op basis daarvan een plan van aanpak ontwikkelen.

In verkeerstermen uitgedrukt wil het CCB op de internetsnelweg zorgen voor veilige wegen, voor veilige auto's en voor een rijbewijs. Gelet op het open karakter van het internet is het echter moeilijk om bepaalde veiligheidsmaatregelen te eisen van de gebruikers. Wel is het mogelijk te sensibiliseren en te waarschuwen.

Het Centrum zal dus niet bepaalde criminaliteitsfenomenen op het internet gaan bestrijden. Dat belet echter niet dat wordt samengewerkt met organisaties zoals Child Focus. Zo wordt momenteel met Child Focus samengewerkt rond een bewustmakingscampagne over internetgebruik die gericht is op kinderen.

le fait que les responsables se connaissent, et donc, sur de bons rapports personnels. La formalisation de cette bonne coopération permettrait d'assurer la continuité nécessaire et pourrait même stimuler encore plus les échanges d'informations. L'une des tâches du CCB est en effet de prévoir des plates-formes d'échanges d'informations, et ce, non seulement entre les services de renseignement et de sécurité, mais aussi avec les secteurs privés.

Pour M. De Bruycker, les entreprises sont, d'une part, des clients des normes, directives et bonnes pratiques, et, d'autre part, des partenaires. Le Centre entretient, à cet effet, des contacts avec la FEB (Fédération des entreprises de Belgique), mais aussi avec d'autres organisations.

B. ***Portée de la responsabilité***

Lors du lancement du Centre, d'aucuns sont partis du principe que le CCB jouerait un rôle dans la lutte contre différentes activités criminelles sur Internet, par exemple dans la lutte contre la diffusion de fichiers musicaux ou de fichiers images illégaux, la lutte contre la pédopornographie ou la lutte contre la propagande islamiste en ligne.

Dès le départ, il est donc apparu très important de définir correctement et de délimiter clairement la mission du Centre. Cette mission consiste à assurer la sécurisation des systèmes et des réseaux en Belgique, et ce, pour les secteurs vitaux, les entreprises et le citoyen. Par exemple, le Centre va donc essayer de répertorier le nombre de systèmes qui, en Belgique, tournent encore sur des versions Windows qui ne sont plus supportées et de développer un plan d'action sur cette base.

Pour exprimer les choses à l'aide du vocabulaire de la circulation routière, le CCB souhaite que, sur "l'autoroute de l'information" qu'est l'Internet, les chaussées et les véhicules soient sûrs et que le permis de conduire soit obligatoire. Compte tenu du caractère ouvert de l'Internet, il est toutefois difficile d'exiger des utilisateurs qu'ils prennent certaines mesures de sécurité. On peut néanmoins les sensibiliser et les mettre en garde.

Le Centre ne va donc pas s'attaquer à certaines formes de criminalité sur Internet. Mais cela ne l'empêchera pas de développer une collaboration avec des organisations comme Child Focus. Dans ce cadre, il collabore actuellement avec cette dernière à une campagne de sensibilisation sur l'utilisation de l'Internet à destination des enfants.

C. ***Personeel en rekrutering***

Vervolgens gaat de spreker in op de vragen rond het personeel en de rekrutering van het Centrum. Gelet op de coördinerende opdracht van het Centrum, is er geen nood aan vergaande technische capaciteiten. Wel is er een zekere basiskennis vereist om de coördinatie tussen de verschillende technische entiteiten te kunnen verzorgen. Daartoe dient men immers hun werking en specifieke bezorgdheden, uitdagingen en technologieën te begrijpen.

Wel is het zo dat de huidige aanwervingsprocedure van Selor niet optimaal is voor de zoektocht naar geschikte technische profielen. Een aanwerving voor de loonschaal A vereist bijvoorbeeld een universitair diploma. Meestal wordt dat niveau ook gelinkt aan de leidinggevende en meer "horizontale" functies. De technische of "verticale" profielen situeren zich veeleer onder het niveau B van "deskundige". De kans dat kandidaten met een technisch profiel, die dus meer in de diepte werken rond een bepaald probleem, met succes deelnemen aan proeven die gericht zijn op de horizontale profielen is dus veeleer klein. De aanwervingsprocedure van technische profielen voor de overheidsdiensten dient dus zeker te worden herbekeken.

D. ***Certificering van apparatuur***

In Frankrijk wordt in het kader van de certificering van apparatuur samengewerkt met geaccrediteerde agentschappen. Er worden zeer specifieke technische normen bepaald. In België zou een gelijkaardig model kunnen worden uitgewerkt, met een rol voor de accreditatie-instelling BELAC.

De heer De Bruycker pleit er evenwel voor om de problematiek van de certificering niet aan te pakken op het Belgische, maar op het Europese niveau. Men mag immers doorgaans vertrouwen hebben in de apparatuur die in de Europese Unie wordt gefabriceerd. Wanneer zich incidenten voordoen, heeft dat veeleer te maken met producten die van buiten de EU worden ingevoerd.

Bovendien leert de ervaring dat de problemen met de apparatuur vaak niet aanwezig zijn bij de fabricage van de producten, maar wel ontstaan in een latere fase, door middel van bijvoorbeeld een wijziging in de microcode. Het verdient dus aanbeveling om regelmatig (wekelijks, maandelijks) validatietesten uit te voeren op de apparatuur om na te gaan of er geen wijzigingen werden aangebracht na de initiële installatie. Indien dat het geval is, heeft enkel een certificatie in het begin weinig waarde.

C. ***Personnel et recrutement***

Ensuite, l'orateur répond aux questions relatives au personnel et au recrutement au sein du Centre. Eu égard à sa mission de coordination, le Centre n'a pas besoin de capacités techniques poussées. Certaines connaissances de base sont toutefois nécessaires pour assurer la coordination entre les différentes entités techniques. Pour ce faire, il faut en effet comprendre leur fonctionnement et les préoccupations, les défis et les technologies spécifiques qui sont les leurs.

Or, il est vrai que la procédure de recrutement actuelle du Selor n'est pas optimale pour rechercher des profils techniques adéquats. Un recrutement à l'échelle de traitement A requiert, par exemple, un diplôme universitaire. Ce niveau est en général associé aux fonctions dirigeantes et plus "horizontales". Les profils techniques ou "verticaux" se situent plutôt au niveau B, qui est celui des experts. Il est dès lors relativement peu probable que des candidats ayant un profil technique, qui travaillent en conséquence davantage en profondeur sur un problème donné, réussissent les épreuves s'adressant aux profils horizontaux. Il est donc certain que la procédure de recrutement des profils techniques pour les services publics doit être revue.

D. ***Certification de l'équipement***

Il existe en France une collaboration avec des agences accréditées dans le cadre de la certification de l'équipement. Des normes techniques très spécifiques sont fixées. Un modèle semblable, dans lequel l'organisme d'accréditation BELAC jouerait un rôle, pourrait être développé en Belgique

M. De Bruycker plaide toutefois pour que l'on ne s'attaque pas à la problématique de la certification au niveau belge mais bien au niveau européen. On peut en effet généralement se fier à l'équipement fabriqué dans l'Union européenne. Les incidents concernent plutôt des produits importés dans l'UE.

L'expérience enseigne en outre que, souvent, les problèmes rencontrés avec l'équipement ne sont pas présents lors de la fabrication des produits, mais apparaissent dans une phase ultérieure, par exemple à la suite d'une modification du microcode. Il est dès lors recommandé d'effectuer régulièrement (de manière hebdomadaire, mensuelle) des tests de validité sur l'équipement afin de contrôler si aucune modification n'a été apportée après l'installation initiale. Dans l'affirmative, la seule certification initiale a peu de valeur.

E. ***Privacycommissie***

De vzw DNS Belgium, die verantwoordelijk is voor onder meer de registratie van de domeinnamen met de extensie ".be", merkt in haar systemen op wanneer bepaalde webservers het slachtoffer worden van cyberaanvallen. Zij heeft daarom een mechanisme ontwikkeld om die aanvallen te melden aan de eigenaars van de betrokken sites.

Daarnaast zijn er momenteel ook lijsten beschikbaar met botnet geïnfecteerde systemen in België. Dat gaat hoofdzakelijk om private gebruikers, maar daar zijn ook ondernemingen bij. Er bestaat echter op dit ogenblik geen enkel mechanisme om de eigenaars van die systemen te waarschuwen. Dat punt zou de heer De Bruycker graag met de Privacycommissie bespreken. De identificatie van het slachtoffer is op dit ogenblik immers in strijd met de bescherming van zijn privacy. Het zou mogelijk moeten worden gemaakt om die slachtoffers in te lichten en te begeleiden naar een oplossing.

F. ***OVSE***

De heer De Bruycker geeft aan zelf deel te hebben uitgemaakt van de werkgroep die instaat voor de bouw van "*confidence building measures in cyber security*". De tweede set maatregelen werd inmiddels goedgekeurd, en momenteel wordt gewerkt aan een derde set.

Het gaat om zeer waardevolle internationale maatregelen.

G. ***Responsible disclosure***

De spreker acht het van groot belang dat een technisch expert met kennis van bepaalde kwetsbaarheden een aanspreekpunt heeft binnen de overheid om daarvan melding te doen. Dat kan momenteel al: zowel het CERT.be als het CBB nemen reeds akte van dergelijke meldingen, en ondernemen in de mate van het mogelijke actie. Zo werd recent nog een waarschuwing uitgestuurd over een kwetsbaarheid die was gemeld.

Er wordt evenwel geen officieel beleid rond gevoerd. Dat beleid zal worden uitgeschreven, en is één van de vier prioritaire opdrachten die aan de juristen van het Centrum werden toegekend. Het meldpunt zal dus worden geofficialiseerd, en de operatoren zullen worden aangezet om zelf een beleid rond "*responsible disclosure*" uit te werken.

Op de website van Proximus kan een dergelijke procedure reeds worden geraadpleegd. Het CCB wil er

E. ***Commission de protection de la vie privée***

L'ASBL DNS Belgium, qui est notamment chargée de l'enregistrement des noms de domaine portant l'extension ".be", remarque dans ses systèmes lorsque certains serveurs web sont victimes de cyberattaques. Elle a donc mis au point un mécanisme qui permet de signaler ces attaques aux propriétaires des sites concernés.

Par ailleurs, il existe aussi actuellement des listes de systèmes infectés par des *"botnets"* en Belgique. Il s'agit principalement d'utilisateurs privés, mais des entreprises figurent également sur ces lites. Pour l'instant, il n'existe toutefois pas le moindre mécanisme pour alerter les propriétaires de ces systèmes. M. De Bruycker aimerait évoquer ce problème avec la Commission de protection de la vie privée. En effet, pour l'heure, l'identification de la victime va à l'encontre de la protection de sa vie privée. Il faudrait faire en sorte qu'il soit possible d'informer les victimes et de les guider vers une solution.

F. ***OSCE***

M. De Bruycker indique qu'il a lui-même fait partie du groupe de travail chargé d'élaborer des "mesures de confiance" en matière de cybersécurité. Entre-temps, le deuxième train de mesures a été approuvé, et un troisième train est en cours d'élaboration.

Ces mesures internationales sont très précieuses.

G. ***Divulgation responsable***

L'orateur estime qu'il est très important qu'un expert technique ayant connaissance de certaines vulnérabilités dispose d'un point de contact au sein des pouvoirs publics afin de les signaler. C'est déjà possible actuellement: tant CERT.be que le CBB prennent déjà acte de tels signalements, et interviennent dans la mesure du possible. Ainsi, récemment encore, un avertissement a été envoyé en ce qui concerne une vulnérabilité qui avait été signalée.

Aucune politique officielle n'est cependant menée en la matière. Cette politique sera élaborée et est l'une des quatre missions prioritaires confiées aux juristes du Centre. Le point de contact sera donc officialisé, et les opérateurs seront incités à élaborer eux-mêmes une politique en matière de divulgation responsable.

Une procédure de ce type peut déjà être consultée sur le site internet de Proximus. Le CCB souhaite donc

dus voor zorgen dat de melder in contact komt met de operator. Het Centrum zal zorgen voor een raamwerk, waardoor bijvoorbeeld de andere operatoren worden ingelicht over de kwetsbaarheid. Het Centrum zal ook een *template* uitwerken dat ondernemingen kunnen gebruiken als basis voor hun beleid rond "*responsible disclosure*". In een dergelijk beleidsmodel — en dat is tevens het geval in het beleid van Proximus — zal tevens worden vermeld dat er in het geval van misbruik een klacht zal worden ingediend. Het is dus de bedoeling om te komen tot een samenwerking tussen de melder en de operator, en om te allen tijde een "*Far West*"-scenario te vermijden.

In verband met de problematiek van de klokkenluiders is immers enige voorzichtigheid geboden. Net zoals het in de fysieke wereld verboden is om uit eigen beweging de beveiliging van huizen te gaan testen, is het niet toegestaan om zomaar de veiligheid van informatienetwerken na te gaan. Men dient er zich dus voor te behoeden om een vrijgeleide te creëren om dat toch te doen. Enerzijds is het zeer moeilijk om die groep te identificeren: op grond van welke criteria gaat men die bevoegdheid toekennen? Anderzijds is er de vraag wat die groep met een dergelijke bevoegdheid zal aanvangen. Het risico bestaat dat een vergoeding zal worden gevraagd voor de verkregen informatie. Wat moeten de organisatie in kwestie en de overheid in dat geval doen?

De regelgeving is ook in die zin opgesteld dat systemen kunnen worden getest, op voorwaarde dat dat op een gecontroleerde wijze gebeurt. Die werkwijze van "*white head hackers*", die met toelating van een organisatie diens netwerk testen, bestaat dus.

H. ***Nucleaire index***

Het Centrum heeft kennis genomen van het verslag over de nucleaire index. Op het vlak van de cyberveiligheid heeft België niet goed gescoord, met een score van 0 op 4 voor cyberveiligheid. Er moet dus zeker actie worden ondernomen. Het FANC is zich daarvan bewust en zal de nodige specifieke beschermingsmaatregelen treffen in verband met de cyberveiligheid. Die specifieke maatregelen zijn er op dit ogenblik niet.

Het FANC beschikt echter reeds over een deskundige op het vlak van cyberveiligheid en die werkt momenteel aan de ontwikkeling van dergelijke regels.

I. ***Noodplan cyberveiligheid***

De noodplanning in verband met cyberveiligheid is geen eenvoudige oefening. Het noodplan bestaat in ieder geval. Daarin worden drie niveaus van ernst van incidenten onderscheiden, die gekoppeld zijn aan drie

faire en sorte que le divulgateur entre en contact avec l'opérateur. Le Centre assurera un encadrement, grâce auquel, par exemple, les autres opérateurs seront informés de la vulnérabilité. Le Centre élaborera aussi un *template* que les entreprises pourront utiliser comme base de leur politique en matière de divulgation responsable. Dans ce modèle de gestion – et c'est également le cas dans la politique de Proximus –, il sera également mentionné qu'une plainte sera déposée en cas d'abus. L'objectif est donc de parvenir à une coopération entre le divulgateur et l'opérateur, et de toujours éviter un scénario de *Far West*.

En ce qui concerne la problématique des lanceurs d'alerte, il convient en effet d'être prudent. Tout comme il est interdit, dans le monde physique, de tester de sa propre initiative la sécurisation des maisons, il n'est pas autorisé de contrôler spontanément la sécurité de réseaux informatiques. Il faut donc se garder de créer un sauf-conduit permettant de le faire malgré tout. D'une part, il est très difficile d'identifier ce groupe: sur la base de quels critères attribuera-t-on cette compétence? D'autre part, la question se pose de savoir ce que ce groupe fera d'une telle compétence. Le risque existe qu'une rémunération soit demandé pour les informations obtenues. Comment doivent alors réagir l'organisation concernée et les autorités?

La réglementation est aussi rédigée en ce sens que les systèmes peuvent être testés à condition que cela ait lieu de manière contrôlée. Ce procédé des "*white hat hackers*", qui testent le réseau d'une organisation avec son autorisation, existe donc.

H. ***Index de sécurité nucléaire***

Le Centre a pris connaissance du rapport sur l'index de sécurité nucléaire. Avec un score de 0 sur 4, la Belgique a obtenu de mauvais résultats en matière de cybersécurité. Il faut dès lors absolument agir. L'AFCN en est consciente et prendra les mesures de protection spécifiques nécessaires en matière de cybersécurité qui n'existent pas encore actuellement.

Toutefois, l'AFCN dispose déjà d'un expert en cybersécurité qui travaille actuellement à l'élaboration de ces mesures.

I. ***Plan d'urgence en matière de cybersécurité***

La planification d'urgence en matière de cybersécurité n'est pas un exercice facile. En tout cas, le plan d'urgence existe. Il distingue trois niveaux de gravité des incidents, et leur associe trois procédures d'évaluation:

evaluatieprocedures: hoe ernstiger het incident, hoe meer evaluaties er zullen gebeuren. In die processen is duidelijk opgenomen wie welke taken op zich zal nemen. In grote lijnen zal de respons in handen liggen van de politie en het CERT.be, waarbij het stellen van een eerste diagnose naar misdrijf en dader en het veiligstellen van de eventuele forensische gegevens een taak zal zijn van de politie. Die taak kadert ook volledig binnen het geheel van opdrachten die aan de politie is toegewezen.

De heer De Bruycker hoopt de noodplanning eind maart 2016 te kunnen afronden. Het Centrum heeft echter de taak van coördinator: het behalen van deadlines is dus afhankelijk van de inspanningen van andere organisaties. De samenwerking met de verschillende betrokken organisaties verloopt thans hoe dan ook zeer goed.

De rapporteur, *De voorzitter,*

Eric THIÉBAUT Brecht VERMEULEN

plus l'incident est grave, plus le nombre d'évaluations effectuées sera élevé. Pour ces procédures, la répartition des tâches est claire. Dans les grandes lignes, la police et la CERT.be seront chargées de la réponse. La police aura pour mission d'établir un premier diagnostic relatif à l'infraction et à l'auteur des faits ainsi que de préserver les éventuelles données de police scientifique. Cette mission s'inscrit également parfaitement dans le cadre des missions confiées à la police.

M. De Bruycker espère pouvoir achever la planification d'urgence pour la fin mars 2016. La mission du Centre est toutefois limitée à la coordination: le respect des délais dépendra par conséquent des efforts des autres organismes. Quoi qu'il en soit, la collaboration avec les différents organismes concernés est actuellement excellente.

Le rapporteur, *Le président,*

Eric THIÉBAUT Brecht VERMEULEN

Centrale drukkerij – Imprimerie centrale