DOC 55 **3862/002**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

12 avril 2024

PROJET DE LOI

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

Proposition de loi modifiant la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vue de soumettre les fournisseurs de services essentiels du service public qui dépendent des réseaux et des systèmes d'information à certaines exigences en matière de sécurité et de notification

Rapport

fait au nom de la commission
de l'Intérieur,
de la Sécurité, de la Migration et
des Matières administratives
par
M. **Daniel Senesael**

Sommaire Pages

Voir:

Doc 55 **3862/ (2023/2024)**:
001: Projet de loi.

Voir aussi:
003: Texte adopté par la commission.

Doc 55 **2401/ (2021/2022)**:
001: Proposition de loi de M. Freilich et consorts.

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

12 april 2024

WETSONTWERP

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

Wetsvoorstel tot wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, teneinde de aanbieders van essentiële diensten in de publieke sector die afhankelijk zijn van netwerk- en informatiesystemen te onderwerpen aan bepaalde eisen inzake beveiliging en meldingen

Verslag

namens de commissie
voor Binnenlandse Zaken,
Veiligheid, Migratie en
Bestuurszaken
uitgebracht door
de heer **Daniel Senesael**

Inhoud Blz.

Zie:

Doc 55 **3862/ (2023/2024)**:
001: Wetsontwerp.

Zie ook:
003: Tekst aangenomen door de commissie.

Doc 55 **2401/ (2021/2022)**:
001: Wetsvoorstel van de heer Freilich c.s.

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

A. — Titulaires / Vaste leden:

N-VA	Sigrid Goethals, Yngvild Ingels, Koen Metsu
Ecolo-Groen	Julie Chanson, Simon Moutquin, Eva Platteau
PS	Hervé Rigot, Daniel Senesael, Eric Thiébaut
VB	Ortwin Depoortere, Barbara Pas
MR	Philippe Pivin, Caroline Taquin
cd&v	Franky Demon
PVDA-PTB	Nabil Boukili
Open Vld	Tim Vandenput
Vooruit	Meryame Kitir

B. — Suppléants / Plaatsvervangers:

Christoph D'Haese, Tomas Roggeman, Darya Safai, Valerie Van Peel
Wouter De Vriendt, Claire Hugon, Sarah Schlitz, Stefaan Van Hecke
Khalil Aouasti, Hugues Bayet, André Flahaut, Ahmed Laaouej
Joris De Vriendt, Frank Troosters, Hans Verreyt
Denis Ducarme, Philippe Goffin, Florence Reuter
Jan Briers, Nahima Lanjri
Gaby Colebunders, Greet Daems
Egbert Lachaert, Marianne Verhaert
Ben Segers, Anja Vanrobaeys

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

Les Engagés	Vanessa Matz
INDEP	Emir Kir
ONAFH	Emir Kir

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
cd&v	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
Les Engagés	:	*Les Engagés*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de nummering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénière*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de sa réunion du 27 mars 2024.

I. — **PROCÉDURE**

Conformément à l'article 24, alinéa 3, du Règlement, la proposition de loi modifiant la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vue de soumettre les fournisseurs de services essentiels du service public qui dépendent des réseaux et des systèmes d'information à certaines exigences en matière de sécurité et de notification (DOC 55 2401/001) a été intégrée à la discussion du projet de loi à l'examen, à la demande de l'auteur principal.

Cette proposition de loi a été commentée par son auteur principal le 18 mai 2022. Au cours de cette même réunion, la commission a décidé, conformément à l'article 28, n° 1, du Règlement, de recueillir l'avis écrit du Centre pour la Cybersécurité Belgique, du procureur fédéral et du premier ministre. Ces avis ont été mis à la disposition des membres.

II. — **EXPOSÉS INTRODUCTIFS**

A. **Projet de loi DOC 3862/001**

Mme Annelies Verlinden, ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, est heureuse de présenter le projet de loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Ce projet de loi a été rédigé et coordonné par le Centre pour la Cybersécurité Belgique (CCB) et par les services du premier ministre. Ce dernier a invité la ministre à présenter le projet de loi aux membres de cette commission. Étant donné que ce projet de loi n'aborde que de manière limitée les compétences de la ministre, le directeur général du CCB est également présent en commission afin de répondre aux questions éventuelles. Il expliquera également les aspects plus techniques du projet de loi.

Les réseaux et systèmes d'information sont devenus des caractéristiques essentielles de notre vie quotidienne en raison de la transformation numérique rapide et de

DAMES EN HEREN,

Tijdens haar vergadering van 27 maart 2024 heeft uw commissie dit wetsontwerp besproken.

I. — **PROCEDURE**

Overeenkomstig artikel 24, derde lid, van het Reglement werd het wetsvoorstel tot wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, teneinde de aanbieders van essentiële diensten in de publieke sector die afhankelijk zijn van netwerk- en informatiesystemen te onderwerpen aan bepaalde eisen inzake beveiliging en meldingen (DOC 55 2401/001) op verzoek van de hoofdindiener bij de bespreking van het voorliggende wetsontwerp gevoegd.

Dat wetsvoorstel werd op 18 mei 2022 toegelicht door de hoofdindiener. Op diezelfde vergadering besloot de commissie om, overeenkomstig artikel 28.1 van het Reglement de schriftelijke adviezen in te winnen van het Centrum voor Cybersecurity België, de federaal procureur en de eerste minister. Deze adviezen werden ter beschikking gesteld van de leden.

II. — **INLEIDENDE UITEENZETTINGEN**

A. **Wetsontwerp DOC 3862/001**

Mevrouw Annelies Verlinden, minister van Binnenlandse Zaken, Institutionele Hervorming en Democratische Vernieuwing, stelt hierbij graag het wetsontwerp voor tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Dit wetsontwerp werd opgesteld en gecoördineerd door het Centrum voor Cybersecurity België (CCB) en de diensten van de eerste minister. De eerste minister vroeg aan de minister om dit wetsontwerp aan de leden van deze commissie voor te stellen. Aangezien dit wetsontwerp slechts beperkt raakt aan haar bevoegdheden is vandaag ook de directeur-generaal van het CCB aanwezig, om eventuele vragen mee te beantwoorden. Hij zal ook de meer technische aspecten van de wet toelichten.

Netwerk- en informatiesystemen hebben zich ontwikkeld tot een centraal kenmerk van het dagelijks leven door de digitale transformatie en de onderlinge verbondenheid

l'interconnexion de la société. En effet, de nombreuses activités sociétales ou économiques critiques dépendent du bon fonctionnement de ces réseaux et systèmes d'information.

Cette évolution a conduit à une expansion du paysage des cybermenaces et des cyberincidents. Le nombre, la taille, la complexité, la fréquence et les conséquences des cyberincidents ne cessent de croître, constituant une véritable menace pour la population, les entreprises et les autorités publiques.

De nos jours, un cyberincident est, en effet, susceptible de provoquer des perturbations opérationnelles graves dans des secteurs critiques et ainsi affecter des personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Une société de plus en plus numérique et le recours accru aux nouvelles technologies s'accompagne mondialement d'une recrudescence des cyberattaques mais également, comme de nombreux incidents récents nous l'ont encore démontré, d'une intensification de la gravité et du degré de ces attaques. Ces attaques sont menées par des criminels, des terroristes, des activistes ou des services militaires et de renseignement étrangers, en vue de nuire à l'intégrité, la disponibilité et la confidentialité des données utilisées par les systèmes d'information.

L'ensemble des citoyens, des entreprises et des pouvoirs publics doivent dès lors être conscients de l'importance de se protéger préventivement contre les cybermenaces et les cyberincidents.

Le projet de loi à l'examen vise à établir un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Il s'inscrit dans le cadre de la stratégie de cybersécurité 2.0 adoptée par le Conseil national de sécurité (CNS) en 2021. Cette stratégie définit l'approche et les objectifs nationaux visant à protéger les organisations d'intérêt vital contre les cybermenaces. Elle a pour ambition de faire de la Belgique l'un des pays les moins vulnérables d'Europe.

Le projet de loi prévoit la transposition de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, ci-après dénommée la "directive NIS2 ". Cette directive doit être transposée en droit belge au plus tard le 17 octobre 2024.

La directive NIS2 remplace la directive européenne (UE) 2016/1148 du Parlement européen et du Conseil

van de samenleving. Veel kritieke maatschappelijke of economische activiteiten zijn afhankelijk van de goede werking van netwerk- en informatiesystemen.

Die ontwikkeling heeft geleid tot een uitbreiding van het cyberdreigingslandschap en van cyberincidenten. Het aantal, de omvang, de complexiteit, de frequentie en de impact van cyberincidenten blijft toenemen en vormt een reële bedreiging voor de bevolking, de ondernemingen en de overheden.

Een cyberincident kan vandaag immers ernstige operationele verstoringen in kritieke sectoren teweegbrengen en natuurlijke of rechtspersonen treffen, met aanzienlijke materiële, lichamelijke of morele schade als gevolg.

De samenleving wordt alsmaar digitaler en er wordt vaker een beroep gedaan op nieuwe technologieën. Dat gaat wereldwijd gepaard met een toename van het aantal cyberaanvallen, die ook qua ernst en omvang driester worden, zoals veel recente voorvallen hebben aangetoond. Die aanvallen zijn het werk van criminelen, terroristen, activisten of buitenlandse militaire en inlichtingendiensten, die erop uit zijn de integriteit, beschikbaarheid en vertrouwelijkheid van de door de informatiesystemen gebruikte gegevens te schaden.

Alle burgers, ondernemingen en overheden moeten zich dan ook bewust zijn van het belang zich preventief te beschermen tegen cyberdreigingen en cyberincidenten.

Het voorliggend wetsontwerp heeft als doel om netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid te beschermen.

Dit wetsontwerp maakt deel uit van de cybersecuritystrategie 2.0 die in 2021 werd aangenomen door de Nationale Veiligheidsraad (NVR). Deze strategie beschrijft de nationale aanpak en de doelstellingen om organisaties van essentieel belang te beschermen tegen alle cyberdreigingen. De ambitie is om van België een van de minst kwetsbare landen in Europa te maken.

Het wetsontwerp voorziet in de omzetting van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, oftewel de "NIS2-richtlijn". Deze richtlijn dient uiterlijk op 17 oktober 2024 in Belgisch recht te worden omgezet.

De NIS2-richtlijn vervangt Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016

du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après dénommée la "directive NIS1".

Compte tenu des nombreuses modifications nécessaires, ce projet de loi vise à remplacer intégralement les dispositions prévues par la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, qui avait transposé la directive NIS1 en Belgique.

Le projet à l'examen est le résultat de nombreux mois de consultations avec les acteurs privés (les associations et fédérations d'entreprises) et les acteurs publics (l'administration fédérale et les entités fédérées), coordonné par le cabinet du premier ministre et le CCB. Le projet de loi a également fait l'objet d'une consultation publique au mois de décembre 2023. Les commentaires et suggestions formulés ont été pris en compte dans toute la mesure du possible lors de l'élaboration du projet de loi.

Conformément à la directive, le champ d'application du projet de loi – voir le titre 1er – est principalement déterminé par le service essentiel fourni par l'entité concernée et sa taille.

Les entités concernées sont celles fournissant au sein de l'Union européenne des services essentiels énumérés dans les "secteurs hautement critiques" de l'annexe I ou dans les "autres secteurs critiques" de l'annexe II du projet de loi et qui constituent au moins des entreprises de taille moyenne au sens de la recommandation 2003/361/CE.

Parmi ces services essentiels figurent notamment l'énergie, le transport, la santé, les infrastructures numériques, les services de technologies de l'information et de la communication, l'eau potable, les administrations publiques, le spatial, etc.

Le titre 2 du projet de loi définit les différentes missions de l'autorité nationale de cybersécurité, qui sera chargée de coordonner et de surveiller le respect de la loi. Cette mission sera confiée par le Roi au CCB. À cette fin, le projet de loi combine les missions existantes du CCB et celles prévues par la directive NIS2, en particulier en ce qui concerne la surveillance des entités.

Toutefois, le projet de loi confie également diverses missions aux autorités sectorielles, notamment en ce qui concerne l'identification complémentaire, la gestion des incidents ou la supervision. Cela permettra de s'assurer que les règles communes en matière de cybersécurité soient coordonnées au mieux.

houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, oftewel de "NIS1-richtlijn".

Gezien de vele vereiste wijzigingen beoogt dit wetsontwerp de bepalingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, waarmee de NIS1-richtlijn in België werd omgezet, volledig te vervangen.

Dit wetsontwerp is de vrucht van vele maanden overleg met de private actoren (ondernemingsverenigingen en -verbonden) en de overheid (federale overheid en deelstaten), dat werd gecoördineerd door het kabinet van de eerste minister en het CCB. Het wetsontwerp is ook het voorwerp geweest van een openbare raadpleging in december 2023. Bij het uitwerken van het wetsontwerp werd in de mate van het mogelijke rekening gehouden met de in dat raam geformuleerde opmerkingen en suggesties.

Overeenkomstig de richtlijn wordt het toepassingsgebied van het wetsontwerp – zie titel 1 – hoofdzakelijk bepaald door de essentiële dienst die wordt verleend door de betrokken entiteit en de omvang ervan.

De betrokken entiteiten zijn entiteiten die binnen de Europese Unie essentiële diensten verlenen die opgesomd staan bij de "zeer kritieke sectoren" van bijlage I of bij de "andere kritieke sectoren" van bijlage II en die minstens middelgrote ondernemingen vormen in de zin van Aanbeveling 2003/361/EG.

Onder die essentiële diensten vallen onder meer energie, vervoer, gezondheid, digitale infrastructuur, informatie- en communicatietechnologiediensten, drinkwater, overheidsbestuur, ruimtevaart enzovoort.

In titel 2 van het wetsontwerp worden de verschillende taken van de nationale cyberbeveiligingsautoriteit omschreven, die verantwoordelijk zal zijn voor de coördinatie van en het toezicht op de wet. Deze rol zal door de Koning worden toevertrouwd aan het CCB. Daartoe combineert het ontwerp de bestaande taken van het CCB met de aanvullingen waarin de NIS2-richtlijn voorziet, namelijk met betrekking tot het toezicht op entiteiten.

Het wetsontwerp voorziet echter ook in diverse taken voor eventuele sectorale overheden, met name op het gebied van aanvullende identificatie, het beheer van incidenten of het toezicht. Dit zal ervoor zorgen dat de gemeenschappelijke regels inzake cybersecurity zo goed mogelijk worden gecoördineerd.

Le Centre de crise national (NCCN), sera toujours étroitement impliqué dans l'identification des entités et la notification des incidents, en raison de ses fonctions en matière de gestion de crise.

Au niveau national et européen, le projet de loi prévoit une coopération renforcée pour permettre l'échange d'informations sur les cybermenaces et les cyberincidents, ainsi que la réalisation d'inspections coordonnées.

Le titre 3 du projet de loi définit les règles légales minimales en matière de mesures de sécurité et de gestion des risques auxquelles doivent se conformer les entités essentielles et importantes.

M. Miguel De Bruycker, directeur général du Centre pour la Cybersécurité Belgique (CCB), explique que, pour être conforme aux exigences de la loi en matière de la cybersécurité, ces mesures doivent être appropriées et proportionnées aux risques qui menacent la sécurité de leurs réseaux et systèmes d'information. Elles doivent également éliminer ou réduire les conséquences que de potentiels incidents pourraient avoir sur les destinataires de leurs services ainsi que sur d'autres services. Pour ce faire, il est tenu compte du degré d'exposition de l'entité aux risques, de sa taille, de la probabilité qu'un incident se produise et de la gravité si un incident se produit.

Pour faciliter la mise en œuvre pratique de ces mesures de cybersécurité, le CCB a déjà élaboré et mis gratuitement à la disposition des entités concernées un cadre de référence: le "*Cyberfundamentals*", comportant quatre niveaux différents. Ces "*Cyberfundamentals*" combinent les principales normes internationales en matière de cybersécurité et l'expérience acquise par le CCB lors d'incidents en tant que Centre national de réponse aux incidents de sécurité informatique (CSIRT).

Le CCB a également développé un outil d'analyse des risques permettant de déterminer le niveau le plus approprié à utiliser. Le projet de loi et l'arrêté d'exécution y afférent accordent aux entités essentielles et importantes qui décident d'utiliser le cadre de référence *Cyberfundamentals* ou la norme internationale ISO/IEC 27001 une présomption de conformité en ce qui concerne les mesures de cybersécurité.

Pour ce qui concerne les incidents, les entités soumises à la loi devront notifier les incidents ayant un impact significatif sur la fourniture de ses services dans les secteurs repris aux annexes au CSIRT national (CCB). La notification obligatoire se déroule en plusieurs phases. L'entité concernée fournit une alerte précoce sans retard

Het nationaal Crisiscentrum (NCCN) zal steeds nauw worden betrokken bij het identificeren van entiteiten en het melden van incidenten, gelet op diens taken in het kader van het beheer van crises.

Op nationaal en Europees niveau voorziet het wetsontwerp in een versterkte samenwerking om de uitwisseling van informatie over cyberdreigingen en cyberincidenten mogelijk te maken en ook om gecoördineerde inspecties uit te voeren.

In titel 3 van het wetsontwerp worden de wettelijke minimumregels op het gebied van beveiligingsmaatregelen en risicobeheer uiteengezet die essentiële en belangrijke entiteiten dienen te hanteren.

De heer Miguel De Bruycker, directeur-generaal van het Centrum voor Cybersecurity België (CCB), legt uit dat de maatregelen, om te stroken met de wettelijke vereisten inzake cyberbeveiliging, gepast moeten zijn en in verhouding moeten staan tot de risico's voor de veiligheid van de netwerk- en informatiesystemen. Ze moeten ook de eventuele gevolgen van potentiële incidenten voor de bestemmelingen van hun diensten en voor andere diensten uitsluiten of zoveel mogelijk beperken. Daartoe wordt rekening gehouden met de mate waarin een entiteit aan risico's is blootgesteld, alsook met de omvang van de entiteit, de waarschijnlijkheid van een incident en de ernst ervan.

Om de praktische implementatie van deze cyberbeveiligingsmaatregelen te vergemakkelijken, heeft het CCB reeds een referentiekader ontwikkeld en gratis beschikbaar gesteld aan de betrokken entiteiten: de "*Cyberfundamentals*" met vier verschillende niveaus. Deze *Cyberfundamentals* combineren de belangrijkste internationale cybersecuritynormen met de verworven ervaring bij incidenten door het CCB als het *National Computer Security Incident Response Team* (CSIRT).

Het CCB ontwikkelde eveneens een risicoanalyse-instrument om te bepalen welk te hanteren niveau het meest geschikt is. Het wetsontwerp en het bijbehorende uitvoeringsbesluit bieden essentiële en belangrijke entiteiten die besluiten om gebruik te maken van het referentiekader *Cyberfundamentals* of de internationale ISO/IEC 27001-norm, een vermoeden van conformiteit met betrekking tot cyberbeveiligingsmaatregelen.

Wat de incidenten betreft, zullen de aan de wet onderworpen entiteiten melding moeten maken van de incidenten met een significante weerslag op de levering van die diensten in de sectoren opgenomen in de bijlagen bij het nationale CSIRT (CCB). De verplichte melding gebeurt in meerdere fasen. De desbetreffende entiteit

injustifié et au plus tard dans les 24 heures après avoir eu connaissance de l'incident significatif.

Ensuite, l'entité soumet une notification d'incident sans retard injustifié et au plus tard dans les 72 heures après avoir eu connaissance de l'incident. L'entité fournit un rapport final dans un délai d'un mois à compter du traitement définitif de l'incident. Outre la notification obligatoire des incidents significatifs par les entités essentielles et importantes, il existe également la possibilité de notifications volontaires.

D'une part, il peut s'agir de la notification d'incidents non significatifs par des entités essentielles ou importantes et, d'autre part, de la notification d'incidents significatifs, de cybermenaces ou de quasi-incidents par des entités non soumises à la loi NIS2.

Le service d'inspection de l'autorité nationale de cybersécurité a pour mission d'effectuer des contrôles en vue de vérifier si les entités essentielles et importantes prennent les mesures adéquates en matière de gestion des risques de cybersécurité et de notification des incidents.

Les entités essentielles doivent, dans le cadre de la surveillance dont elles font l'objet, se soumettre régulièrement à une évaluation de la conformité. Les entités importantes peuvent également se soumettre à une évaluation régulière de la conformité, mais elles n'en ont pas l'obligation. Les entités importantes ne sont soumises qu'à un contrôle *a posteriori*.

L'évaluation régulière de la conformité peut prendre la forme d'une évaluation réalisée par un organisme d'évaluation de la conformité accrédité ou d'une inspection régulière effectuée par le service d'inspection. Le recours à des organismes d'évaluation de la conformité accrédités pour assurer l'évaluation régulière de la conformité permet de garantir un niveau élevé d'expertise et de maîtriser les coûts budgétaires des services d'inspection compétents. Les autorités fédérales auront la possibilité de charger l'Audit interne fédéral (FAI) de procéder à cette évaluation régulière de la conformité si nécessaire.

Pour les infrastructures critiques, la supervision sera réalisée de manière conjointe entre le CCB et les autorités sectorielles concernées. Le CCB pourrait également déléguer la supervision à une autorité sectorielle.

Les exploitants d'une infrastructure critique ou les futures entités critiques au sens de la directive UE 2022/2557 du 14 décembre 2022 sur la résilience

stuurt onverwijld een vroegtijdige waarschuwing uit, uiterlijk binnen 24 uur na kennis te hebben genomen van het significante incident.

Vervolgens meldt de entiteit het incident onverwijld en uiterlijk binnen 72 uur na kennis te hebben genomen van het incident. De entiteit bezorgt een eindverslag binnen één maand na de definitieve afhandeling van het incident. Naast de verplichte melding van de significante incidenten door de essentiële en belangrijke entiteiten is er de mogelijkheid tot vrijwillige melding.

Het kan enerzijds gaan om de melding van niet-significante incidenten door essentiële of belangrijke entiteiten en anderzijds om de melding van significante incidenten, cyberdreigingen of quasi-incidenten door entiteiten die niet aan de NIS2-wet zijn onderworpen.

Het is de taak van de inspectiedienst van de nationale cyberbeveiligingsautoriteit om controles uit te voeren om na te gaan of essentiële en belangrijke entiteiten de gepaste maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

Essentiële entiteiten moeten, als onderdeel van hun toezicht, zich regelmatig onderwerpen aan een conformiteitsbeoordeling. Belangrijke entiteiten kunnen zich ook onderwerpen aan een regelmatige conformiteitsbeoordeling, maar dit is voor hen niet verplicht. Belangrijke entiteiten zijn enkel onderworpen aan controle achteraf.

Een regelmatige conformiteitsbeoordeling kan de vorm aannemen van een beoordeling door een geaccrediteerde conformiteitsbeoordelingsinstantie of van een regelmatige inspectie door de inspectiedienst. Door gebruik te maken van geaccrediteerde conformiteitsbeoordelingsinstanties om een regelmatige beoordeling van de conformiteit te garanderen, kan een hoog niveau van deskundigheid worden gewaarborgd en kunnen de begrotingskosten voor de bevoegde inspectiediensten in de hand worden gehouden. De federale overheden zullen de mogelijkheid krijgen om deze regelmatige conformiteitsbeoordeling, indien nodig, te laten uitvoeren door de Federale Interne Audit (FIA).

Voor de kritieke infrastructuren zal het toezicht gezamenlijk worden uitgevoerd door het CCB en de betrokken sectorale overheden. Het CCB zou het toezicht ook kunnen delegeren aan een andere sectorale overheid.

De exploitanten van een kritieke infrastructuur in de betekenis van Richtlijn EU 2022/2557 van 14 december 2022 betreffende de weerbaarheid van kritieke

des entités critiques, “la directive CER”, seront d’ailleurs automatiquement identifiés comme des entités essentielles sous l’emprise de la présente loi.

Enfin, le projet de loi clarifie également les mesures administratives et les amendes que les autorités de contrôle compétentes peuvent prendre à l’égard des entités essentielles ou importantes, ainsi que la procédure qui doit les précéder. Parmi les mesures possibles figurent les avertissements, les recommandations, la surveillance, les instructions contraignantes, les inspections ciblées et *ad hoc*, les obligations de divulgation d’informations et les amendes administratives. Conformément à la directive, certaines mesures et amendes ne s’appliquent pas aux entités relevant du secteur des administrations publiques.

Afin de mettre en œuvre les dispositions de la loi, toutes les entités relevant de la loi devront s’enregistrer et fournir des informations précises sur leurs activités. Une campagne de communication sera menée pour informer le plus grand nombre d’organisations possible et une plateforme d’enregistrement sera mise à disposition.

L’objectif du projet de loi est non seulement d’accroître la résilience des réseaux et des systèmes d’information des entités les plus sensibles, mais aussi de faire figure d’exemple pour d’autres organisations et citoyens en vue de tendre à un niveau élevé de cybersécurité en Belgique.

B. **Proposition de loi DOC 2401/001**

M. Michael Freilich (N-VA) souligne que la proposition de loi vise à renforcer la sécurité nationale. Par l’intermédiaire de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique, la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d’information dans l’Union (ci-après la “directive NIS1”) a été transposée dans la législation nationale.

L’Union européenne (UE) a observé que l’ampleur, la fréquence et les conséquences des incidents de sécurité ne cessent de croître, ces incidents représentant une menace majeure pour le bon fonctionnement des réseaux et des systèmes d’information. Ces systèmes peuvent aussi devenir des cibles pour des actions intentionnelles malveillantes qui visent la détérioration ou l’interruption de leur fonctionnement. C’est pourquoi la directive NIS1 a défini à l’intention des opérateurs

entiteiten, de zogenaamde CER-richtlijn, zullen overigens op grond van deze wet automatisch als essentiële entiteiten worden geïdentificeerd.

Ten slotte verduidelijkt het wetsontwerp ook welke administratieve maatregelen en geldboetes de bevoegde toezichthoudende autoriteiten kunnen opleggen aan de essentiële of belangrijke entiteiten en welke procedure daaraan dient vooraf te gaan. Tot de mogelijke maatregelen behoren waarschuwingen, aanbevelingen, toezicht, bindende instructies, gerichte en ad-hocinspecties, bekendmakingsverplichtingen en administratieve geldboetes. Overeenkomstig de richtlijn zijn bepaalde maatregelen en geldboetes niet van toepassing op de entiteiten van de sector van de overheidsinstanties.

Om de bepalingen van de wet uit te voeren, moeten alle entiteiten die onder de wet vallen zich registreren en nauwkeurige informatie over hun activiteiten verstrekken. Er zal een communicatiecampagne worden gevoerd om zoveel mogelijk organisaties te informeren en er zal een registratieplatform ter beschikking worden gesteld.

Terwijl het doel van het wetsontwerp is om de weerbaarheid van netwerk- en informatiesystemen van de meest gevoelige entiteiten te verhogen, is het daarnaast ook bedoeld om een voorbeeld te stellen aan andere organisaties en burgers om een hoog niveau van cybersecurity in België na te streven.

B. **Wetsvoorstel DOC 2401/001**

De heer Michael Freilich (N-VA) stipt aan dat het wetsvoorstel de nationale veiligheid beoogt te verhogen. Aan de hand van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid werd Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS1-richtlijn) omgezet in nationale wetgeving.

De Europese Unie (EU) zag de omvang, de frequentie en de gevolgen van beveiligingsincidenten toenemen. Die incidenten vormen een grote bedreiging voor de goede werking van netwerk- en informatiesystemen. De systemen kunnen het doelwit worden van opzettelijke schadelijke acties, met de bedoeling de werking ervan te verstoren of te onderbreken. De NIS1-richtlijn stelde daarom bepaalde eisen inzake beveiliging en meldingen, van toepassing op aanbieders van essentiële diensten,

de services essentiels plusieurs exigences en matière de sécurité et de notification afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.

Ayant constaté que les autorités publiques ne figurent pas sur la liste des organisations et entités tenues de se conformer à la directive NIS1, l'intervenant a déposé la proposition de loi à l'examen, qui vise à faire entrer le secteur de l'administration publique dans le champ d'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Le CCB fait observer que les organisations d'intérêt vital (OIV) sont confrontées à des cybermenaces de plus en plus fortes et sophistiquées. Étant donné que les cyberattaques contre ces organisations peuvent avoir un impact significatif sur la société et sur la sécurité nationale, il est crucial de les soutenir dans leur protection de manière adéquate. En tant qu'autorité nationale chargée de la cybersécurité, le CCB reçoit toutes les informations pertinentes concernant les menaces. Il analyse les informations reçues et envoie des alertes. Ainsi, les OIV sont informées en permanence des menaces, vulnérabilités ou incidents pertinents en matière de cybersécurité. Pour lutter rapidement contre la cybercriminalité et les menaces à l'encontre des autorités, il convient d'investir dans l'identification rapide des menaces qui pèsent sur la population, l'économie ou les OIV.

Dans le cadre de la transposition de la directive NIS1, le CCB avait proposé dès 2019 d'inclure les autorités publiques dans la liste des OIV. Lors de l'audition sur les cyberattaques dirigées contre l'infrastructure IT de l'État, le procureur fédéral Frédéric Van Leeuw avait ainsi indiqué que la directive NIS1 devrait également s'appliquer au secteur de l'administration publique. Malheureusement, ce n'est toujours pas le cas aujourd'hui.

Selon M. Wim Van Langenhove, *Head of Cybersecurity Advisory* auprès *d'Orange Cyberdefense*, l'absence des services publics de la liste constitue une lacune de la loi NIS. Un expert de l'industrie de l'eau a fait observer que la loi NIS les contraint à partager des données critiques sur leur sécurité avec les autorités et que le secteur se tient à cette obligation. Les experts s'inquiètent des conséquences qu'aurait un piratage du SPF Intérieur. En effet, si certaines informations tombent entre les mauvaises mains, les conséquences peuvent être importantes. Ce SPF partage-t-il des informations sensibles avec une infrastructure qui est moins bien sécurisée que celle de l'industrie de l'eau? Nous sommes d'avis que l'absence des services publics de la liste constitue en effet une lacune de la loi NIS justifiant une modification de la loi en question.

om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld.

De spreker stelt echter vast dat de overheid zelf niet opgenomen is in de lijst van organisaties en entiteiten die aan de NIS1-richtlijn moeten voldoen. Vandaar dat de spreker dit wetsvoorstel indient, teneinde de overheidssector onder te brengen in het toepassingsgebied van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Het CCB merkt op dat de Organisaties van Vitaal Belang (OVI's) worden geconfronteerd met een sterk toenemende en meer geavanceerde cyberdreiging. Het is cruciaal hen op gepaste wijze te ondersteunen in hun bescherming: cyberaanvallen tegen die organisaties kunnen immers een aanzienlijke impact hebben op de maatschappij en op de nationale veiligheid. Het CCB ontvangt als nationale autoriteit voor cyberveiligheid alle pertinente dreigingsinformatie, analyseert die en stuurt waarschuwingen uit. De OVI's worden op die manier permanent geïnformeerd over relevante cybersecuritydreigingen, kwetsbaarheden of incidenten. Om cybercriminaliteit en overheidsdreigingen snel te kunnen aanpakken, moet er worden geïnvesteerd in de snelle identificatie van en reactie op bedreigingen met gevaar voor de bevolking, voor de economie of voor OVI's.

In het kader van omzetting van de NIS1-richtlijn had het CCB reeds in 2019 voorgesteld om de overheid ook op te nemen in de lijst van de OVI's. Zo stelde de federaal procureur, Frédéric Van Leeuw, tijdens de hoorzitting over de cyberaanvallen op de IT-infrastructuur van de Staat, dat de NIS1-richtlijn ook van toepassing zou moeten zijn op de overheidssector. Helaas is dat tot op heden nog steeds niet het geval.

Voor de heer Wim Van Langenhove, *Head of Cybersecurity Advisory* bij *Orange Cyberdefense*, is het ontbreken van overheidsdiensten een hiaat in de huidige NIS-wet. Een expert uit de waterindustrie merkte op dat de NIS-wet hen ertoe verplicht om kritieke data over hun beveiliging te delen met de overheid en dat de sector zich daaraan houdt. Als de FOD Binnenlandse Zaken wordt gehackt, dan baart dat de expert zorgen; als bepaalde informatie in verkeerde handen valt, kan dat immers grote gevolgen hebben. Deelt die FOD gevoelige informatie met een infrastructuur die minder goed beveiligd is dan die van de waterindustrie? Het ontbreken van overheidsdiensten is volgens de spreker inderdaad een lacune in de huidige NIS-wet, die een wijziging van de aangehaalde wet verantwoord maakt.

La proposition de loi à l'examen laisse au Roi le soin de déterminer les services du secteur public qui doivent être considérés comme essentiels au maintien d'activités sociétales ou économiques critiques. À cet égard, il convient également de démontrer que la fourniture du service essentiel dépend des réseaux et des systèmes d'information.

L'intervenant fait en outre observer que le nombre de cyberattaques a régulièrement augmenté au cours des dernières années. En 2013, nous avons été confrontés à plusieurs révélations embarrassantes concernant des cyberattaques contre les pouvoirs publics. En 2011, des programmes malveillants ont été détectés sur des ordinateurs du SPF Affaires étrangères, puis supprimés avec l'aide de la Défense. Le service de renseignement militaire, le SPF Justice et Belgacom ont également été victimes de cyberattaques.

Trois ans plus tard, il est apparu que le nombre de cyberattaques perpétrées contre les services publics fédéraux était passé de 405 en 2014 à 666 en 2015. Au début de l'année 2017, il s'est à nouveau avéré que l'administration fédérale était de plus en plus ciblée par des cyberattaques. La diplomatie belge en était la principale cible (4.000 attaques par mois, soit près de 130 par jour). Ces attaques ont également visé l'Agence fédérale pour la sécurité de la chaîne alimentaire (6.000 tentatives par an), le Registre national, un site web du Centre de crise, le SPF Économie, l'ONEm, l'ONSS, l'INASTI, le SPF Santé publique et l'armée.

Selon une enquête menée auprès de tous les ministres fédéraux en 2018, les services publics fédéraux sont confrontés à au moins une cyberattaque ciblée chaque semaine. Au SPF Finances, des ordinateurs ont été pris en otage et paralysés et ces attaques ont également visé la Chancellerie, l'Institut géographique national et le Service fédéral des Pensions.

Plus récemment, en mars 2021, nous avons encore été frappés par deux cyberincidents de grande ampleur dans les pouvoirs publics. En juin 2021, une attaque *Distributed Denial of Sevice* (attaque DDoS) visant le réseau Belnet a complètement bloqué différents sites web publics. Il est ensuite apparu que le SPF Intérieur avait été espionné durant deux ans par des pirates informatiques (supposément étrangers).

La proposition de loi à l'examen a été déposée le 21 décembre 2021 et, dans l'intervalle, l'infrastructure informatique du ministère de la Défense a également été piratée. En résumé, la cybermenace est actuelle et elle mérite une réponse adéquate. Le gouvernement s'efforce de créer un environnement informatique sécurisé. La proposition de loi à l'examen s'inscrit donc dans le droit

In het voorliggend wetsvoorstel wordt aan de Koning overgelaten welke diensten van de publieke sector als essentieel voor de instandhouding van kritieke maatschappelijke en economische activiteiten moeten worden beschouwd. Er moet daarbij ook worden aangetoond dat de verlening van de essentiële dienst afhankelijk is van netwerk- en informatiesystemen.

Daarnaast merkt de spreker op dat het aantal cyberaanvallen de afgelopen jaren gestaag is toegenomen. In 2013 werden we geconfronteerd met een aantal pijnlijke onthullingen over cyberaanvallen op de overheid. Op computers van de FOD Buitenlandse Zaken waren in 2011 schadelijke programma's aangetroffen die met de hulp van Defensie waren verwijderd. Andere slachtoffers van cyberaanvallen waren de militaire inlichtingendienst, de FOD Justitie en Belgacom.

Drie jaar later bleek dat het aantal cyberaanvallen op de federale overheidsdiensten was toegenomen van 405 in 2014 naar 666 in 2015. Begin 2017 bleek opnieuw dat de federale overheidsdiensten steeds vaker het doelwit zijn van cyberaanvallen. De Belgische diplomatie was het belangrijkste doelwit (4.000 aanvallen per maand of bijna 130 per dag). Andere slachtoffers waren het Federaal Agentschap voor de Veiligheid van de Voedselketen (6.000 pogingen per jaar), het Rijksregister, een website van het Crisiscentrum, de FOD Economie, de RVA, het RIZIV, de RSZ, De FOD Volksgezondheid en het leger.

Uit een rondvraag bij alle federale ministers in 2018 bleek dat de federale overheidsdiensten minstens elke week met een gerichte cyberaanval te maken krijgen. Bij de FOD Financiën werden computers gegijzeld en lamgelegd; andere slachtoffers waren de Kanselarij, het Nationaal Geografisch Instituut en de Federale Pensioendienst.

Meer recent werden we in maart 2021 nog opgeschrikt door twee grote cyberincidenten bij de overheid. Eerst was er de *Distributed Denial of Service*-aanval (DDoS-aanval) op Belnet, die verschillende overheidswebsites volledig platlegde. Daarna bleek dat de FOD Binnenlandse Zaken twee jaar lang werd bespioneerd door (vermoedelijk buitenlandse) hackers.

Dit wetsvoorstel werd ingediend op 21 december 2021 en in de tussentijd werd ook de IT-infrastructuur van het ministerie van Defensie gehackt. Kortom, de cyberdreiging is actueel en omvangrijk en verdient een adequate respons. De huidige regering stelt zich tot doel van België tegen 2025 een cyberveilige omgeving te maken. Het voorliggend wetsvoorstel past dan ook perfect binnen

fil de cet objectif en soumettant également les services publics, et non pas seulement quelques acteurs privés, à la législation européenne en vigueur, afin de renforcer et de généraliser la cybersécurité.

III. — **DISCUSSION GÉNÉRALE**

A. **Questions et observations des membres**

M. Michael Freilich (N-VA) fait observer que, selon l'exposé des motifs, les obligations de la directive NIS2 ne s'appliquent qu'à un nombre limité d'entités faisant partie de secteurs critiques et fournissant des services d'intérêt général pour la population et les entreprises, ou critiques pour le potentiel économique du pays (DOC 55 3862/001, p. 7). Dans sa note de politique générale, le premier ministre a toutefois fait observer qu'avec la mise en œuvre de la loi NIS2, des milliers d'entités nationales essentielles et importantes devront améliorer leur niveau de cybersécurité. La ministre peut-elle transmettre une liste de ces entités? Combien d'entre elles relèvent-elles du secteur privé? Combien du secteur public? Comment ces dernières sont-elles réparties entre les différents niveaux (fédéral, régional et local)?

Cette dernière question n'est pas sans importance, dès lors que les pouvoirs publics sont visés par la directive NIS2. Les auteurs du projet de loi à l'examen estiment effectivement que cette matière relève des compétences résiduelles exclusives du législateur fédéral. Selon les auteurs, le projet de loi à l'examen n'a pas pour conséquence de rendre impossible ou exagérément difficile l'exercice normal des compétences régionales ou communautaires dans les domaines d'activités de certaines entités essentielles ou importantes concernées. L'incidence sur les Régions a-t-elle été calculée? Une concertation a-t-elle été menée à ce sujet avec les Régions?

L'intervenant ajoute que l'article 5 du projet de loi à l'examen ne mentionne pas les autorités du pouvoir législatif, car elles ne relèvent pas de la notion d'entité de l'administration publique. L'intervenant le déplore car, compte tenu de l'importance des missions de la Chambre des représentants, cette entité constitue une cible potentielle pour une cyberattaque hostile. Quelles mesures de cybersécurité les autorités du pouvoir législatif doivent-elles prendre? Qui doit y veiller?

Selon l'article 21 du projet de loi à l'examen, le centre national de réponse aux incidents de sécurité informatique (CSIRT) joue également un rôle de prévention, de recherche et de détection en matière d'infractions

deze beoogde doelstelling door ook de overheidsdiensten, en dus niet enkele private actoren, te onderwerpen aan de vigerende Europese wetgeving, teneinde de cyberveiligheid te versterken en te veralgemenen.

III. — **ALGEMENE BESPREKING**

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

De heer Michael Freilich (N-VA) merkt op dat volgens de memorie van toelichting de verplichtingen van de NIS2-richtlijn alleen van toepassing zijn op een beperkt aantal entiteiten die deel uitmaken van kritieke sectoren en diensten van algemeen belang verlenen voor de bevolking en ondernemingen, of kritiek zijn voor het economisch potentieel van het land (DOC 55 3862/001, blz. 7). In zijn beleidsnota merkte de premier echter op dat met de implementatie van de NIS2-wet duizenden nationale essentiële en belangrijke entiteiten hun niveau van cyberveiligheid zullen moeten opkrikken. Kan de minister een overzicht laten bezorgen van die entiteiten? Hoeveel behoren tot de private sector? Hoeveel tot de publieke sector? Hoe zijn die laatste verdeeld over de verschillende niveaus (federaal, regionaal en lokaal)?

Deze laatste vraag is niet onbelangrijk nu de overheid is opgenomen in de NIS2-richtlijn. De indieners van het wetsontwerp zijn namelijk van mening dat dit wetsontwerp tot de exclusieve restbevoegdheid van de federale wetgever behoort. Het wetsontwerp heeft volgens de indieners niet tot gevolg dat het voor de gewesten of gemeenschappen onmogelijk of bovenmatig moeilijk zou zijn om hun bevoegdheden op de werkterreinen van sommige betrokken essentiële of belangrijke entiteiten gewoon uit te oefenen. Werd de impact op de regio's berekend? Werd daar overleg over gepleegd met de regio's?

Daarnaast merkt de spreker op dat in artikel 5 van het voorliggend wetsontwerp de autoriteiten van de wetgevende macht niet vermeld worden, omdat zij niet onder het begrip overheidsinstantie vallen. De spreker betreurt dit aangezien er belangrijk werk geleverd wordt in de Kamer van volksvertegenwoordigers waardoor deze instantie een potentieel doelwit vormt voor een vijandige cyberaanval. Welke cyberbeveiligingsmaatregelen moeten de autoriteiten van de wetgevende macht? Wie zal daarop toezien?

Volgens artikel 21 van dit wetsontwerp speelt het nationale *Computer Security Incident Response Team* (CSIRT) een rol bij het voorkomen, onderzoeken en opsporen van misdrijven die online of via een

commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave. La détection et la recherche des infractions seront effectuées par les services de police, avec le soutien éventuel du *Cyber Emergency Response Team* (CERT) en tant qu'expert. La ministre peut-elle préciser le rôle de prévention, de recherche et de détection en matière d'infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave? Comment s'articule la coopération avec les services de police? Quand le CERT apportera-t-il un appui? Une concertation a-t-elle été menée à ce sujet avec les services concernés? Quels en sont les résultats?

L'article 50 du projet de loi à l'examen prévoit que le Roi est habilité à déterminer, par (sous-) secteur, des rétributions, en ce compris les modalités de calcul et de paiement, relatives aux prestations d'inspection. Quels sont les montants en jeu? Comment seront-ils calculés?

L'article 62 du projet de loi à l'examen dispose que les amendes et les mesures en cas de non-exécution d'une décision ou de non-respect de la loi ne s'appliquent pas aux entités faisant partie du secteur de l'administration publique. Cette dérogation est laissée, en partie, à l'appréciation des États membres par la directive NIS2. Pourquoi le gouvernement a-t-il opté pour cette dérogation? Qu'adviendra-t-il si elles ne respectent pas la loi? L'intervenant estime que le législateur va ainsi ancrer légalement une inégalité de traitement entre le secteur privé et le secteur public.

L'intervenant conclut en indiquant que son groupe soutient la transposition de la directive NIS2, qui vise à accroître la résilience numérique et économique des États membres. La transformation numérique rapide et l'interconnexion de la société ont fait des réseaux et des systèmes d'information des caractéristiques essentielles de notre vie quotidienne. L'expansion du paysage des cybermenaces entraîne de nouveaux défis qui nécessitent des réponses adaptées, coordonnées et novatrices. La cybersécurité protégera également les utilisateurs contre les cybermenaces. Les cyberincidents se multiplient quelle que soit la manière. Ils constituent une menace majeure pour le bon fonctionnement des activités sociétales ou économiques critiques et des services publics. Son groupe se réjouit dès lors qu'un cadre réglementaire ait enfin été élaboré pour protéger les hackers éthiques.

Son groupe ne peut toutefois pas adhérer au projet de loi à l'examen, dans la mesure où 22 de ses articles contiennent 32 habilitations au Roi, ce qui est bien trop

elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten. Het opsporen en onderzoeken van misdrijven zal door de politionele diensten gebeuren, al dan niet met steun als expert door het *Cyber Emergency Response Team* (CERT). Kan de minister de rol van het CSIRT bij het voorkomen, onderzoeken en opsporen van misdrijven die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten? Hoe wordt de samenwerking met de politionele diensten geregeld? Wanneer zal het CERT steun verlenen? Werd daarover overleg gepleegd met de betrokken diensten? Met welke resultaten?

Artikel 50 van het voorliggend wetsontwerp bepaalt dat de Koning is gemachtigd om, per (deel)sector, retributies te bepalen, met inbegrip van de berekenings- en betalingsregels, voor de inspectieprestaties. Over welke bedragen zal het gaan? Hoe zullen die worden berekend?

Artikel 62 van dit wetsontwerp bepaalt dat de geldboetes en maatregelen bij het negeren van een beslissing en niet-naleving van de wet niet van toepassing zijn op entiteiten die deel uitmaken van de overheidssector. De NIS2-richtlijn laat deze afwijking gedeeltelijk over aan het oordeel van de lidstaten. Waarom kiest de regering voor deze afwijking? Wat als zij de wet niet naleven? De spreker meent dat de wetgever op deze manier een ongelijke behandeling tussen de private en de publieke sector wettelijk gaat verankeren.

Tot slot stipt de spreker aan dat zijn fractie haar steun toezegt aan de omzetting van de NIS2-richtlijn, die de digitale en economische weerbaarheid van de lidstaten wil verhogen. De snelle digitale transformatie en de onderlinge digitale verbondenheid van de samenleving hebben ervoor gezorgd dat netwerk- en informatiesystemen een centraal kenmerk van het dagelijks leven zijn geworden. De uitbreiding van het cyberdreigingslandschap brengt nieuwe uitdagingen met zich mee die aangepaste gecoördineerde en innovatieve respons vereisen. Cyberbeveiliging zal ook de gebruikers beschermen tegen cyberdreigingen. Cyberincidenten nemen toe op alle mogelijke manieren. Ze vormen een grote bedreiging voor de goede werking van kritieke maatschappelijke en economische activiteiten en van openbare diensten. Zijn fractie is dan ook tevreden dat er eindelijk een regelgevend beschermend kader is ontworpen voor ethische hackers.

Evenwel kan zijn fractie dit wetsontwerp niet goedkeuren. Er zitten in 22 artikelen van het voorliggend wetsontwerp 32 machtigingen aan de Koning. Dat is voor

aux yeux de son groupe. En tant que membre de l'opposition, son groupe ne peut autoriser autant d'habilitations au ministre et/ou au gouvernement. C'est la raison pour laquelle son groupe s'abstiendra lors du vote du projet de loi à l'examen.

M. Samuel Cogolati (Ecolo-Groen) fait observer que la justice américaine a inculpé les sept auteurs qui se cachent derrière le groupe de hackers chinois baptisé "APT31" (*Advanced Persistent Threat*), également connu sous le nom de Zirconium. Ces sept auteurs sont tous liés au ministère chinois de la sécurité d'État et opèrent depuis la ville chinoise de Wuhan.

Ils ont été formellement poursuivis par la justice américaine devant une juridiction new yorkaise. Les autorités américaines ont également prononcé des sanctions à l'encontre de ces sept personnes, tandis que le ministre des Affaires étrangères du Royaume-Uni, M. David Cameron, a convoqué l'ambassadeur de Chine à Londres. Les autorités belges compétentes, notamment le CCB, ont-elles été informées des mesures prises respectivement par les autorités britanniques et américaines? Dans l'affirmative, de quelles informations les autorités belges disposent-elles concernant les victimes belges potentielles de ces activités de hacking? L'intervenant ajoute qu'un membre de la Chambre des représentants figure parmi ces victimes et ce membre n'est autre que lui-même. Quelle est par ailleurs l'étendue de la fuite de données?

Les auteurs ayant été formellement identifiés par les autorités américaines, l'intervenant se demande si les autorités belges entreprendront également une action. Quelles mesures le CCB prendra-t-il par exemple à l'encontre d'APT31, dont les activités de hacking ont déjà visé des victimes belges par le passé?

M. Daniel Senesael (PS) souligne l'importance du projet de loi à l'examen, qui vise à transposer une directive européenne. Les systèmes d'information numériques sont devenus des éléments centraux de notre société et, vu leur nombre, leur ampleur et leur sophistication, les cyberattaques représentent des menaces considérables pour notre société, ses habitants et ses institutions.

L'objectif du projet de loi est donc de renforcer le cadre réglementaire en matière de cybersécurité afin d'armer l'infrastructure informatique existante et de la rendre suffisamment résiliente aux cyberattaques. Il s'agira d'améliorer considérablement le fonctionnement et de veiller à une harmonisation et à une meilleure coordination entre les différents services concernés.

zijn fractie van het goede te veel. Vanuit de oppositie kan zijn fractie zoveel machtigingen aan de minister en/of de regering niet toestaan. Daarom zal zijn fractie zich onthouden bij de stemming van dit wetsontwerp.

De heer Samuel Cogolati (Ecolo-Groen) merkt op dat de Amerikaanse overheid de zeven daders in beschuldiging heeft gesteld die schuilgaan achter het Chinese hackerscollectief APT31 (*Advanced Persistent Threat*), ook wel gekend onder de naam Zirkonium. Deze zeven personen zijn allen verbonden aan de diensten van de Chinese staatsveiligheid. Ze opereren vanuit de Chinese stad Wuhan.

Thans worden ze formeel vervolgd door de Amerikaanse autoriteiten, vanuit een gerechtelijk district gelegen te New York. De Amerikaanse overheid heeft trouwens ook sancties uitgesproken tegen deze zeven personen, terwijl de minister van Buitenlandse Zaken van het Verenigd Koninkrijk, de heer David Cameron, de Chinese ambassadeur te London op het matje heeft geroepen. Werden de bevoegde Belgische autoriteiten waaronder het CCB, op de hoogte gebracht van de maatregelen die door de respectieve Britse en Amerikaanse autoriteiten werden genomen? Indien ja, over welke informatie beschikken de Belgische autoriteiten betreffende potentiële Belgische slachtoffers van hun hackingactiviteiten? Volgens de spreker is er onder deze slachtoffers een lid van de Kamer van volksvertegenwoordigers, met name hemzelf. Wat is daarbij de omvang van het datalek?

Aangezien de daders thans formeel door de Amerikaanse autoriteiten werden geïdentificeerd, vraagt de spreker zich af of ook de Belgische autoriteiten stappen zullen ondernemen. Welke stappen zal het CCB ondernemen tegen APT31, dat in het verleden reeds hackingactiviteiten heeft uitgevoerd tegen Belgische doelwitten?

De heer Daniel Senesael (PS) stipt aan dat dit wetsontwerp een belangrijk wetsontwerp is dat de omzetting beoogt van een Europese richtlijn. Hij benadrukt het belang van de vele digitale informaticanetwerken in de hedendaagse samenleving en wijst op de vele en steeds meer belangrijke en omvangrijke cyberaanvallen die een ernstige bedreiging vormen voor deze samenleving, haar bevolking en haar instellingen.

Het doel van het wetsontwerp bestaat er dan ook in om het regelgevend kader inzake cyberbeveiliging te versterken, teneinde de bestaande informatica-infrastructuur te bewapenen en voldoende weerbaar te maken tegen cyberaanvallen. Hierbij is er aandacht om de werking ingrijpend te verbeteren alsook om de verschillende betrokken diensten beter op elkaar af te stemmen en

L'intervenant se demande dès lors comment, en cas de cyberattaque, la collaboration se déroulera entre le CCB, d'une part, et la *Computer Crime Unit* de la Police fédérale et la future composante de la Défense chargée de la cybersécurité, d'autre part. À cet égard, il rappelle que, par le passé, le manque de coordination et d'échange d'informations entre les différents services de sécurité a malheureusement nui à leur performance.

M. Jef Van den Bergh (cd&v) fait observer que le projet de loi à l'examen porte sur une matière importante. La numérisation et internet sont désormais indissociables de notre quotidien, et c'est d'autant plus vrai pour les secteurs critiques qui assurent le bon fonctionnement de notre pays. Il est donc particulièrement important de veiller à protéger au mieux ces secteurs contre les cybermenaces, qui ne sont malheureusement pas hypothétiques. L'intervenant donne l'exemple d'une cyberattaque dirigée contre le SPF Intérieur. Dans le contexte international actuel, caractérisé par une polarisation croissante au sein des différents pays et blocs de pouvoir et entre ceux-ci, il est donc plus que jamais opportun de renforcer sensiblement le cadre législatif en matière de cybersécurité afin de pouvoir formuler des réponses adéquates aux menaces dans ce domaine.

L'intervenant constate que les explications très claires et complètes de la ministre et du directeur général du CCB ont permis de répondre à toutes ses questions. Il conclut donc en faisant part du soutien de son groupe au projet de loi à l'examen.

Mme Meryame Kitir (Vooruit) souligne à quel point il est important de renforcer la cybersécurité. Elle renvoie, dans ce cadre, aux récentes cyberattaques qui mettent en avant l'urgence d'intervenir tant dans le secteur privé que dans le secteur public. Dans le cadre de la discussion du projet de loi à l'examen, l'intervenante aimerait savoir si des particuliers et des entreprises privées figurent également sur la liste des entités qui méritent une attention particulière dans le cadre de la cybersécurité. Le présent dossier couvrira-t-il l'ensemble des autorités publiques? Quel sera leur rôle et pourquoi des exceptions ont-elles été prévues pour les autorités publiques dans le cadre du projet de loi à l'examen?

B. **Réponses du ministre et du directeur général**

Mme Annelies Verlinden, ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique, indique que le gouvernement a choisi de

de werking meer te harmoniseren. Bijgevolg vraagt de spreker zich af hoe de samenwerking tijdens een cyberaanval zal verlopen tussen het CCB, enerzijds, en de *Computer Crime Unit* van de Federale Politie en de toekomstige component van het Belgische leger die zich zal bezighouden met de cyberveiligheid, anderzijds. Hij brengt hierbij in herinnering dat het gebrek aan afstemming en informatie-uitwisseling tussen de verschillende veiligheidsdiensten in het verleden jammer genoeg een performante werking van deze diensten in de weg heeft gestaan.

De heer Jef Van den Bergh (cd&v) merkt op dat het voorwerp van dit wetsontwerp belangrijk is. De digitalisering en het internet kunnen niet meer weggedacht worden uit het dagelijks leven en dit geldt zeker voor de kritieke sectoren die ervoor zorgen dat het land blijft draaien. Het is daarom bijzonder belangrijk om ervoor te zorgen dat deze sectoren optimaal beschermd zijn tegen cyberdreigingen. Dergelijke dreigingen zijn jammer genoeg geen hypothetisch gegeven. De spreker verwijst hierbij bijvoorbeeld naar een cyberaanval tegen de FOD Binnenlandse Zaken. Binnen de huidige internationale context die gekenmerkt wordt door toenemende polarisering binnen en tussen verschillende landen en machtsblokken is het dan ook meer dan aangewezen om het wetgevend kader inzake cyberveiligheid gevoelig te versterken, teneinde adequate antwoorden op bedreigingen ter zake te kunnen formuleren.

Gelet op de heel heldere alsook volledige toelichting van de minister en de administrateur-generaal van het CCB, stelt de spreker vast dat al zijn vragen reeds werden beantwoord. Er rest hem enkel nog mee te delen dat zijn fractie dit wetsontwerp zal goedkeuren.

Mevrouw Meryame Kitir (Vooruit) benadrukt het belang van de versterking van de cyberveiligheid. Ze verwijst in dit kader naar recente cyberaanvallen die de urgentie van deze cyberveiligheid zowel in de private sector als in de publieke sector kunnen onderstrepen. De spreekster wil in het kader van de bespreking van het voorliggend wetsontwerp graag vernemen of er ook private personen alsook privébedrijven zijn opgenomen in de lijst die bijzondere aandacht verdienen in het kader van cyberbeveiliging. Is de volledige overheid gevat in dit dossier? Wat is de rol van de overheid en waarom werden er uitzonderingen verleend aan de overheid in het kader van dit wetsontwerp?

B. **Antwoorden van de minister en de directeur-generaal**

Mevrouw Annelies Verlinden, minister van Binnenlandse Zaken, Institutionele Hervorming en Democratische Vernieuwing, stipt aan dat de regering ervoor gekozen

reprendre la notion d'autorité administrative visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur le Conseil d'État, à laquelle sont ajoutés les critères de ne pas avoir de caractère industriel ou commercial, de ne pas exercer à titre principal une activité relevant de l'un des autres secteurs ou sous-secteurs repris dans les annexes du présent projet de loi et de ne pas être une personne morale de droit privé. Le choix de prendre cette définition pour base s'explique par le fait que la plupart des critères repris dans la définition de la directive se retrouvent dans les critères qui délimitent la notion d'autorité administrative définie ou visée par les lois coordonnées sur le Conseil d'État.

Cette définition doit être combinée aux définitions des entités de l'annexe I "secteurs hautement critiques" – secteur 10 Administration publique. Il s'agit des autorités publiques qui dépendent de l'État fédéral, des autorités publiques qui dépendent des entités fédérées et des zones de secours, qui fournissent des services essentiels à la population et aux entreprises. Il va de soi que ces autorités jouent également un rôle important dans les situations de crise.

D'autre part, un article énumère les autorités publiques auxquelles la loi ne s'applique pas. L'article 2, paragraphes 7 et 8, de la directive exclut effectivement de son champ d'application les entités de l'administration publique ou des entités spécifiques qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense, ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière, pour autant qu'elles ne constituent pas des prestataires de services de confiance. Cet élément a également été pris en compte au moment de transposer la directive. Toutefois, il n'en résulte pas que les instances concernées ne doivent pas prendre de mesures de cybersécurité, mais uniquement qu'elles ne relèvent pas du champ d'application défini.

La ministre conclut en précisant que ces instances devraient bénéficier d'un niveau de protection au moins équivalent, voire supérieur au niveau de base imposé à certaines entités essentielles, compte tenu de la nature essentielle du service. Comme c'est déjà le cas actuellement s'agissant des cyberincidents significatifs notifiés au CCB selon des modalités particulières et dans le respect des exigences liées à la sécurité nationale et du plan national d'urgence cyber, les activités les plus sensibles des autorités publiques sont réalisées, comme indiqué, au moyen de réseaux et de systèmes approuvés pour traiter des informations classifiées.

heeft om te verwijzen naar het begrip administratieve overheid zoals bedoeld in artikel 14, paragraaf 1, eerste lid, van de gecoördineerde wetten op de Raad van State, waaraan de criteria worden toegevoegd zodat het moet gaan om overheden die niet van industriële of commerciële aard zijn, die niet hoofdzakelijk een activiteit uitoefenen die tot een van de andere sectoren of deelsectoren opgenomen in de bijlagen van dit wetsontwerp behoren en die ook geen privaatrechtelijke rechtspersoon zijn. De keuze voor deze definitie wordt verklaard door het feit dat de meeste criteria in de definitie van de richtlijn eveneens terug te vinden zijn in de criteria verbonden aan het begrip administratieve overheid, zoals gedefinieerd of bedoeld door de gecoördineerde wetten op de Raad van State.

Deze definitie moet met de definities van entiteiten in bijlage I "zeer kritieke sectoren" – sector 10 Overheid gecombineerd worden, zijnde overheidsinstanties die van de Federale Staat afhangen, overheidsinstanties die van de deelgebieden afhangen en de hulpverleningszones, die essentiële diensten verlenen aan de bevolking alsook aan bedrijven. Zij spelen uiteraard ook een belangrijke rol in crisissituaties.

Daarnaast is er ook een artikel opgenomen dat de overheden oplijst waarop de wet niet van toepassing is. Artikel 2, paragrafen 7 en 8, van de Richtlijn sluit overheidsinstanties en specifieke entiteiten die activiteiten uitoefenen uit op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, voor zover zij geen aanbieders zijn van vertrouwensdiensten. In dit kader heeft er dus ook een vertaling van de richtlijn plaatsgevonden. Dat betekent echter niet dat de betrokken instanties geen cyberveiligheidsmaatregelen moeten nemen. Het betekent louter dat zij niet onder het toepassingsgebied vallen.

De minister besluit dat deze instanties minstens een gelijkwaardig en zelfs een hoger niveau van bescherming zouden moeten bereiken dan het basisniveau dat aan sommige essentiële entiteiten wordt opgelegd, gelet op het essentiële karakter van de dienstverlening. Zoals vandaag al het geval is voor de significante cyberincidenten gemeld aan het CCB, met inachtneming van de vereiste van nationale veiligheid en het nationaal cybernoodplan volgens de bijzondere modaliteiten, moeten de meest gevoelige activiteiten van de overheidsinstanties, zoals net aangehaald, worden uitgevoerd door middel van netwerksystemen die zijn goedgekeurd voor de verwerking van geclassificeerde informatie.

En ce qui concerne les rétributions et les amendes, la ministre fait observer que certaines dispositions feront l'objet d'un arrêté royal à venir, mais que plusieurs dispositions importantes concernant notamment les montants des amendes administratives ont été définies et inscrites dans le projet de loi à l'examen, en particulier dans son article 59. Les montants de ces amendes varieront également en fonction des comportements ou des conduites sanctionnés par les amendes. En résumé, il existera bien une base légale et les critiques portant sur le pouvoir de décision conféré au Roi par arrêté royal sont donc difficilement compréhensibles selon la ministre.

M. Miguel De Bruycker, directeur général du Centre pour la Cybersécurité Belgique, souligne que le CCB est une entité particulièrement transparente qui est avant tout responsable du traitement des incidents graves, mais qui tente également de répertorier les principales menaces et, en particulier, d'identifier les systèmes vulnérables et d'avertir leurs propriétaires avant que les pirates informatiques s'y introduisent.

Il existe une différence importante entre la directive NIS1 et la directive NIS2 en ce qui concerne l'identification et le nombre d'entités. En effet, l'Union européenne applique à présent une règle associée à un plafond explicite (*size-cap*) à 18 secteurs, à savoir à 11 secteurs énumérés à l'annexe I et à 7 secteurs énumérés à l'annexe II. Ainsi, toute entité visée à l'annexe I doit, pour être considérée comme importante, compter au moins 50 travailleurs ou réaliser un chiffre d'affaires annuel de plus de 10 millions d'euros. Si le nombre de ses travailleurs se monte à ou moins 250 et si son chiffre d'affaires annuel dépasse 50 millions d'euros, l'entité visée est jugée essentielle. La CCB a calculé, en s'appuyant sur des informations provenant de la Banque Carrefour des Entreprises (BCE) et du SPF Économie, que la Belgique compte environ 800 entités essentielles et 1.600 entités importantes. Au total, 2.400 entités devraient relever donc du champ d'application de cette législation, y compris les autorités publiques.

En ce qui concerne les autres services en matière de cybersécurité et les missions du CERT, qui fait partie du CCB, l'orateur indique que la mission du CCB est d'assurer la protection grâce à l'identification des systèmes vulnérables ainsi que contre les cyber-attaques et les menaces dans le but d'alerter le propriétaire du système visé dès que possible afin de lui permettre de prendre les mesures appropriées pour mieux protéger son réseau, au besoin en étant accompagné, s'il le souhaite, par le CCB.

Met betrekking tot de retributies en de boetes merkt de minister op dat een aantal bepalingen in een toekomstig koninklijk besluit zullen worden opgenomen, maar een aantal significante bepalingen zoals de bedragen van de administratieve boetes ook worden gedefinieerd en opgenomen in het voorliggend wetsontwerp, met name in artikel 59. De hoogte van die boetes verschilt ook naargelang van het gedrag dat of de handelswijze die aan de basis lag van de boete. Kortom, er bestaat in dit geval wel degelijk een wettelijke basis, waardoor de minister niet goed de kritiek begrijpt dat er te veel beslissingsbevoegdheid via een koninklijk besluit in de handen van de Koning wordt gelegd.

De heer Miguel De Bruycker, directeur-generaal van het Centrum voor Centrum voor Cybersecurity België, stipt aan dat het CCB een zeer transparante entiteit is die in eerste instantie instaat voor het behandelen van ernstige incidenten, maar dat het CCB ook probeert de voornaamste dreigingen in kaart te brengen en vooral de kwetsbare systemen te identificeren en de eigenaars ervan te waarschuwen alvorens hackers kunnen binnendringen in deze systemen.

Inzake de identificatie en het aantal entiteiten is er een groot verschil tussen de NIS1-richtlijn en de NIS2-richtlijn, in die zin dat de Europese Unie nu heel duidelijk voor achttien sectoren, met name 11 sectoren in bijlage I en 7 sectoren in bijlage II, werkt met een systeem van een *sizecap*. Dus wat betreft bijlage I, de belangrijke entiteiten, geldt dat zodra men ten minste 50 werknemers heeft of een jaarlijkse omzet draait ten belope van meer dan 10 miljoen euro, de desbetreffende entiteit als een belangrijke entiteit wordt beschouwd. Zodra het aantal werknemers ten minste 250 bedraagt en de jaarlijkse omzet hoger is dan 50 miljoen euro, behoort de desbetreffende entiteit tot de essentiële entiteiten. Op basis van informatie afkomstig van de Kruispuntbank van Ondernemingen (KBO) en de FOD Economie berekende het CCB dat er in België ongeveer 800 essentiële entiteiten en 1.600 belangrijke entiteiten zijn. In totaal zouden dus 2.400 entiteiten onder het toepassingsgebied van deze wetgeving moeten vallen, inclusief de overheden.

Met betrekking tot de andere diensten inzake cyberveiligheid en de opdrachten van CERT, dat onderdeel uitmaakt van het CCB, merkt de spreker op dat de opdracht van het CCB erin bestaat om bescherming te bieden via de identificatie van kwetsbare systemen alsook van cyberaanvallen en dreigingen, met als doel de eigenaar van het systeem zo snel mogelijk te waarschuwen, zodat hij de gepaste maatregelen kan nemen, desnoods met de begeleiding van het CCB, indien gewenst, om zijn netwerk beter te beschermen.

Pour ce faire, le CCB collabore étroitement avec les différents services membres du Comité de coordination du renseignement et de la sécurité, dont le CCB est membre à part entière. Cette coopération implique que, dès l'instant où le CCB, conformément au plan d'urgence national, fait passer un incident au niveau d'incident national, les huit services concernés sont informés automatiquement. Il est envisagé de désigner le CCB en tant qu'expert juridique, afin d'optimiser l'échange d'informations, lorsqu'une enquête judiciaire est entamée. Cette désignation présente un inconvénient pour le CCB, qui est alors lié par le secret de l'enquête et ne peut pas partager des données avec les CERT's des autorités nationales d'autres pays. Enfin, l'orateur souligne qu'il appartient à la Justice et à la police d'enquêter au sujet de l'infraction et de l'auteur de celle-ci, et que ce travail ne relève aucunement des missions du CCB.

En ce qui concerne les rétributions relatives aux prestations d'inspection, l'orateur indique que le montant de la rétribution correspondra au coût d'une évaluation menée par un organisme accrédité d'évaluation de la conformité (*Conformity Assessment Body)*. Cette option est possible mais il va de soi que l'entité qui décidera d'opter pour l'évaluation de la conformité standard pourra s'appuyer sur une certification, ce qui constituera pour elle un élément important. Cette certification est particulièrement importante car une responsabilité est désormais prévue par la loi, en la matière, pour les personnes qui assurent la direction de ces entités. Cette certification constituera donc une forme de preuve attestant que ces personnes ont pris les mesures appropriées pour protéger leurs réseaux et leurs systèmes d'information en cas de cyberattaque.

En ce qui concerne APT31, l'orateur souligne que le CCB a reçu des informations indiquant que toutes les victimes de la fuite de données ont été mises au courant. Le CCB reçoit de temps en temps en provenance de services de sécurité étrangers de nouvelles indications concernant APT31. Plusieurs pistes de contre-mesures peuvent aujourd'hui être envisagées. L'orateur évoque à cet égard la possibilité dont dispose le SPF Affaires étrangères d'attribuer l'origine d'une cyberattaque à une entité donnée. Toutefois, la décision finale en la matière constitue une décision politique. Le CCB fournira alors les informations permettant d'attribuer l'origine de la cyberattaque ou de l'incident à un acteur déterminé. Par ailleurs, le CCB tentera d'identifier un maximum de victimes ainsi que les failles exploitées par APT31 pour attaquer les réseaux et s'y introduire, afin de faire disparaître ces failles en les corrigeant.

Het CCB werkt daarbij zeer nauw samen met de verschillende diensten die lid zijn van het Coördinatiecomité Inlichtingen en Veiligheid, waarvan het CCB een volwaardig lid is. De samenwerking houdt in dat, vanaf het ogenblik dat het CCB, volgens het nationaal noodplan, een incident naar een nationaal incident escaleert, automatisch alle acht betrokken diensten worden geïnformeerd. Indien er een juridisch onderzoek wordt opgestart, is er een overweging om het CCB aan te stellen als juridisch expert, zodat dat de uitwisseling van informatie optimaal kan verlopen. Dit is in dat geval voor het CCB een nadeel aangezien het CCB op dat ogenblik gebonden is aan het geheim van het onderzoek en geen gegevensuitwisseling kan laten plaatsvinden met de CERT's van nationale overheden van andere landen. Tot slot stipt de spreker aan dat het de taak van het gerecht en de politie is om het onderzoek naar het misdrijf en de dader te voeren, en helemaal niet van het CCB.

Aangaande de retributies stipt de spreker aan dat wat de inspecties betreft, de grootte van de retributie in overeenstemming is met de kosten van een evaluatie door een geaccrediteerde conformiteitsbeoordelingsinstantie (*Conformity Assessment Body*). Deze optie is mogelijk, maar het spreekt voor zich dat een entiteit die kiest voor de standaard conformiteitsbeoordeling, gebruik zal kunnen maken van een certificatie, die een belangrijk element uitmaakt voor deze entiteit. Deze certificatie is met name belangrijk omdat de mensen die het bestuur van dergelijke entiteiten waarnemen een aansprakelijkheid ter zake dragen die thans wettelijk wordt bepaald. Deze certificatie geldt dus als een vorm van bewijs dat zij de gepaste maatregelen hebben genomen teneinde hun netwerk- en informatiesystemen te beschermen bij een eventuele cyberaanval.

Met betrekking tot APT31 merkt de spreker op dat het CCB informatie heeft ontvangen waaruit blijkt dat alle betrokken slachtoffers van het datalek op de hoogte werden gebracht. Van tijd tot tijd ontvangt het CCB nieuwe aanwijzingen die afkomstig zijn van buitenlandse veiligheidsdiensten met betrekking tot APT31. Thans kunnen als tegenmaatregel verschillende pistes bewandeld worden. De spreker verwijst hierbij naar de mogelijkheid waarover de FOD Buitenlandse Zaken beschikt om de oorsprong van de cyberaanval toe te wijzen aan een bepaalde entiteit. De finale beslissing hieromtrent is echter een politieke beslissing. Het CCB zal op dat ogenblik de informatie aanreiken om de cyberaanval of incident toe te schrijven aan een welbepaalde actor. Daarnaast zal het CCB zoveel mogelijk slachtoffers proberen op te sporen alsook zoveel mogelijk de zwaktes proberen te begrijpen die APT31 gebruikt om de netwerken aan te vallen en binnen te dringen, teneinde de zwaktes te kunnen oplossen en te verwijderen.

Dans le cadre de la coopération avec le *Cyber Command* (la composante militaire en charge de la cybersécurité), l'orateur a participé la semaine dernière à une réunion avec le chef de cette composante. Tous les services concernés sont en train de définir clairement quelles sont leurs compétences et leurs responsabilités spécifiques concernant cette mission particulière. Si la répartition des compétences n'est pas clarifiée en profondeur, des questions risquent de ne pas être traitées. Cette coopération se déroule de manière exemplaire et la répartition des différentes missions est très bien définie. Lorsqu'un point manque de clarté, on s'efforce d'apporter des éclaircissements et des précisions. La coopération avec le Centre de crise national est également importante pour le CCB, car elle lui permet à tout moment de réagir très rapidement, et le Centre de crise national peut à son tour s'adresser aux permanences nécessaires du CCB.

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

TITRE 1ER

Définitions et dispositions générales

CHAPITRE 1ER

Objet et champ d'application

Article 1er

Cet article fixe le fondement constitutionnel de la compétence. Il ne donne lieu à aucune observation.

L'article 1er est adopté à l'unanimité.

Art. 2 à 7

Ces articles ne donnent lieu à aucune observation.

L'article 2 est adopté à l'unanimité.

L'article 3 est adopté par 10 voix et 3 abstentions.

Les articles 4 à 6 sont successivement adoptés à l'unanimité.

L'article 7 est adopté par 10 voix et 3 abstentions.

In het kader van de samenwerking met de militaire component bevoegd voor cyberveiligheid, met name *Cyber Command*, heeft de spreker afgelopen week een vergadering gehad met de chef van *de Cyber Command* waarbij alle betrokken diensten gaan uitklaren wat de specifieke bevoegdheden en verantwoordelijkheden zijn van elk van hen met betrekking tot deze specifieke zaak. Indien deze bevoegdheidsverdeling niet grondig wordt uitgeklaard, dreigen er elementen niet behandeld te worden. De samenwerking verloopt voorbeeldig en de opsplitsing van de verschillende taken is zeer goed afgelijnd, en waar er thans nog onduidelijkheid heerst wordt gezocht naar opheldering en meer verduidelijking. Voor het CCB is ook de samenwerking met het Nationaal Crisiscentrum van belang omdat deze samenwerking het CCB toelaat om 24 op 7 heel snel te reageren, waarbij het Nationaal Crisiscentrum op zijn beurt de nodige permanenties van het CCB kan aanspreken.

IV. — **ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN**

TITEL 1

Definities en algemene bepalingen

HOOFDSTUK 1

Onderwerp en toepassingsgebied

Artikel 1

Dit artikel bepaalt de constitutionele grondslag van het wetsontwerp. Er worden geen opmerkingen over gemaakt.

Artikel 1 wordt eenparig aangenomen.

Art. 2 tot 7

Deze artikelen geven geen aanleiding tot opmerkingen.

Artikel 2 wordt eenparig aangenomen.

Artikel 3 wordt aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 4 tot 6 worden achtereenvolgens eenparig aangenomen.

Artikel 7 wordt aangenomen met 10 stemmen en 3 onthoudingen.

CHAPITRE 2

Définitions

Art. 8

Cet article ne donne lieu à aucune observation.

L'article 8 est adopté à l'unanimité.

CHAPITRE 3

Catégories d'entités

Art. 9 et 10

Ces articles ne donnent lieu à aucune observation.

Les articles 9 et 10 sont adoptés à l'unanimité.

CHAPITRE 4

Identification

Art. 11 et 12

Ces articles ne donnent lieu à aucune observation.

L'article 11 est adopté par 10 voix et 3 abstentions.

L'article 12 est adopté à l'unanimité.

CHAPITRE 5

Enregistrement des entités

Art. 13 et 14

Ces articles ne donnent lieu à aucune observation.

Les articles 13 et 14 sont successivement adoptés par 10 voix et 3 abstentions.

HOOFDSTUK 2

Definities

Art. 8

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 8 wordt eenparig aangenomen.

HOOFDSTUK 3

Categorieën van entiteiten

Art. 9 en 10

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 9 en 10 worden eenparig aangenomen.

HOOFDSTUK 4

Identificatie

Art. 11 en 12

Deze artikelen geven geen aanleiding tot opmerkingen.

Artikel 11 wordt aangenomen met 10 stemmen en 3 onthoudingen.

Artikel 12 wordt eenparig aangenomen.

HOOFDSTUK 5

Registratie van de entiteiten

Art. 13 en 14

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 13 en 14 worden achtereenvolgens aangenomen met 10 stemmen en 3 onthoudingen.

TITRE 2

Autorités compétentes et coopération au niveau national

CHAPITRE 1ER

Autorités compétentes

Art. 15 à 24

Ces articles ne donnent lieu à aucune observation.

L'article 15 est adopté par 10 voix et 3 abstentions.

L'article 16 est adopté à l'unanimité.

L'article 17 est adopté par 10 voix et 3 abstentions.

L'article 18 est adopté à l'unanimité.

L'article 19 est adopté par 10 voix et 3 abstentions.

Les articles 20 à 24 sont successivement adoptés à l'unanimité.

CHAPITRE 2

Coopération au niveau national

Art. 25

Cet article ne donne lieu à aucune observation.

L'article 25 est adopté à l'unanimité.

CHAPITRE 3

Confidentialité et échanges d'information

Art. 26 et 27

Ces articles ne donnent lieu à aucune observation.

Les articles 26 et 27 sont successivement adoptés à l'unanimité.

TITEL 2

Bevoegde autoriteiten en samenwerking op nationaal niveau

HOOFDSTUK 1

Bevoegde autoriteiten

Art. 15 tot 24

Deze artikelen geven geen aanleiding tot opmerkingen.

Artikel 15 wordt aangenomen met 10 stemmen en 3 onthoudingen.

Artikel 16 wordt eenparig aangenomen.

Artikel 17 wordt aangenomen met 10 stemmen en 3 onthoudingen.

Artikel 18 wordt eenparig aangenomen.

Artikel 19 wordt aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 20 tot 24 worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Samenwerking op nationaal niveau

Art. 25

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 25 wordt eenparig aangenomen.

HOOFDSTUK 3

Vertrouwelijkheid en informatie-uitwisseling

Art. 26 en 27

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 26 en 27 worden achtereenvolgens eenparig aangenomen.

CHAPITRE 4

Stratégie nationale en matière de cybersécurité

Art. 28

Cet article ne donne lieu à aucune observation.

L'article 28 est adopté à l'unanimité.

CHAPITRE 5

Le plan national de réaction aux crises cyber et incidents de cybersécurité

Art. 29

Cet article ne donne lieu à aucune observation.

L'article 29 est adopté à l'unanimité.

TITRE 3

Mesures de gestion des risques en matière de cybersécurité et obligations d'information

CHAPITRE 1ER

Mesures de gestion des risques en matière de cybersécurité

Art. 30 à 33

Ces articles ne donnent lieu à aucune observation.

Les articles 30 à 32 sont successivement adoptés à l'unanimité.

L'article 33 est adopté par 10 voix et 3 abstentions.

CHAPITRE 2

Notification d'incidents

Art. 34 à 38

Ces articles ne donnent lieu à aucune observation.

L'article 34 est adopté par 10 voix et 3 abstentions.

HOOFDSTUK 4

Nationale cyberbeveiligingsstrategie

Art. 28

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 28 wordt eenparig aangenomen.

HOOFDSTUK 5

Het nationale plan voor Cyberbeveiligingsincidenten en cybercrisisrespons

Art. 29

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 29 wordt eenparig aangenomen.

TITEL 3

Maatregelen voor het beheer van Cyberbeveiligingsrisico's en rapportageverplichtingen

HOOFDSTUK 1

Maatregelen voor het beheer van Cyberbeveiligingsrisico's

Art. 30 tot 33

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 30 tot 32 worden achtereenvolgens eenparig aangenomen.

Artikel 33 wordt aangenomen met 10 stemmen en 3 onthoudingen.

HOOFDSTUK 2

Melding van incidenten

Art. 34 tot 38

Deze artikelen geven geen aanleiding tot opmerkingen.

Artikel 34 wordt aangenomen met 10 stemmen en 3 onthoudingen.

Les articles 35 à 38 sont successivement adoptés à l'unanimité.

TITRE 4

Supervision et sanctions

CHAPITRE 1ER

Supervision

Art. 39 à 50

Ces articles ne donnent lieu à aucune observation.

Les articles 39 à 41 sont successivement adoptés par 10 voix et 3 abstentions.

Les articles 42 à 46 sont successivement adoptés à l'unanimité.

L'article 47 est adopté par 10 voix et 3 abstentions.

Les articles 48 et 49 sont successivement adoptés à l'unanimité.

L'article 50 est adopté par 10 voix et 3 abstentions.

CHAPITRE 2

Les mesures et amendes administratives

Art. 51 à 61

Ces articles ne donnent lieu à aucune observation.

Les articles 51 à 61 sont successivement adoptés à l'unanimité.

TITRE 5

Dispositions spécifiques au secteur de l'administration publique

Art. 62 à 65

Ces articles ne donnent lieu à aucune observation.

Les articles 62 à 64 sont successivement adoptés par 10 voix et 3 abstentions.

De artikelen 35 tot 38 worden achtereenvolgens eenparig aangenomen.

TITEL 4

Toezicht en sancties

HOOFDSTUK 1

Toezicht

Art. 39 tot 50

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 39 tot 41 worden achtereenvolgens aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 42 tot 46 worden achtereenvolgens eenparig aangenomen.

Artikel 47 wordt aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 48 en 49 worden achtereenvolgens eenparig aangenomen.

Artikel 50 wordt aangenomen met 10 stemmen en 3 onthoudingen.

HOOFDSTUK 2

De administratieve maatregelen en geldboetes

Art. 51 tot 61

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 51 tot 61 worden achtereenvolgens eenparig aangenomen.

TITEL 5

Specifieke bepalingen voor de overheidssector

Art. 62 tot 65

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 62 tot 64 worden achtereenvolgens aangenomen met 10 stemmen en 3 onthoudingen.

L'article 65 est adopté à l'unanimité.

TITRE 6

Traitement des données à caractère personnel

CHAPITRE 1ER

Principes relatifs au traitement

Art. 66 à 70

Ces articles ne donnent lieu à aucune observation.

Les articles 66 à 70 sont successivement adoptés à l'unanimité.

CHAPITRE 2

Durée de conservation

Art. 71

Cet article ne donne lieu à aucune observation.

L'article 71 est adopté à l'unanimité.

CHAPITRE 3

Limitation des droits des personnes concernées

Art. 72 et 73

Ces articles ne donnent lieu à aucune observation.

Les articles 72 et 73 sont successivement adoptés à l'unanimité.

CHAPITRE 4

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

Art. 74

Cet article ne donne lieu à aucune observation.

L'article 74 est adopté à l'unanimité.

Artikel 65 wordt eenparig aangenomen.

TITEL 6

Verwerking van persoonsgegevens

HOOFDSTUK 1

Beginselen betreffende de verwerking

Art. 66 tot 70

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 66 tot 70 worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 2

Bewaartermijn

Art. 71

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 71 wordt eenparig aangenomen.

HOOFDSTUK 3

Beperking van de rechten van de betrokkenen

Art. 72 en 73

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 72 en 73 worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 4

Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens

Art. 74

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 74 wordt eenparig aangenomen.

TITRE 7

Dispositions finales

CHAPITRE 1ER

Disposition transitoire

Art. 75

Cet article ne donne lieu à aucune observation.

L'article 75 est adopté par 10 voix et 3 abstentions.

CHAPITRE 2

Dispositions modificatives

Art. 76 à 94

Ces articles ne donnent lieu à aucune observation.

Les articles 76 à 87 sont successivement adoptés à l'unanimité.

L'article 88 est adopté par 10 voix et 3 abstentions.

Les articles 89 à 91 sont successivement adoptés à l'unanimité.

L'article 92 est adopté par 10 voix et 3 abstentions.

Les articles 93 et 94 sont successivement adoptés à l'unanimité.

CHAPITRE 3

Disposition abrogatoire

Art. 95

Cet article ne donne lieu à aucune observation.

L'article 95 est adopté à l'unanimité.

TITEL 7

Slotbepalingen

HOOFDSTUK 1

Overgangsbepaling

Art. 75

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 75 wordt aangenomen met 10 stemmen en 3 onthoudingen.

HOOFDSTUK 2

Wijzigingsbepalingen

Art. 76 tot 94

Deze artikelen geven geen aanleiding tot opmerkingen.

De artikelen 76 tot 87 worden achtereenvolgens eenparig aangenomen.

Artikel 88 wordt aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 89 tot 91 worden achtereenvolgens eenparig aangenomen.

Artikel 92 wordt aangenomen met 10 stemmen en 3 onthoudingen.

De artikelen 93 en 94 worden achtereenvolgens eenparig aangenomen.

HOOFDSTUK 3

Opheffingsbepaling

Art. 95

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 95 wordt eenparig aangenomen.

CHAPITRE 4

Entrée en vigueur

Art. 96

Cet article ne donne lieu à aucune observation.

L'article 96 est adopté à l'unanimité.

*
* *

L'ensemble de la proposition de loi, telle qu'elle a été corrigée sur le plan légistique, ainsi que les annexes I et II, sont adoptés, par vote nominatif, par 10 voix et 3 abstentions.

En conséquence, la proposition de loi jointe (DOC 55 2401/001) devient sans objet.

Résultat du vote nominatif:

Ont voté pour:

Ecolo-Groen: Samuel Cogolati, Eva Platteau, Gilles Vanden Burre;

PS: Daniel Senesael, Eric Thiébaut;

MR: Philippe Pivin, Caroline Taquin;

cd&v: Jef Van den Bergh;

Open Vld: Robby De Caluwé;

Vooruit: Meryame Kitir.

Ont voté contre: nihil.

Se sont abstenus:

N-VA: Yngvild Ingels;

VB: Ortwin Depoortere, Barbara Pas.

Le rapporteur, *Le président,*

Daniel Senesael Ortwin Depoortere

HOOFDSTUK 4

Inwerkingtreding

Art. 96

Dit artikel geeft geen aanleiding tot opmerkingen.

Artikel 96 wordt eenparig aangenomen.

*
* *

Het gehele, wetgevingstechnisch verbeterde wetsvoorstel, alsook de bijlagen I en II, worden bij naamstemming aangenomen met 10 stemmen en 3 onthoudingen.

Bijgevolg vervalt het toegevoegde wetsvoorstel DOC 55 2401/001.

De naamstemming is als volgt:

Hebben voorgestemd:

Ecolo-Groen: Samuel Cogolati, Eva Platteau, Gilles Vanden Burre;

PS: Daniel Senesael, Eric Thiébaut;

MR: Philippe Pivin, Caroline Taquin;

cd&v: Jef Van den Bergh;

Open Vld: Robby De Caluwé;

Vooruit: Meryame Kitir.

Hebben tegengestemd: nihil.

Hebben zich onthouden:

N-VA: Yngvild Ingels;

VB: Ortwin Depoortere, Barbara Pas.

De rapporteur, *De voorzitter,*

Daniel Senesael Ortwin Depoortere

Dispositions nécessitant une mesure d'exécution (article 78.2, alinéa 4 du Règlement):

— Art. 3, § 2, alinéa 3, et § 6;
— Art. 7, 1° et 2°;
— Art. 11, § 5;
— Art. 13, § 1er, alinéa 2;
— Art. 14, §3;
— Art. 15, § 1er, § 2, alinéa 1er et 3;
— Art. 17, 12°;
— Art. 19, § 1er, alinéa 2;
— Art. 29, § 1er;
— Art. 33;
— Art. 34, § 3;
— Art. 39, alinéa 1er;
— Art. 40, § 1er, alinéa 1er;
— Art. 41;
— Art. 47, § 1er et § 3, alinéa 3;
— Art. 50, § 2, alinéa 2;
— Art. 63, § 1er et § 2, alinéa 1er;
— Art. 75;
— Art. 77 ;
— Art. 88;
— Art. 94 (ancien art. 92).

Bepalingen die een uitvoeringsmaatregel vereisen (artikel 78.2, vierde lid van het Reglement):

— Art. 3, § 2, derde lid, en § 6;
— Art. 7, 1° en 2°;
— Art. 11, § 5;
— Art. 13, § 1er, tweede lid;
— Art. 14, §3;
— Art. 15, § 1er, § 2, eerste en derde lid;
— Art. 17, 12°;
— Art. 19, § 1er, tweede lid;
— Art. 29, § 1er ;
— Art. 33;
— Art. 34, § 3;
— Art. 39, eerste lid;
— Art. 40, § 1er, eerste lid;
— Art. 41;
— Art. 47, § 1er en § 3, derde lid;
— Art. 50, § 2, tweede lid;
— Art. 63, § 1er en § 2, eerste lid;
— Art. 75;
— Art. 77;
— Art. 88;
— Art. 94 (vroeger art. 92).

Imprimerie centrale – Centrale drukkerij