CRABV 55 **COM 964**

DE KAMER BE
LA CHAMBRE BE

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

COMPTE RENDU ANALYTIQUE

BEKNOPT VERSLAG

COMMISSIONS RÉUNIES DE L'INTÉRIEUR, DE LA SÉCURITÉ, DE LA MIGATION ET DES MATIÈRES ADMINISTRATIVES ET DE LA DÉFENSE

VERENIGDE COMMISSIES VOOR BINNENLANDSE ZAKEN, VEILIGHEID, MIGRATIE EN BESTUURSZAKEN EN VOOR LANDSVERDEDIGING

Mercredi

18-01-2023

Après-midi

Woensdag

18-01-2023

Namiddag

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 :		*Afkortingen bij de nummering van de publicaties* :	
DOC 55 0000/000	*Document parlementaire de la 55e législature, suivi du n° de base et du n° consécutif*	*DOC 55 0000/000*	*Parlementair stuk 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 définitif 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 (op beigekleurig papier)*

Publications officielles éditées par la Chambre des représentants
Commandes :
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
e-mail : publications@lachambre.be

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers
Bestellingen :
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

SOMMAIRE

Échange de vues sur la protection des infrastructures critiques et questions jointes de 1

- Daniel Senesael à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La Direction de la sécurisation (DAB) et les infrastructures critiques" (55033224C) 1

- Franky Demon à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "Les infrastructures critiques" (55033233C) 1

- Franky Demon à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La reconnaissance des centres de distribution des supermarchés comme infrastructures critiques" (55033234C) 1

- Kris Verduyckt à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La protection des infrastructures critiques" (55033235C) 1

- Kris Verduyckt à Ludivine Dedonder (Défense) sur "La protection des infrastructures critiques" (55033236C) 1

- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La sécurisation des infrastructures critiques (secteurs du transport, de l'énergie et de l'eau)" (55033239C) 1

- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "Les infrastructures critiques (réseaux informatiques, santé, prisons et stockage d'armements)" (55033240C) 1

- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La sécurité des infrastructures critiques (DAB, incidents, intrusions et évaluation globale)" (55033241C) 2

Orateurs: **Annelies Verlinden**, ministre de l'Intérieur, des Réformes institutionnelles et du Renouveau démocratique**, Ludivine Dedonder**, ministre de la Défense**, Yngvild Ingels, Éric Thiébaut, Steven Creyelman, Philippe Pivin, Franky Demon, Tim Vandenput, Kris Verduyckt, Theo Francken**

INHOUD

Gedachtewisseling over de bescherming van de kritieke infrastructuren en toegevoegde vragen van 1

- Daniel Senesael aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De Directie beveiliging (DAB) en de kritieke infrastructuur" (55033224C) 1

- Franky Demon aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De kritieke infrastructuren" (55033233C) 1

- Franky Demon aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De erkenning van de distributiecentra van supermarkten als kritieke infrastructuren" (55033234C) 1

- Kris Verduyckt aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De bescherming van de kritieke infrastructuren" (55033235C) 1

- Kris Verduyckt aan Ludivine Dedonder (Defensie) over "De bescherming van de kritieke infrastructuren" (55033236C) 1

- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De beveiliging van de kritieke infrastructuur (transport, energie en water)" (55033239C) 1

- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De kritieke infrastructuur (IT, gezondheidszorg, gevangenissen en wapenopslag)" (55033240C) 2

- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De beveiliging van de kritieke infrastructuur (DAB, incidenten, intrusies en globale evaluatie)" (55033241C) 2

Sprekers: **Annelies Verlinden**, minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische vernieuwing**, Ludivine Dedonder**, minister van Defensie**, Yngvild Ingels, Éric Thiébaut, Steven Creyelman, Philippe Pivin, Franky Demon, Tim Vandenput, Kris Verduyckt, Theo**

Francken

COMMISSIONS REUNIES DE L'INTERIEUR, DE LA SECURITE, DE LA MIGATION ET DES MATIERES ADMINISTRATIVES ET DE LA DEFENSE

du

MERCREDI 18 JANVIER 2023

Après-midi

_____

VERENIGDE COMMISSIES VOOR BINNENLANDSE ZAKEN, VEILIGHEID, MIGRATIE EN BESTUURSZAKEN EN VOOR LANDSVERDEDIGING

van

WOENSDAG 18 JANUARI 2023

Namiddag

_____

La réunion publique de commission est ouverte à 14 h 06 par MM. Peter Buysrogge et Ortwin Depoortere, présidents.

Le texte en italiques est un résumé de la question préalablement déposée.

01 Échange de vues sur la protection des infrastructures critiques et questions jointes de
- Daniel Senesael à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La Direction de la sécurisation (DAB) et les infrastructures critiques" (55033224C)
- Franky Demon à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "Les infrastructures critiques" (55033233C)
- Franky Demon à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La reconnaissance des centres de distribution des supermarchés comme infrastructures critiques" (55033234C)
- Kris Verduyckt à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La protection des infrastructures critiques" (55033235C)
- Kris Verduyckt à Ludivine Dedonder (Défense) sur "La protection des infrastructures critiques" (55033236C)
- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La sécurisation des infrastructures critiques (secteurs du transport, de l'énergie et de l'eau)" (55033239C)
- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "Les infrastructures critiques (réseaux informatiques, santé, prisons et stockage

De openbare commissievergadering wordt geopend om 14.06 uur en voorgezeten door de heren Peter Buysrogge en Ortwin Depoortere.

De cursieve tekst is een samenvatting van de tekst die de vraagsteller vooraf heeft ingediend.

01 Gedachtewisseling over de bescherming van de kritieke infrastructuren en toegevoegde vragen van
- Daniel Senesael aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De Directie beveiliging (DAB) en de kritieke infrastructuur" (55033224C)
- Franky Demon aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De kritieke infrastructuren" (55033233C)
- Franky Demon aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De erkenning van de distributiecentra van supermarkten als kritieke infrastructuren" (55033234C)
- Kris Verduyckt aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De bescherming van de kritieke infrastructuren" (55033235C)
- Kris Verduyckt aan Ludivine Dedonder (Defensie) over "De bescherming van de kritieke infrastructuren" (55033236C)
- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De beveiliging van de kritieke

d'armements)" (55033240C)
- Philippe Pivin à Annelies Verlinden (Intérieur, Réformes instit. et Renouveau démocratique) sur "La sécurité des infrastructures critiques (DAB, incidents, intrusions et évaluation globale)" (55033241C)

01.01 **Annelies Verlinden**, ministre *(en néerlandais)*: Je vais à présent vous exposer les actions prises par les services de l'Intérieur à la suite des fuites sur les gazoducs Nord Stream 1 et 2.

(En français) Conformément à la loi du 1er juillet 2011 sur la sécurité et protection des infrastructures critiques, le Centre de crise coordonne la politique nationale en cette matière. Les infrastructures critiques, au sein des secteurs critiques définis dans cette loi, doivent être identifiées formellement par les autorités sectorielles après analyse et en concertation avec le Centre de crise. Celles-ci doivent inspecter les plans et mesures de sécurité de l'exploitant. Ces obligations visent la sécurité interne et la protection externe.

(En néerlandais) L'exploitant d'une infrastructure critique procède à une analyse des risques et établit, sur la base de cette analyse, un plan de sécurité, le P.S.E.. Il existe des mesures de sécurité permanentes et graduelles. Ces dernières sont activées lorsque l'OCAM identifie une menace accrue. L'exploitant doit effectuer des exercices de sécurité et maintenir le P.S.E. à jour.

L'autorité sectorielle doit mettre à jour la liste des infrastructures critiques au moins tous les cinq ans. Une telle révision a eu lieu au cours du premier semestre 2022 pour le secteur des télécommunications et de l'énergie.

L'OCAM élabore des analyses stratégiques des menaces par sous-secteur ou secteur et effectue ces analyses au moins tous les cinq ans. Cette analyse porte sur la menace de l'extrémisme, du terrorisme, de l'activisme, de l'espionnage, de l'ingérence et du crime organisé. En se basant sur les scénarios de menace les plus plausibles proposés par l'OCAM, l'opérateur peut optimiser le

infrastructuur (transport, energie en water)" (55033239C)
- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De kritieke infrastructuur (IT, gezondheidszorg, gevangenissen en wapenopslag)" (55033240C)
- Philippe Pivin aan Annelies Verlinden (Binnenlandse Zaken en Institutionele Hervormingen en Democratische Vernieuwing) over "De beveiliging van de kritieke infrastructuur (DAB, incidenten, intrusies en globale evaluatie)" (55033241C)

01.01 Minister **Annelies Verlinden** *(Nederlands)*: Ik zal de acties door de diensten van Binnenlandse Zaken naar aanleiding van de lekken in Nord Stream 1 en 2 toelichten.

(Frans) Overeenkomstig de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren coördineert het Nationaal Crisiscentrum het beleid op dat vlak. De kritieke infrastructuur, in de in deze wet gedefinieerde kritieke sectoren, moet formeel door de sectorale overheden worden geïdentificeerd, na analyse en in overleg met het Nationaal Crisiscentrum. Zij moeten de beveiligingsplannen en –maatregelen van de exploitant inspecteren. Die verplichtingen hebben betrekking op de interne beveiliging en de externe bescherming.

(Nederlands) De exploitant van kritieke infrastructuur voert een risicoanalyse uit en stelt op basis daarvan een beveiligingsplan op, het B.P.E. Er zijn zowel permanente als graduele beveiligingsmaatregelen. Die laatste worden geactiveerd wanneer het OCAD een verhoogde dreiging vaststelt. De exploitant moet veiligheidsoefeningen houden en het B.P.E. actueel houden.

De sectorale overheid moet minstens om de vijf jaar de lijst met kritieke infrastructuren actualiseren. In de eerste helft van 2022 vond een herziening plaats van de telecommunicatie- en de energiesector.

Het OCAD stelt strategische dreigingsanalyses op per subsector of sector en voert de analyses minstens elke vijf jaar uit. Men kijkt naar de dreiging van extremisme, terrorisme, activisme, spionage, inmenging en georganiseerde misdaad. Op basis van de meest plausibele dreigingsscenario's die het OCAD naar voren schuift, kan de exploitant het B.P.E. optimaliseren. De exploitant moet 24/7 een

P.S.E.. L'opérateur doit disposer d'un point de contact pour la sécurité 24 heures sur 24 et 7 jours sur 7 pour communiquer avec l'autorité sectorielle, le Centre de crise et la police.

beveiligingscontactpunt hebben voor communicatie met de sectorale overheid, het Crisiscentrum en de politie.

(En français) Selon la directive ministérielle MFO-5, le Centre de crise impose les mesures de protection externe des infrastructures critiques sur la base d'une menace accrue concrète. Pour déterminer ces mesures, le Centre de crise utilise divers outils et l'expertise de différents services partenaires, notamment les analyses de l'OCAM. Des évaluations régulières sont demandées pour les infrastructures critiques et sensibles, mais également à la suite d'incidents survenus en Belgique et à l'étranger. Ensuite, le Centre de crise réalise des analyses de risque qui définissent les mesures de protection, notamment policières.

(Frans) Conform de ministeriële richtlijn MFO-5, baseert het Nationaal Crisiscentrum zich op een concrete verhoogde dreiging om de maatregelen voor de externe bescherming van de kritieke infrastructuur op te leggen. Voor de bepaling van die maatregelen gebruikt het Nationaal Crisiscentrum verscheidene tools en doet het een beroep op de expertise van verschillende partnerdiensten, met name op de analyses van het OCAD. Er worden regelmatige evaluaties gevraagd met betrekking tot de kritieke en gevoelige infrastructuur, maar ook naar aanleiding van incidenten die zich in België of in het buitenland voorgedaan hebben. Vervolgens voert het Nationaal Crisiscentrum risicoanalyses uit die bepalen welke beschermingsmaatregelen, en meer bepaald welke politiemaatregelen er genomen worden.

Lorsqu'un incident grave se produit, le Centre de crise organise une réunion de coordination avec tous les services concernés pour dresser un état des lieux et définir des mesures de protection. Le Centre de crise peut imposer certaines mesures. Les services partenaires peuvent aussi en proposer.

Wanneer er zich een ernstig incident voordoet, organiseert het Nationaal Crisiscentrum een coördinatievergadering met alle betrokken diensten om een stand van zaken op te maken en beschermingsmaatregelen vast te stellen. Het Nationaal Crisiscentrum kan bepaalde maatregelen opleggen. De partnerdiensten kunnen eveneens maatregelen voorstellen.

(En néerlandais) La situation en Ukraine reste dramatique. Aujourd'hui, le ministre de l'Intérieur ukrainien est décédé dans un accident d'hélicoptère. À la suite du déclenchement de la guerre en Ukraine, le Conseil national de sécurité a élargi l'année dernière le mandat de l'OCAM aux menaces interétatiques. Le Comité de coordination du renseignement et de la sécurité (CCRS) poursuit ce travail.

(Nederlands) De situatie in Oekraïne blijft dramatisch. Vandaag nog is de Oekraïense minister van Binnenlandse Zaken omgekomen bij een helikoptercrash. Naar aanleiding van de oorlog in Oekraïne heeft de Nationale Veiligheidsraad vorig jaar het mandaat van het OCAD uitgebreid naar dreigingen die interstatelijk kunnen zijn. Het Coördinatiecomité voor Inlichtingen en Veiligheid (CCIV) werkt dit verder uit.

En septembre 2022, des fuites ont été constatées sur les gazoducs Nord Stream 1 et 2. Les compétences de l'Intérieur concernant l'approvisionnement en gaz sont limitées. Le Centre de crise a immédiatement pris contact avec la direction générale Énergie du SPF Économie. Les fuites n'ont pas de répercussions directes sur la sécurité d'approvisionnement de l'Union européenne. Nord Stream 2 n'a jamais été mis en service, et Nord Stream 1 n'achemine plus aucun volume depuis le 31 août 2022.

In september 2022 waren er lekken in de pijpleidingen Nord Stream 1 en 2. De bevoegdheden van Binnenlandse Zaken inzake gasbevoorrading zijn beperkt. Het Crisiscentrum heeft meteen contact opgenomen met de algemene directie Energie van de FOD Economie. De lekken hebben geen onmiddellijke impact op de bevoorradingszekerheid van de EU. Nord Stream 2 is nooit in gebruik genomen en sinds 31 augustus 2022 werden er geen volumes meer doorgevoerd via Nord Stream 1.

Le Centre de crise a demandé à l'OCAM de procéder à une évaluation de la menace interétatique pour les infrastructures gazières belges. La situation a été discutée à plusieurs

Het Crisiscentrum heeft aan het OCAD een evaluatie gevraagd van de interstatelijke dreiging voor de Belgische gasinfrastructuur. De situatie is meermaals besproken met de partnerdiensten,

reprises avec les services partenaires, tels que les services de renseignements et l'OCAM. Un avertissement a été envoyé aux exploitants d'infrastructures critiques, qui ont été priés de continuer à assurer la fourniture, de faire preuve d'une vigilance accrue et de respecter scrupuleusement les mesures. Les services de renseignements et de sécurité ont mis à jour les niveaux de menace. Il n'y avait pas lieu de relever ces niveaux.

zoals de inlichtingendiensten en het OCAD. Naar de exploitanten van kritieke infrastructuur is een waarschuwing verstuurd met de vraag om de levering te blijven verzekeren, extra waakzaam te zijn en de maatregelen strikt na te leven. De inlichtingen- en veiligheidsdiensten hebben de dreigingsniveaus geüpdatet. Er was geen aanleiding tot een verhoging van de niveaus.

01.02 **Ludivine Dedonder**, ministre *(en néerlandais)*: Nos infrastructures critiques, qui sont définies par la loi, doivent être protégées car elles sont essentielles à notre vie quotidienne et à notre économie. Il en va de notre sécurité et de notre prospérité.

01.02 Minister **Ludivine Dedonder** *(Nederlands)*: Onze kritieke infrastructuren, die bij wet zijn gedefinieerd, moeten worden beschermd, want ze zijn essentieel voor ons dagelijks leven en onze economie. Het gaat over onze veiligheid en onze welvaart.

(En français) Ces infrastructures sont de plus en plus exposées aux menaces de perturbation et aux cyberattaques, au terrorisme ou au sabotage. Outre les cyberattaques contre des services de l'État ou des hôpitaux en Belgique, il y a eu le sabotage des gazoducs Nordstream en septembre en mer Baltique.

(Frans) De dreiging van een verstoring van de werking ervan, van een cyberaanval, terreuraanslag of sabotage wordt steeds groter voor die infrastructuur. Naast de cyberaanvallen tegen overheidsdiensten of ziekenhuizen in België was er in september de sabotage van de Nord Streamgaspijpleiding in de Oostzee.

(En néerlandais) Les atteintes portées à nos infrastructures critiques peuvent avoir des répercussions graves et de longue durée. Raison pour laquelle nous devons encore mieux les protéger afin d'éviter un impact majeur dans notre pays, voire dans les pays qui nous entourent.

(Nederlands) Aantastingen aan onze kritieke infrastructuur kunnen ernstige en langdurige gevolgen hebben. Daarom moeten we ze nog beter beschermen, opdat we een grote impact in ons land en mogelijk zelfs in onze buurlanden kunnen vermijden.

Au sein de la Défense, le Service Général du Renseignement et de la Sécurité (SGRS) est responsable, en coordination avec l'État-major de la Défense, de la surveillance des infrastructures critiques qui font partie de son patrimoine.

Bij Defensie is de Algemene Dienst Inlichting en Veiligheid (ADIV), in coördinatie met de Defensiestaf, verantwoordelijk voor het toezicht op de kritieke infrastructuur in zijn patrimonium.

(En français) La protection des infrastructures critiques incombe avant tout aux propriétaires et exploitants, surtout en haute mer, mais la Défense peut venir en appui avec certaines capacités si les services civils le demandent. Les capacités duales, assurées par le plan STAR et la loi de programmation militaire 2023-2030, concernent la marine, le cyber et la *Belgian pipeline organisation*. La Défense met à profit son expertise lors d'incidents, menaces ou attaques chimiques, biologiques, radiologiques ou nucléaires (CBRN) et intervient dans des missions de police aérienne.

(Frans) De bescherming van de kritieke infrastructuur is eerst en vooral de taak van de eigenaars en exploitanten, vooral in volle zee, maar Defensie kan met bepaalde capaciteiten bijstand verlenen als de civiele diensten daarom vragen. De duale capaciteiten, die vastgelegd zijn in het STAR-plan en de wet houdende de militaire programmering 2023-2030, betreffen de marine, de cybercomponent en de Belgian Pipeline Organisation. Defensie wendt haar expertise aan bij chemische, biologische, radiologische of nucleaire (CBRN) incidenten, dreigingen en aanvallen, en treedt op in het kader van luchtruimbewakingsopdrachten.

(En néerlandais) La Défense participe ainsi au renforcement de la sécurisation de nos infrastructures critiques. À cet effet, nous investissons dans les technologies de sécurité,

(Nederlands) Zo draagt Defensie bij aan een sterkere beveiliging van onze kritieke infrastructuur. Daarvoor investeren we in veiligheidstechnologie, vormen we het personeel en werken we samen met

nous formons le personnel et nous collaborons avec d'autres départements. La collaboration étroite avec nos partenaires stratégiques de l'UE et de l'OTAN nous permet de renforcer la capacité de la Défense afin de réagir rapidement et efficacement aux menaces éventuelles.

01.03 **Yngvild Ingels** (N-VA): Par "menaces sur nos infrastructures critiques", l'on vise souvent les actes de sabotage, mais d'autres risques existent. En effet, les infrastructures peuvent être touchées par des catastrophes naturelles telles qu'une inondation ou un tremblement de terre. J'ai le souvenir que des infrastructures énergétiques critiques sont situées non seulement en zone inondable, mais également sous une zone d'atterrissage d'avions à proximité de l'aéroport de Zaventem. Ces différents risques sont-ils tous répertoriés?

La présidente de la Commission européenne, Ursula von der Leyen, a indiqué que des satellites pouvaient également être déployés pour assurer un meilleur suivi dans des cas tels que celui des gazoducs Nord Stream. Ce déploiement serait coordonné avec l'OTAN. La Belgique y participerait-elle?

Le premier ministre a annoncé qu'un budget annuel de 1,2 million d'euros serait débloqué pour mieux armer la Belgique contre des attaques et des cyberattaques visant notre infrastructure énergétique critique. Dix-huit spécialistes devaient également être recrutés à cet effet. Comment cet argent a-t-il été utilisé? Ces spécialistes ont-ils déjà été engagés? De quelles infrastructures s'agit-il précisément? Des efforts comparables sont-ils effectués dans d'autres secteurs?

Une approche par secteur impliquant une responsabilité sectorielle constitue la bonne méthode de travail, mais il ne faut pas pour autant perdre de vue les influences intersectorielles. Quelqu'un doit garantir une vision d'ensemble.

De quelle manière la Direction de la sécurisation (DAB) est-elle mobilisée dans la surveillance d'infrastructures critiques? S'agit-il de surveillances permanentes?

01.04 **Éric Thiébaut** (PS): Madame la ministre, votre note de politique générale indique que les effectifs de la DAB seront étoffés ces prochains mois. Vu les 1 343 agents engagés en 2022 (sur les 1 600 initialement prévus), il y a un déficit de 250 ETP, alors que les missions de sécurisation de ce corps s'intensifient, notamment pour le procès des attentats.

andere departementen. Door nauw samen te werken met onze strategische partners in de EU en de NAVO versterken we het vermogen van Defensie om bij mogelijke dreigingen snel en effectief te reageren.

01.03 **Yngvild Ingels** (N-VA): Bij dreigingen voor onze kritieke infrastructuur spreken we vaak over sabotage, maar daarnaast zijn er nog andere risico's. Zo kan infrastructuur ook uitvallen bij een calamiteit zoals een overstroming of een aardbeving. Ik herinner mij dat kritieke energie-infrastructuur niet alleen in een overstromingsgebied is gelegen, maar ook nog eens onder een landingszone voor vliegtuigen vlakbij de luchthaven van Zaventem. Worden al die verschillende risico's in kaart gebracht?

Commissievoorzitster von der Leyen heeft aangegeven dat ook satellieten kunnen worden ingezet om zaken zoals de Nord Stream-pijpleiding beter op te volgen. Dat zou gebeuren in coördinatie met de NAVO. Neemt België daaraan ook deel?

De premier heeft aangekondigd dat er jaarlijks 1,2 miljoen euro zal worden vrijgemaakt om België beter te wapenen tegen aanvallen en cyberaanvallen op onze kritieke energie-infrastructuur. Daarvoor zouden ook achttien specialisten worden aangeworven. Wat is er met die centen gebeurd? Zijn die specialisten al aangeworven? Over welke infrastructuur gaat het precies? Worden er gelijkaardige inspanningen gedaan voor andere sectoren?

Een aanpak op sectorniveau, met een sectorale verantwoordelijkheid, is de juiste manier van werken, maar daarnaast moeten we ook oog hebben voor intersectorale invloeden. Iemand moet het overzicht bewaren.

Op welke manier wordt de Directie beveiliging (DAB) ingezet voor de bewaking van kritieke infrastructuur? Gaat het om permanente bewakingen?

01.04 **Éric Thiébaut** (PS): Mevrouw de minister, in uw beleidsnota staat te lezen dat de DAB de komende maanden versterkt zal worden. In 2022 werden er 1.343 agenten aangeworven (van de 1.600 zoals oorspronkelijk gepland); er is dus nog een tekort van 250 vte's, terwijl dit korps steeds meer beveiligingsopdrachten krijgt, onder meer op het proces over de aanslagen.

Votre note réaffirme aussi la reprise de missions, précédemment assumées par la Défense, de sécurisation de sites nucléaires en Flandre (Doel, Mol, Geel, etc.) dès ce 1er janvier.

In uw nota lezen we ook dat de DAB de beveiliging van nucleaire sites in Vlaanderen (Doel, Mol, Geel, enz.) sinds 1 januari overgenomen heeft van Defensie.

Quels sont vos objectifs d'augmentation d'effectifs de la DAB pour 2023? Comment y arriverez-vous? Qu'en est-il de la concertation sociale? Quelle est la répartition des effectifs mis à disposition de la DAB pour sécuriser les sites nucléaires? Quels sont les effectifs dédiés à la sécurisation des procès des attentats? La DAB sera-t-elle déployée pour la protection d'autres infrastructures critiques? Si oui, lesquelles? Un renforcement des missions et formations de la DAB dans la protection de ces dernières est-il à l'ordre du jour?

Wat zijn uw doelstellingen met betrekking tot de verhoging van de personeelssterkte van de DAB voor 2023? Hoe denkt u die doelen te bereiken? Hoe staat het met het sociaal overleg? Wat is de verdeling van het DAB-personeel voor de beveiliging van de nucleaire sites? Hoeveel manschappen worden er ingezet voor de beveiliging op het proces over de aanslagen? Zal de DAB ingezet worden voor de bescherming van andere kritieke infrastructuur? Zo ja, welke? Is een uitbreiding van de opdrachten en opleidingen van de DAB inzake de beveiliging van de kritieke infrastructuur aan de orde?

01.05 **Steven Creyelman** (VB): Quelles infrastructures sont-elles considérées comme critiques sur le plan matériel et immatériel? Existe-t-il une liste claire? Est-elle dynamique et régulièrement mise à jour? Quels paramètres sont-ils utilisés pour décider de l'ajout ou de la suppression d'une infrastructure? De quelle manière les services publics de l'Intérieur et de la Défense collaborent-ils pour garantir notre sécurité?

01.05 **Steven Creyelman** (VB): Wat wordt beschouwd als kritieke infrastructuur op materieel en immaterieel vlak? Bestaat er een duidelijke lijst? Is die dynamisch? Wordt die regelmatig bijgewerkt? Welke parameters worden er gebruikt om bepaalde infrastructuur toe te voegen of te schrappen? Hoe werken de overheidsdiensten van Binnenlandse Zaken en Defensie samen om onze veiligheid te garanderen?

Quels efforts sont-ils fournis pour améliorer la cybersécurité? Une série de cyberattaques de grande ampleur ont été commises en 2022, notamment par des pirates chinois. Notre pays a appelé la Chine à prendre des mesures appropriées. N'est-ce pas un peu naïf? L'État chinois a commandité ces attaques. Pourquoi prendrait-il des mesures contre ses propres pirates informatiques? Les instances chinoises ont-elles déjà réagi? Entre-temps, avons-nous pris des mesures pour mieux sécuriser notre infrastructure? Les mesures de sécurité existantes sont-elles suffisantes?

Welke inspanningen worden er geleverd om de cyberveiligheid te vergroten? In 2022 waren er een aantal grootschalige cyberaanvallen, onder meer door Chinese hackers. Ons land riep China op om gepaste maatregelen te nemen. Is dat niet een beetje naïef? De Chinese overheid is de opdrachtgever. Waarom zou ze maatregelen nemen tegen haar eigen hackers? Hebben de Chinese instanties al gereageerd? Hebben wij ondertussen maatregelen genomen om onze infrastructuur beter te beveiligen? Zijn de huidige veiligheidsmaatregelen voldoende?

Le débat sur le traitement judiciaire des cyberattaques doit encore être mené, y compris au niveau international. Ce nouveau type de guerre hybride doit-il être considéré comme une attaque armée légitimant une réaction d'autodéfense? Une cyberattaque doit être suivie d'une réaction ferme. Nous devons disposer non seulement d'une capacité défensive, mais également d'une capacité offensive. Nous devons pouvoir réagir à armes égales. Pour cela, nous devons toutefois savoir d'où provient la cyberattaque. Il est difficile de prouver qu'un pays est à l'origine d'une cyberattaque. Où en est le déploiement de la procédure d'attribution des cyberattaques? Quels paramètres sont pris en

Het debat over de gerechtelijke behandeling van cyberaanvallen moet nog gevoerd worden, ook op internationaal niveau. Moet dit soort van hybride oorlogsvoering als een gewapende aanval worden beschouwd, waarna een reactie van zelfverdediging gewettigd is? Een cyberaanval moet krachtdadig worden beantwoord. We moeten niet alleen over defensieve capaciteit beschikken, maar ook over een offensieve. We moeten met gelijke wapens kunnen reageren. Dan moeten we wel weten uit welke hoek de cyberaanval komt. Het is moeilijk te bewijzen dat een land achter een cyberaanval zit. Hoe staat het met de uitrol van de toewijzingsprocedure voor cyberaanvallen? Welke

considération pour l'attribution des cyberattaques? Où en est le développement de la composante Cyber? Parvient-on à attirer suffisamment d'informaticiens qualifiés?

Où en est la sécurité de nos infrastructures énergétiques? Des mesures de sécurité supplémentaires ont-elles été prises après le sabotage du gazoduc Nord Stream?

À la suite d'une cyberattaque, la ville d'Anvers a dû subir une sorte de lockdown numérique. Il faudrait encore attendre la fin de ce mois pour que tout rentre dans l'ordre. Quelle a été la collaboration entre la ville et l'État fédéral? Une concertation a-t-elle lieu entre les différents niveaux de pouvoir en cas de cyberattaque de ce genre? Existe-t-il une feuille de route concernant la protection d'infrastructures critiques contre des cyberattaques qui serait également destinée aux pouvoirs locaux? Un accompagnement structurel est-il prévu? Existe-t-il des analyses d'impact par secteur et des plans de continuité qui permettent de répertorier les processus critiques?

Existe-t-il un plan de communication qui définit ce qui doit être communiqué en cas de calamité, quand, comment, par qui et à qui? Si nous identifions à l'avance les groupes cibles, les canaux de communication et les messages, nous pouvons élaborer une communication de crise solide. S'y attelle-t-on?

01.06 **Philippe Pivin** (MR): *Quelles mesures et investissements nouveaux ont-ils été décidés pour protéger les systèmes des opérateurs des services essentiels du pays et des infrastructures critiques comme les établissements hospitaliers? Quelles sont les normes pour la protection des données médicales et des systèmes informatiques de ces établissements? Quel soutien apporte-t-on aux hôpitaux à cet effet?*

Alors que le serveur central du SPF Intérieur a été piraté, il y a deux ans, quelles sont les mesures des systèmes numériques gérant les données et les espaces internes des prisons? Comment détermine-t-on les infrastructures critiques parmi les lieux de justice et comment les sécurise-t-on?

Comment sont sécurisés les stocks d'armements de la police et de la Défense? Quelles sont les mesures nouvelles en la matière? Comment évalue-t-on les systèmes de sécurité de ces infrastructures?

parameters worden overwogen voor de attributie van cyberaanvallen? Hoe staat het met de uitbouw van de cybercomponent? Kunnen er voldoende bekwame IT'ers worden aangetrokken?

Hoe staat het met de veiligheid van onze energie-infrastructuur? Zijn er extra beveiligingsmaatregelen getroffen na de sabotage van de Nord Stream-pijpleiding?

Na de cyberaanval is de stad Antwerpen in een soort digitale lockdown moeten gaan. Het zou nog tot het eind van deze maand duren om alle gevolgen ervan weg te werken. Welke samenwerking was er tussen de stad en de federale overheid? Is er overleg tussen de verschillende beleidsniveaus bij dit soort cyberaanvallen? Is er een draaiboek voor de bescherming van kritieke infrastructuur tegen cyberaanvallen, ook voor lokale en lagere overheden? Is er structurele begeleiding? Bestaan er impactanalyses per sector? Zijn er continuïteitsplannen waarmee kritieke processen in kaart kunnen worden gebracht?

Is er een communicatieplan dat bepaalt wat, wanneer, hoe, door wie en aan wie er wordt gecommuniceerd in het geval van calamiteiten? Als we de doelgroepen, communicatiekanalen en boodschappen op voorhand in kaart brengen, kunnen we een sterke crisiscommunicatie ontwikkelen. Wordt daar aan gewerkt?

01.06 **Philippe Pivin** (MR): *Welke nieuwe maatregelen en investeringen werden er vastgesteld om de systemen van de operatoren van de essentiële diensten van het land en van de kritieke infrastructuur, zoals ziekenhuisvoorzieningen, te beschermen? Wat zijn de normen voor de bescherming van de medische gegevens en van de computersystemen van deze voorzieningen? Welke ondersteuning krijgen de ziekenhuizen in dat kader?*

Twee jaar geleden werd de centrale server van de FOD Binnenlandse Zaken gehackt. Welke beschermingsmaatregelen zijn er van toepassing op de digitale systemen die de gegevens en de binnenruimten van de gevangenissen beheren? Hoe bepaalt men welke justitieplaatsen tot de kritieke infrastructuur behoren en hoe beveiligt men die?

Hoe worden de wapenvoorraden van de politie en van Defensie beveiligd? Welke nieuwe maatregelen zijn er ter zake van kracht? Hoe evalueert men de systemen voor de beveiliging van die infrastructuur?

Des rapports du Centre pour la Cybersécurité concluent-ils à la nécessité de consacrer des moyens supplémentaires à certains lieux? Quelles sont les mesures pour 2023 et 2024?

Wordt er in de verslagen van het Centrum voor Cybersecurity België de conclusie getrokken dat er extra middelen besteed moeten worden aan de beveiliging van bepaalde plaatsen? Wat zijn de maatregelen voor 2023 en 2024?

Combien le Centre de crise a-t-il reçu de signalements d'incidents ces trois dernières années, pour quelles infrastructures et quelles atteintes ou menaces? Combien d'intrusions physiques a-t-on constatées dans les infrastructures critiques depuis 2019? Quelles infrastructures en ont-elles été victimes?

Hoeveel meldingen van incidenten ontving het Nationaal Crisiscentrum de voorbije drie jaar, voor welke infrastructuur en voor welke inbreuken of dreigingen? Hoeveel fysieke inbraken in kritieke infrastructuur werden er sinds 2019 vastgesteld? Welke infrastructuur was daarvan het doelwit?

Combien de piratages a-t-on décelés dans les systèmes numériques des services essentiels et des infrastructures critiques depuis 2019? Combien d'opérateurs le Centre pour la Cybersécurité a-t-il identifiés?

Hoeveel hackings van de computersystemen van de essentiële diensten en van de kritieke infrastructuur kwam men sinds 2019 op het spoor? Hoeveel operatoren heeft het Centrum voor Cybersecurity België geïdentificeerd?

Quels lieux stratégiques sont sécurisés par la DAB? Quel est l'effectif chargé de sécuriser les infrastructures critiques? Comment a-t-il évolué depuis 2019? Quels services et infrastructures sont-ils sécurisés par des sociétés privées de gardiennage? Quelle est la régularité du screening des agents y travaillant?

Welke strategische plaatsen worden door de DAB beveiligd? Hoeveel personeelsleden zijn er belast met de beveiliging van de kritieke infrastructuur? Hoe is dat personeelsbestand sinds 2019 geëvolueerd? Welke diensten en infrastructuur worden door privébewakingsfirma's beveiligd? Met welke regelmaat worden de bewakingsagenten die voor die firma's werken gescreend?

Quelles autorités sectorielles ont-elles déterminé des nouvelles mesures internes de protection et quelles infrastructures ont-elles été désignées critiques depuis 2019?

Welke sectorale overheden hebben nieuwe interne beschermingsmaatregelen bepaald en welke infrastructuur werd sinds 2019 als kritiek bestempeld?

Quels ont été les risques liés au changement climatique et en particulier d'inondations, analysés par les experts sur la période 2018-2023? Quel est le nouveau Belgian National Risk Assessment pour les prochaines années?

Welke aan de klimaatverandering gerelateerde risico's werden er voor de periode 2018-2023 door de experts geanalyseerd, met bijzondere aandacht voor overstromingen? Wat is het nieuwe Belgian National Risk Assessment voor de komende jaren?

01.07 **Franky Demon** (cd&v): La guerre en Ukraine nous a fait prendre conscience de notre dépendance stratégique, particulièrement en ce qui concerne notre approvisionnement en énergie, comme l'a montré l'incident du gazoduc Nord Stream.

01.07 **Franky Demon** (cd&v): De oorlog in Oekraïne maakte ons bewust van onze strategische afhankelijkheid, zeker ook wat onze energiebevoorrading betreft. Het incident met de Nord Stream-gaspijpleiding was illustratief daarvoor.

La note de politique générale Intérieur pour 2023 aborde largement la question de la protection de nos infrastructures critiques. Il y est également indiqué que certaines échéances concernant les analyses de la menace n'ont pas été respectées, en raison de capacités insuffisantes au sein de l'OCAM et d'une déficience des échanges d'informations avec les services partenaires.

De beleidsnota van Binnenlandse Zaken voor 2023 gaat uitgebreid in op de bescherming van onze kritieke infrastructuur. Er staat ook in dat bepaalde deadlines inzake de dreigingsanalyses niet gehaald werden door een capaciteitstekort bij het OCAD en door gebrekkige informatie-uitwisseling met partnerdiensten.

Il était prévu que la ministre remédie à ce problème

De minister zou dat verhelpen door het OCAD in het

en renforçant l'OCAM à l'automne 2022 et en s'attelant au problème de la transmission d'informations. Ces mesures sont nécessaires, d'autant plus que la situation sur le plan international nous contraint à ne rien laisser au hasard.

najaar van 2022 te versterken en door het probleem met de informatiedoorstroming aan te pakken. Dat zijn noodzakelijke stappen, zeker ook omdat de internationale situatie ertoe noopt niets aan het toeval over te laten.

À l'heure actuelle, nos gazoducs constituent des infrastructures prioritaires susceptibles d'être menacées. Nous ne pouvons toutefois pas perdre de vue d'autres secteurs, même s'ils ne sont pas considérés comme critiques pour l'instant. J'ai déjà attiré l'attention sur les centres de distribution de produits alimentaires qui approvisionnent les supermarchés. Comeos insiste pour qu'ils soient placés sur la liste des infrastructures critiques, principalement en raison des conséquences très importantes en cas de panne de courant. Je demande une nouvelle fois à la ministre d'accéder à cette demande.

Onze gaspijpleidingen zijn op dit ogenblik prioritaire infrastructuur die bedreigd zou kunnen worden. Toch mogen we ook andere sectoren niet uit het oog verliezen, ook als ze vandaag niet als kritiek gelden. Ik wees vroeger al op de voedseldistributiecentra van supermarkten. Comeos dringt erop aan die op de lijst van kritieke infrastructuur te plaatsen en dat heeft veel te maken met de enorme gevolgen die een stroomonderbreking zou hebben. Ik vraag de minister nogmaals om die vraag in te willigen.

Au sein de la police, c'est la Direction de la sécurisation (DAB) qui est compétente pour protéger les infrastructures critiques. La ministre a déjà beaucoup relevé les capacités de cette direction et poursuivra cette opération cette année. Le cd&v soutient totalement cette initiative.

De bevoegdheid binnen de politie om kritieke infrastructuur te beveiligen, zit bij de DAB. De minister heeft de capaciteit daar al flink opgevoerd en doet daar dit jaar mee verder. Cd&v staat daar volledig achter.

01.08 **Tim Vandenput** (Open Vld): L'enchevêtrement des instances et des compétences est souvent pointé comme un problème complexe. Le ministre de la Justice a confectionné une nouvelle loi sur la sécurité maritime et un carrefour de l'information maritime pour mieux protéger les infrastructures critiques situées en mer du Nord. Comment la coopération se déroule-t-elle dans d'autres domaines?

01.08 **Tim Vandenput** (Open Vld): Vaak wordt het kluwen van instanties en bevoegdheden aangewezen als een moeilijk probleem. De minister van Justitie kwam met een nieuwe wet maritieme beveiliging en een maritiem informatiekruispunt om kritieke infrastructuur op de Noordzee beter te beschermen. Hoe verloopt de samenwerking op andere domeinen?

Le moment n'est-il pas venu de tendre vers une unité de commandement concernant la sécurité de toutes les infrastructures critiques afin de garantir une réponse efficace? La Belgique étant un pays importateur et exportateur, les ports maritimes et les aéroports, y compris les aéroports militaires, font partie des infrastructures critiques. En 2016, l'aéroport de Zaventem, la deuxième porte d'entrée économique de notre pays, a été inaccessible pendant des semaines.

Is de tijd niet rijp om inzake de veiligheid van alle kritieke infrastructuur naar een eenheid van commando te streven, zodat er efficiënt kan worden gereageerd? België is een import- en exportland en daarom behoren de zeehavens en luchthavens, inclusief de militaire, tot de kritieke infrastructuur. In 2016 lag de luchthaven van Zaventem, de tweede economische poort van ons land, wekenlang uit.

Des tests de résistance sont déjà effectués, mais sont-ils suffisants? Devons-nous réaliser davantage de tests pour être préparés aux catastrophes?

Er worden al stresstests gedaan, maar volstaan die? Moeten we meer testen om voorbereid te zijn op calamiteiten?

Quel est l'effectif actuel de la DAB? Combien de ces personnes sont-elles affectées quotidiennement aux infrastructures critiques?

Wat is de huidige bezetting van de DAB? Hoeveel van die mensen worden dagelijks ingezet om de kritieke infrastructuur te verzorgen?

01.09 **Kris Verduyckt** (Vooruit): La guerre en

01.09 **Kris Verduyckt** (Vooruit): De oorlog in

Ukraine met en lumière l'importance de l'énergie ainsi que des infrastructures critiques qui produisent et transportent cette énergie. Pour la première fois, des centrales nucléaires sont au cœur du champ de bataille, ce qui représente également un risque. Heureusement, la production d'énergie dans notre pays sera de plus en plus décentralisée, même s'il restera de grands sites tels que les centrales nucléaires, mais aussi une future île énergétique en mer du Nord.

Comment pourra-t-on protéger de manière raisonnable cette île énergétique? Demeurerons-nous dépendants des satellites étrangers ou permettrons-nous à nos institutions de développer leurs propres capacités d'observation?

01.10 **Theo Francken** (N-VA): La France est un précurseur dans cette problématique. Je ne suis pas le plus grand fan de l'appareil militaire français, mais il est très solide et efficace. Les Français ont une longue tradition dans l'art de la guerre et la constitution d'une défense. Il y a près d'un an, en février 2022, la France a été la première nation de l'OTAN à adopter une stratégie nationale de guerre sous-marine. Ce document vaut la peine d'être analysé.

Ostende accueille le centre d'excellence de déminage de l'OTAN, qui a bâti une très bonne réputation. Pourquoi ne pas élargir le champ d'action et créer un centre d'excellence de la guerre sous-marine?

Nous avons en effet une très bonne réputation en la matière. Nous avons également acquis de nouveaux navires, et l'entreprise ECA à Ostende construit des drones sous-marins. Nous disposons donc d'une expertise considérable, outre le NATO Center of Excellence. Il s'agit d'une occasion rêvée pour le conseil de la défense et de l'industrie de la ministre Dedonder. Peut-être pouvons-nous devenir les leaders, au niveau de l'OTAN, de la guerre des fonds marins et de la protection des infrastructures critiques?

Au total, nous disposons de 807 000 miles de câbles sous-marins, de gazoducs et autres, qui doivent être protégés au sein de l'alliance de l'OTAN. La marine italienne sécurise l'ensemble du réseau de câbles en Méditerranée et en mer Adriatique. À cet effet, elle a conclu un accord avec l'entreprise informatique Sparkle. Cette entreprise protège les câbles italiens en échange de l'accès à ceux-ci. Les câbles détectent par exemple tout ce qui bouge en termes de drones ou de navires et ces données sont directement transmises à la défense italienne. Que pensent les ministres de l'Intérieur et

Oekraïne zet een spot op het belang van energie en op de kritieke infrastructuur die die energie produceert en vervoert. Voor het eerst staan er kerncentrales in een strijdperk en ook dat is een risico. Een goede zaak is dat de energieproductie in ons land steeds meer gedecentraliseerd zal worden, maar toch zullen er grote sites blijven bestaan. De kerncentrales zijn daar een voorbeeld van, maar ook een eventueel energie-eiland op de Noordzee.

Hoe kan dat energie-eiland op redelijke wijze worden beschermd? Willen we afhankelijk blijven van buitenlandse satellieten of laten we onze instellingen zelf observatiecapaciteit ontwikkelen?

01.10 **Theo Francken** (N-VA): Frankrijk is in deze problematiek een voorloper. Ik ben niet de grootste fan van het Franse militaire apparaat, al is het wel heel degelijk uitgebouwd. De Fransen hebben een grote traditie op het vlak van oorlogsvoering en de opbouw van een verdediging. Bijna een jaar geleden, in februari 2022, heeft Frankrijk als eerste natie binnen de NAVO een nationale strategie voor zeebodemoorlogvoering ingevoerd en dat document is het bestuderen waard.

In Oostende is het NATO Center of Excellence voor mijnbestrijding gevestigd, dat ondertussen een heel goede reputatie heeft opgebouwd. Waarom zouden we dat niet uitbreiden naar een NATO Center of Excellence voor zeebodemoorlogvoering?

We hebben op dat gebied immers een zeer goede reputatie. We hebben ook nieuwe schepen aangekocht en er zijn onderwaterdrones, gebouwd door de firma ECA in Oostende. We hebben dus een enorme expertise, naast het NATO Center of Excellence. Dat is een enorme opportuniteit voor de defensie- en industrieraad van minister Dedonder. Misschien kunnen wij de koploper worden van de NAVO inzake zeebodemoorlogvoering en de bescherming van kritieke infrastructuur?

In totaal hebben we 807.000 mijl aan onderzeese kabels, gasleidingen en dergelijke die we moeten beschermen binnen het NAVO-bondgenootschap. De Italiaanse marine beveiligt het hele kabelnetwerk in de Middellandse en de Adriatische Zee. Zij hebben daarvoor een akkoord gesloten met het IT-bedrijf Sparkle. Zij beschermen de Italiaanse kabels in ruil voor toegang tot die kabels. De kabels detecteren bijvoorbeeld alles wat er beweegt op het vlak van drones of schepen en die data gaan rechtstreeks naar de Italiaanse defensie. Wat vinden de ministers van Binnenlandse Zaken en

de la Défense d'un tel accord de coopération? J'annonce d'ailleurs une proposition de résolution du groupe N-VA visant à inciter le gouvernement à conclure un tel accord. Je la déposerai à la Chambre avec d'autres parlementaires dans les semaines à venir.

01.11 **Yngvild Ingels** (N-VA): Le Centre de crise élabore une stratégie visant à accroître la résilience de notre société, et je pense que la protection des infrastructures critiques joue également un rôle à cet égard. Qu'en est-il?

01.12 **Annelies Verlinden**, ministre *(en néerlandais)*: En ce qui concerne l'approche multirisque, la législation existante se concentre principalement sur les risques d'origine humaine. La directive sur les entités critiques, une fois transposée en droit belge, garantira l'application de cette approche multirisque dans tous les éléments. C'est déjà le cas aujourd'hui dans la pratique et ce sera le cas demain sur la base de cette nouvelle législation. L'approche multirisque fait effectivement partie de la stratégie nationale de résilience en cours d'élaboration, coordonnée par le Centre de crise. L'élément central de cette approche est une évaluation transparente des risques et des menaces auxquels notre pays et les différents secteurs et sous-secteurs peuvent être confrontés.

La stratégie de résilience comprenant une approche multirisque découle de l'évaluation des vulnérabilités des systèmes au sein de chaque secteur, afin de mieux se préparer à d'éventuels chocs et perturbations. C'est dans l'optique de cette préparation que le déploiement du Belgian National Risk Assessment (BNRA) est poursuivi. La stratégie nationale de résilience doit aussi tenir compte du contexte international et des initiatives prises tant par l'OTAN que par l'UE. L'approche de résilience de l'OTAN et ses sept principes constituent également une orientation pour nous et le Centre de crise.

Dans le contexte énergétique, les entreprises disposent d'un plan d'urgence interne pour les situations d'urgence. En tant que gestionnaire des lignes à haute tension, Elia peut décréter un plan d'urgence interne en cas d'incident, en concertation avec le Centre de crise et les autres autorités sectorielles telles que la DG Énergie. En fonction de l'analyse de l'incident, d'autres acteurs peuvent éventuellement être informés et des accords peuvent être conclus sur les mesures à prendre ainsi que sur la convocation éventuelle de cellules de crise d'autres secteurs et départements. En dernier recours, la phase fédérale peut être

van Defensie van zo een samenwerkingsverband? Ik kondig overigens een voorstel van resolutie van de N-VA-fractie aan om de regering daartoe aan te zetten. Ik zal het de komende weken samen met een aantal andere parlementairen indienen in de Kamer.

01.11 **Yngvild Ingels** (N-VA): Het Crisiscentrum stelt een strategie op om de weerbaarheid van onze samenleving te verhogen en de bescherming van kritieke infrastructuur speelt daarin volgens mij ook een rol. Wat is de stand van zaken daarvan?

01.12 Minister **Annelies Verlinden** *(Nederlands)*: Wat de multirisicoaanpak betreft, is de bestaande wetgeving vooral gericht op de *man-made* risico's. De *Critical Entities*-richtlijn zal er na omzetting in de Belgische regelgeving voor zorgen dat die multirisicoaanpak in alle onderdelen wordt gebruikt. Vandaag is dat al het geval in de praktijk en morgen zal dat ook zo zijn op basis van die nieuwe wetgeving. De multirisicobenadering maakt inderdaad deel uit van de nationale weerbaarheidsstrategie die nu wordt opgesteld, gecoördineerd door het Crisiscentrum. Centraal staat een transparante beoordeling van de risico's en de bedreigingen waarmee ons land en de verschillende sectoren en subsectoren kunnen worden geconfronteerd.

De weerbaarheidsstrategie met de multirisicobenadering gaat uit van de inschatting van de kwetsbaarheden van de systemen binnen elk van de sectoren om zich beter te kunnen voorbereiden op eventuele schokken en storingen. Daarom wordt ook verdergebouwd op de Belgian National Risk Assessment (BNRA) om dat te kunnen voorbereiden. De nationale weerbaarheidsstrategie moet tevens rekening houden met de internationale context en de initiatieven die daar worden genomen, zowel door de NAVO als de EU. De NATO *resilience*, met de zeven uitgangspunten, is ook voor ons en voor het Crisiscentrum richtinggevend.

In de context van energie hebben bedrijven een intern noodplan voor een noodsituatie. Elia kan als beheerder van hoogspanningslijnen bij een incident een intern noodplan afkondigen, uiteraard in overleg met het Crisiscentrum en de andere sectorale overheden zoals de DG Energie. In functie van de analyse van het incident worden andere partijen mogelijk op de hoogte gebracht en zullen afspraken worden gemaakt over de te nemen maatregelen en het eventueel samenroepen van crisiscellen van andere sectoren en departementen. In het uiterste geval kan dat ook leiden tot de afkondiging van een federale fase.

décrétée.

Lorsque l'approvisionnement en gaz est touché, l'on tente de préserver les centrales électriques le plus possible et de les maintenir en fonctionnement le plus longtemps possible, afin d'examiner, dans le cadre du plan de délestage, quels secteurs, domaines et régions peuvent rester épargnés. Dans les exercices et la planification, cette approche multirisque est intégrée de façon beaucoup plus réfléchie et plusieurs incidents sont regroupés en un seul exercice. Je plaide donc pour une multiplication des exercices à chaque niveau.

Wanneer een gasvoorziening wordt geraakt, wordt geprobeerd de elektriciteitscentrales zoveel mogelijk te vrijwaren en ze zo lang mogelijk actief te houden, om in het kader van het afschakelplan te bekijken welke sectoren, domeinen en regio's gespaard kunnen blijven. In de oefeningen en in de planning wordt veel bewuster omgegaan met die multirisicobenadering en -aanpak en worden meerdere incidenten gebundeld in één oefening. Ik pleit dan ook voor meer oefeningen op elk niveau.

La surveillance des satellites relève de la compétence de la Défense. Pour soutenir la Défense, le Centre de crise peut, en qualité d'utilisateur autorisé unique, réclamer et mettre à disposition des images satellites, y compris à la demande d'autres services. Ces images peuvent être utilisées à des fins d'imagerie et de prise de décisions, au sein de la Défense, par les cellules de crise des différents départements ou en soutien à une éventuelle phase fédérale. Le Centre de crise examine actuellement encore la possibilité d'intégrer les satellites Starlink dans les systèmes d'imagerie.

De monitoring van de satellieten valt onder de bevoegdheid van Defensie. Ter ondersteuning van Defensie kan het Crisiscentrum, als enige *authorised user*, satellietbeelden opvragen en ter beschikking stellen, ook op vraag van andere diensten. Die beelden kunnen worden gebruikt voor beeldvorming en besluitvorming, binnen Defensie, door de crisiscellen van de verschillende departementen of bij het ondersteunen van een eventuele federale fase. Het Crisiscentrum bekijkt momenteel nog de mogelijkheid om de Starlinksatellieten mee in de beeldvorming te integreren.

Les questions relatives à la cybersécurité doivent être adressées au premier ministre.

De vragen over cyberveiligheid moeten aan de eerste minister worden gericht.

Depuis le 1er janvier 2023, la DAB a repris de la Défense la surveillance de la centrale nucléaire de Doel et des sites nucléaires à Mol, Dessel et Geel. Afin de renforcer la capacité en termes de personnel de la DAB, l'Académie nationale de police organisera sept classes l'année prochaine en vue de la formation des agents de sécurisation de la police. L'ambition est de former 168 agents de sécurité. Il faut toutefois également tenir compte des départs. La DAB a connu 18 départs naturels cette année. Par ailleurs, 79 membres du personnel ont entamé ou entameront encore la formation d'inspecteur et quitteront donc également la fonction d'agent de sécurisation. Nous devons donc poursuivre nos efforts au niveau du flux entrant.

De DAB heeft vanaf 1 januari 2023 de bewaking van de kerncentrale van Doel en van de nucleaire sites in Mol, Dessel en Geel overgenomen van Defensie. Om de personeelscapaciteit van de DAB te versterken, zal de Nationale Politieacademie volgend jaar zeven klassen organiseren om de beveiligingsagenten van de politie op te leiden. De ambitie is om 168 beveiligingsagenten op te leiden. Er moet echter ook rekening worden gehouden met de vertrekkers. Bij de DAB waren er dit jaar 18 natuurlijke vertrekkers. Daarnaast zijn er 79 personeelsleden die zijn gestart of nog zullen starten met de opleiding tot inspecteur en die dus ook zullen vertrekken als beveiligingsagent. Wij moeten dus blijven werken aan de instroom.

(En français) La DAB travaille avec la direction du personnel de la police intégrée pour le recrutement des futurs agents. Des contacts ont lieu avec le syndicat pour améliorer les procédures.

(Frans) De DAB werkt samen met de directie personeel van de geïntegreerde politie voor de rekrutering van nieuwe agenten. Er vinden gesprekken plaats met de vakbonden om de procedures te verbeteren.

La répartition des effectifs sur les sites et les centrales nucléaires ne peut être communiquée pour des raisons de sécurité. La sécurisation du procès des attentats mobilise environ 70 membres de la DAB chaque jour, en plus des membres des

De verdeling van de personeelsleden over de sites en de kerncentrales kan niet worden meegedeeld om veiligheidsredenen. Voor het verzekeren van de veiligheid op het proces van de aanslagen worden dagelijks ongeveer 70 personeelsleden van de DAB

polices intégrée et locale de Bruxelles-Nord-Ixelles.

Il n'est pas prévu que la DAB reprenne d'autres responsabilités ou d'autres sites. Ceux qu'elle sécurise figurent dans la loi sur la fonction de police. La sécurisation du palais royal, du SHAPE et de l'OTAN est assurée par une autre direction de la police administrative en attendant qu'elle reprenne ses missions.

La nomination du personnel de sécurité relève de l'exploitant d'une infrastructure critique. L'autorité sectorielle peut légalement demander des vérifications dont les résultats sont valables cinq ans.

(En néerlandais) Nous ne fournissons pas de détails sur l'identification des infrastructures protégées. Sur la base des rapports confidentiels et des évaluations des menaces de l'OCAM et du Centre de crise, des mesures policières sont déterminées. Pour garantir la sécurité de toutes les personnes concernées, nous ne communiquons pas en détail sur ce sujet.

Sur la base de la définition des infrastructures critiques et des paramètres de la loi du 1er juillet 2011, les infrastructures critiques sont identifiées par les autorités sectorielles. L'identification précise s'effectue sur la base de critères intersectoriels et sectoriels déterminés par l'autorité sectorielle, en tenant compte des caractéristiques particulières du secteur. L'on se penche à cet égard notamment sur le nombre de victimes potentielles, les dommages économiques potentiels ou les effets sur l'environnement.

En outre, l'incidence potentielle d'une attaque sur les infrastructures sur l'ensemble de la population est également analysée plus largement. Cette analyse inclut la confiance de la population, la perturbation de la vie quotidienne ou la perte de services essentiels. L'autorité sectorielle calcule les seuils pour les pertes économiques potentielles afin de procéder à l'identification de l'infrastructure critique.

La liste des infrastructures critiques est mise à jour par les autorités sectorielles tous les cinq ans ou lorsque cela s'avère nécessaire en raison de changements évidents. Une autorité sectorielle décide pour son secteur, avec le soutien du Centre de crise.

La liste est gérée par l'autorité sectorielle, mais le Centre de crise dispose évidemment d'une liste

ingezet, naast de leden van de geïntegreerde politie en de lokale politie van Brussel Noord-Elsene.

Het is niet de bedoeling dat de DAB andere verantwoordelijkheden of taken op andere sites overneemt. De activiteiten van de DAB worden vermeld in de wet op het politieambt. De beveiliging van het koninklijk paleis, SHAPE en de NAVO wordt verzekerd door een andere directie van de bestuurlijke politie in afwachting van een overname van die taken door de DAB.

Het is de exploitant van de kritieke infrastructuur die het beveiligingspersoneel aanstelt. De sectorale overheid kan krachtens de wet veiligheidsverificaties vragen, waarvan de resultaten vijf jaar geldig zijn.

(Nederlands) We geven geen details over de identificatie van de beschermde infrastructuren. Op basis van vertrouwelijke rapporten en dreigingsanalyses van het OCAD en het Crisiscentrum worden de politiemaatregelen bepaald. Om de veiligheid van alle betrokkenen te waarborgen, communiceren we daarover niet in detail.

Aan de hand van de definitie van kritieke infrastructuur en de parameters uit de wet van 1 juli 2011 worden de kritieke infrastructuren door de sectorale overheden aangeduid. De precieze identificatie gebeurt op basis van intersectorale en sectorale criteria die de sectorale overheid heeft bepaald, rekening houdend met de bijzondere eigenschappen van de sector. Daarbij kijkt men onder meer naar het aantal potentiële slachtoffers, de potentiële economische schade of de weerslag op het milieu.

Daarnaast wordt ook ruimer gekeken naar de potentiële weerslag van een aanval op de infrastructuur op de hele bevolking. Dan gaat het onder andere over het vertrouwen van de bevolking, de verstoring van het dagelijks leven of het uitvallen van essentiële diensten. De sectorale overheid berekent drempelwaarden voor mogelijke economische verliezen om tot de identificatie van de kritieke infrastructuur over te gaan.

De lijst van kritieke infrastructuren wordt vijfjaarlijks of wanneer het nodig is vanwege evidente wijzigingen door de sectorale overheden geactualiseerd. Een sectorale overheid beslist voor haar sector, met ondersteuning door het Crisiscentrum.

De lijst wordt beheerd door de sectorale overheid, maar uiteraard beschikt het Crisiscentrum over een

d'infrastructures critiques dans tous les secteurs concernés.

Nous avons élaboré au sein du Conseil national de sécurité une procédure pour l'attribution des cyberattaques, qui a déjà été appliquée à quelques reprises. Cela s'est également produit en mai 2021 aux Affaires étrangères, où il aurait été question d'ingérence d'un acteur étranger provenant de Chine. Pour des questions spécifiques à cet incident, je renvoie à la ministre des Affaires étrangères. Pour des questions sur la cyberattaque à Anvers, je renvoie au Centre pour la Cybersécurité Belgique (CCB), qui suit ce dossier.

À la suite de l'incident touchant le gazoduc Nord Stream, nous avons demandé à l'OCAM d'analyser la menace interétatique sur l'infrastructure gazière. Le niveau de menace sur cette dernière n'a heureusement pas dû être relevé, mais la situation reste surveillée en permanence. Des réunions ont également été organisées avec l'ensemble des services partenaires, et les exploitants d'infrastructures critiques qui pourraient être touchés ont été avertis.

En outre, des mesures de sécurité permanentes ont été prises. Des plans de sécurisation ont été actualisés et les autorités sectorielles ont réalisé des inspections.

Nous demandons que les incidents affectant d'autres secteurs soient signalés le plus rapidement possible aux autorités concernées ainsi qu'au Centre de crise.

(En français) Le *screening* des travailleurs portuaires relève du ministre de la Justice. Le processus d'approbation de ce dispositif est en voie de finalisation. Je ne peux vous dire, par sécurité, si une infrastructure est désignée comme critique. Vous devez interroger l'autorité sectorielle.

Pour la distribution de l'eau, je vous renvoie au Comité national de sécurité pour la fourniture et la distribution de l'eau potable, qui est composé des représentants d'entités fédérées et régionales.

La Police de la Navigation (SPN) compte 350 agents, dont 130 à la côte belge, 93 à Anvers auxquels s'ajoute une vingtaine de détachés de longue durée, et une cinquantaine au port de Gand. Aucun portique de sécurité ne relève de la SPN. Celle-ci a signé un accord de coopération avec la douane en juin 2022.

lijst van kritieke infrastructuren in alle betrokken sectoren.

Voor de attributie van cyberaanvallen hebben we een procedure uitgewerkt binnen de Nationale Veiligheidsraad, die ook al enkele keren is toegepast. Dat gebeurde ook in mei 2021 bij Buitenlandse Zaken, waar er sprake geweest zou zijn van inmenging door een buitenlandse actor uit China. Voor specifieke vragen over dit voorval verwijs ik naar de minister van Buitenlandse Zaken. Voor vragen over de cyberaanval in Antwerpen verwijs ik naar het Centrum voor Cybersecurity België (CCB), dat deze kwestie opvolgt.

Naar aanleiding van het incident met de Nord Stream-pijpleiding hebben we aan het OCAD gevraagd de interstatelijke dreiging voor gasinfrastructuur te analyseren. Gelukkig moest het dreigingsniveau voor gasinfrastructuur niet worden verhoogd, maar een en ander wordt continu opgevolgd. Er zijn ook vergaderingen georganiseerd met alle betrokken partnerdiensten en de exploitanten van kritieke infrastructuren die zouden kunnen worden geraakt, zijn gewaarschuwd.

Daarnaast zijn er ook permanente beveiligingsmaatregelen genomen. Beveiligingsplannen werden geactualiseerd en er waren inspecties door de sectorale overheden.

Wij vragen dat incidenten in andere sectoren zo snel mogelijk worden gemeld aan de betrokken overheden en het Crisiscentrum.

(Frans) De screening van havenarbeiders valt onder de bevoegdheid van de minister van Justitie. Het systeem heeft bijna het volledige goedkeuringsproces doorgelopen. Om veiligheidsredenen kan ik u niet vertellen of een infrastructuur als kritiek aangemerkt is. Daarvoor moet u zich tot de sectorale overheid richten.

Wat de waterdistributie betreft, verwijs ik u naar het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater, dat bestaat uit vertegenwoordigers van de federale overheid en de gewesten.

De Scheepvaartpolitie (SPN) telt 350 agenten, van wie er 130 actief zijn aan de Belgische kust, 93 in Antwerpen, plus een twintigtal voor lange duur gedetacheerde medewerkers, en een vijftigtal in de haven van Gent. De detectiepoortjes vallen niet onder de bevoegdheid van de SPN. De dienst heeft in juni 2022 een samenwerkingsakkoord

ondertekend met de douane.

La protection des réseaux informatiques gérés par des opérateurs essentiels et des exploitants d'infrastructure critique relève du Centre pour la Cybersécurité.

De beveiliging van de computernetwerken die beheerd worden door aanbieders van essentiële diensten en exploitanten van kritieke infrastructuren valt onder de verantwoordelijkheid van het Centrum voor Cybersecurity België.

Le premier ministre exerce la tutelle sur le Centre pour la Cybersécurité Belgique (CCB). Pour les questions relatives aux acteurs de la Santé publique, je renvoie vers le ministre compétent. Pour la protection des prisons et des établissements de justice, je renvoie vers le ministre de la Justice, qui rappelle que la loi du 1er juillet 2011 sur la protection des infrastructures critiques ne vise pas les autorités et services publics.

De eerste minister is de voogdijminister van het Centrum voor Cybersecurity België (CCB). Wat de vragen over de stakeholders van Volksgezondheid betreft, verwijs ik naar de bevoegde minister. Wat de beveiliging van de gevangenissen en de justitiegebouwen betreft, verwijs ik naar de minister van Justitie. Ik wijs erop dat de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren niet van toepassing is op de overheden en de openbare diensten.

Le Regional Computer Crime Unit (RCCU) et le Federal Computer Crime Unit (FCCU) contribuent à la *Quick reaction force* (QRF) dans le plan d'urgence cyber du CCB. Un groupe de collaborateurs de différents services CCU a été créé pour enquêter sur la cybercriminalité dans les environnements de réseaux complexes.

De Regional Computer Crime Unit (RCCU) en de Federal Computer Crime Unit (FCCU) werken in het kader van het cybernoodplan van het CCB mee aan de *quick reaction force* (QRF). Er werd een groep met medewerkers van de verschillende CCU-diensten opgericht om een onderzoek in te stellen naar de cybercriminaliteit in de omgeving van complexe netwerken.

La circulaire ministérielle GPI 62 précise des mesures pour la sécurisation des locaux d'entreposage des armes. J'ai demandé qu'un arrêté royal soit préparé pour la sécurisation des bâtiments policiers afin de renforcer les conseils de sécurité concernant le personnel, le matériel ou des informations sensibles.

In de ministeriële omzendbrief GPI 62 worden de maatregelen voor de beveiliging van de wapenopslaglokalen verduidelijkt. Ik heb gevraagd dat er een koninklijk besluit voorbereid zou worden met betrekking tot de beveiliging van de politiegebouwen, teneinde de veiligheidsadviezen betreffende het personeel, het materiaal of de gevoelige informatie te versterken.

Je soumettrai ce projet d'arrêté royal pour publication cette année.

Ik zal dat ontwerp van koninklijk besluit eerlang voorleggen zodat het dit jaar gepubliceerd kan worden.

Dans l'intervalle, la police fédérale procède à des investissements sur fonds propres ou via la Régie des Bâtiments pour la mise en conformité des locaux. Les projets de rénovation ou de construction repris dans les plans directeurs de la Régie comprennent une mise à niveau de ces locaux.

Intussen doet de federale politie met eigen middelen of via de Regie der Gebouwen investeringen om de gebouwen aan de voorschriften aan te passen. De renovatie- en bouwprojecten die in de masterplannen van de Regie zijn opgenomen, omvatten een rehabilitatie van deze gebouwen.

Les mesures de cybersécurité incombent à l'exploitant, qui doit élaborer un plan de sécurité et décrire les mesures prises. L'autorité sectorielle peut superviser et contrôler ces plans pour les infrastructures critiques. Le secteur public n'est pas couvert par la législation sur celles-ci.

Cybersecuritymaatregelen vallen onder de verantwoordelijkheid van de exploitant, die een beveiligingsplan moet uitwerken waarin de genomen maatregelen beschreven worden. De sectorale overheid kan toezicht en controle uitoefenen op deze plannen voor kritieke infrastructuren. De publieke sector valt niet onder de wetgeving betreffende de kritieke infrastructuren.

Les mesures de cybersécurité imposées par la loi NIS prévoient une protection approfondie du réseau et des systèmes d'informations des fournisseurs de services essentiels. Pour en savoir plus, je vous renvoie à la CCB.

De door de NIS-wet opgelegde cybersecuritymaatregelen voorzien in een uitgebreide bescherming van de netwerk- en informatiesystemen van aanbieders van essentiële diensten. Voor meer informatie verwijs ik u naar het CCB.

Je ne peux dévoiler les éléments des infrastructures critiques. La loi exige que les incidents menaçant leur fonctionnement soient signalés par l'exploitant aux services de police, à l'autorité sectorielle et au Centre de crise. Les incidents pris en compte par la loi NIS doivent être signalés aux autorités compétentes.

Ik kan geen informatie geven over de criteria waaraan kritieke infrastructuren moeten beantwoorden. De wet vereist dat incidenten die de werking van de exploitant bedreigen door de exploitant gemeld worden aan de politie, de sectorale overheid en het Crisiscentrum. Incidenten die onder de NIS-wet vallen, moeten aan de bevoegde overheden gemeld worden.

L'évaluation des risques de la Belgique est une analyse de risques au niveau national et n'informe pas sur la vulnérabilité d'infrastructures spécifiques ou de territoires belges.

De risicobeoordeling voor België is een risicoanalyse op nationaal niveau en bevat geen informatie over de kwetsbaarheid van specifieke infrastructuren of Belgische plaatsen.

Les résultats de la dernière itération 2018-2023 sont sur le site www.risk-info.be et peuvent être utilisés par les divers niveaux de pouvoir, y compris locaux, pour aider à réaliser les étapes suivantes du cycle de risques.

De resultaten van de recentste analyse 2018-2023 zijn terug te vinden op de website www.risico-info.be en kunnen door de verschillende beleidsniveaus – ook de lokale – gebruikt worden om de volgende stappen in de risicocyclus te helpen uitvoeren.

La prochaine itération de l'évaluation nationale des risques est en cours et sera valable pour 2023-2026.

De volgende iteratie van de nationale risicoanalyse is aan de gang en zal voor de periode 2023-2026 gelden.

L'identification et l'analyse des risques d'inondation est une responsabilité du gouverneur de province. En principe, cette analyse n'est pas rattachée au plan national et peut servir à établir un plan d'intervention pour les risques pour lesquels l'autorité compétente l'estime nécessaire. Le risque de tempête est couvert par le plan national.

De identificatie en de analyse van de overstromingsrisico's zijn verantwoordelijkheden van de provinciegouverneur. In principe staat deze analyse los van het nationaal plan en kan ze gebruikt worden om een interventieplan op te stellen voor de risico's waarvoor de bevoegde overheid dat nodig acht. Het stormrisico is in het nationaal plan opgenomen.

Pour la province de Liège, le plan reprend le risque d'inondations dans son annexe 49 qui sert de plan d'intervention et de fiche de référence. Pour les risques Seveso, les exploitants des établissements doivent établir un rapport de sécurité, dont le chapitre sur la présentation de l'environnement doit prendre en compte le risque d'inondation. Les services d'évaluation dont le Centre de crise doivent approuver ces rapports.

Voor de provincie Luik is het overstromingsrisico in het plan opgenomen onder bijlage 49, die als interventieplan en referentiefiche dienstdoet. Wat de sevesorisico's betreft, moeten de uitbaters van de inrichtingen een veiligheidsrapport opstellen. In het hoofdstuk van dat rapport waarin de omgeving voorgesteld wordt, moet rekening gehouden worden met het overstromingsrisico. De evaluatiediensten, waartoe ook het Nationaal Crisiscentrum behoort, moeten die rapporten goedkeuren.

(En néerlandais) À ce jour, aucune infrastructure critique n'a été identifiée dans le secteur de la distribution alimentaire. Il n'existe dès lors pas non plus d'analyse de la menace pour ce secteur. Compte tenu de la récente directive sur la résilience des entités critiques, cela va changer à l'avenir.

(Nederlands) Vandaag worden er geen kritieke infrastructuren binnen de voedseldistributie gedefinieerd. Er is dus ook geen dreigingsanalyse. Gelet op de recente richtlijn betreffende de veerkracht van kritieke entiteiten zal dat in de toekomst wel veranderen.

En 2022, le Centre de crise, comme d'autres partenaires, a soutenu le SPF Économie dans l'élaboration d'une proposition de plan de crise alimentaire, destiné à préparer la Belgique à d'éventuelles crises ou d'éventuels incidents qui se produiraient dans les centres de distribution ou dans la chaîne d'approvisionnement alimentaire. Cette démarche s'est appuyée sur une analyse des différents risques susceptibles de perturber la chaîne alimentaire, ainsi que sur l'identification des personnes et des groupes les plus vulnérables. Une étude a également été réalisée sur les vulnérabilités du secteur agroalimentaire et la gestion des crises au Danemark et en Allemagne.

In 2022 ondersteunde het Crisiscentrum, net zoals andere partners, de FOD Economie bij de uitwerking van een voorstel van voedselcrisisplan, dat België moet voorbereiden op crises of incidenten bij distributriecentra of binnen de voedselvoorzieningsketen. Dat was gebaseerd op een analyse van de verschillende risico's die de voedselketen zouden kunnen verstoren, maar ook een identificatie van de meest kwetsbare personen en groepen. Er was ook een studie over de kwetsbaarheden in de agrovoedingssector en het crisisbeheer in Denemarken en Duitsland.

Cette étude montre dans quels domaines notre pays est leader et dans quels domaines un mouvement de rattrapage est nécessaire. Une première version du plan a été transmise au SPF Économie. Il contient les principales directives devant permettre à l'autorité compétente de maîtriser le mieux possible chaque situation ayant des conséquences néfastes afin de rétablir la chaîne alimentaire, de garantir l'approvisionnement et d'informer la population. Dès la finalisation du plan de crise alimentaire, tous les acteurs devront concrétiser les mesures.

Die studie toont op welke vlakken ons land vooroploopt en op welke vlakken een inhaalbeweging nodig is. Een eerste versie van het plan ligt bij de FOD Economie. Het bevat de belangrijkste richtlijnen waarmee de bevoegde autoriteit elke situatie met nadelige gevolgen, zo goed mogelijk moet kunnen beheersen, om de voedingsketen te herstellen, de bevoorrading te verzekeren en de bevolking te informeren. Zodra het voedselcrisisplan definitief is, moeten alle actoren de maatregelen operationaliseren.

Dans le cadre des sept exigences de base de l'OTAN, le Centre de crise réalise une analyse des écarts (*gap analysis*) afin de recenser les lacunes dans l'intérêt de la chaîne alimentaire. Cette analyse doit être prête d'ici février 2023 et nous examinerons alors au niveau sectoriel quels sont les mesures et les plans de mise en œuvre nécessaires.

In het kader van de zeven *baseline requirements* van de NAVO voert het Crisiscentrum een *gap analysis* uit om lacunes in het belang van voedselketen te identificeren. Deze analyse moet klaar zijn tegen februari 2023, waarna we op sectoraal niveau bekijken welke maatregelen en implementatieplannen nodig zijn.

À l'heure actuelle, l'OCAM ne perçoit pas de menaces pesant sur les centres de distribution. Les analyses des infrastructures critiques accusent un léger retard. L'OCAM bénéficiera d'un renforcement structurel. Les sélections sont terminées. Le retard sera comblé dans les plus brefs délais.

Het OCAD ziet vandaag geen dreigingen ten aanzien van distributiecentra. Er is een kleine achterstand bij de analyses van de kritische infrastructuur. Het OCAD krijgt structurele versterking. De selecties zijn afgerond. De achterstand wordt zo snel mogelijk weggewerkt.

Dans le cadre d'une menace concrète, l'OCAM peut toujours procéder à une analyse ponctuelle de la menace, après quoi le Centre de crise peut prendre des mesures. Il a réalisé une analyse de la menace interétatique dans le cadre de la guerre dont la portée dépassait largement les seules infrastructures critiques, mais qui s'est également intéressée à d'autres secteurs sensibles ou à certaines personnes. Nous examinons si l'OCAM doit se voir attribuer une mission supplémentaire explicite en matière de menace interétatique.

Bij een concrete dreiging kan het OCAD altijd een punctuele dreigingsanalyses opstellen, waarna het Crisiscentrum maatregelen kan nemen. Het OCAD heeft een analyse van de interstatelijke dreiging in het kader van oorlog opgemaakt die ruimer ging dan enkel kritische infrastructuren, maar ook andere gevoelige sectoren of bepaalde personen bevatte. We bekijken of het OCAD een expliciete bijkomende opdracht moet krijgen inzake de interstatelijke dreiging.

Le cas échéant, l'OCAM devra faire une proposition

Het OCAD moet desgevallend een voorstel doen

au Comité de coordination du renseignement et de la sécurité (CCRS), au Comité stratégique du renseignement et de la sécurité (CSRS) et au Conseil national de sécurité.

aan het Coördinatiecomité voor Inlichting en Veiligheid (CCIV), het Strategisch Comité voor Inlichtingen en Veiligheid (SCIV) en de Nationale Veiligheidsraad.

Il existe deux mécanismes de coopération interdépartementale en mer du Nord. Le Carrefour de l'information maritime – composé de FedPol, de la DG Navigation, de la douane et de la marine – surveille la mer en permanence et envoie des patrouilles si nécessaire. L'autre mécanisme est l'évaluation des risques dans le cadre du nouveau Code de la navigation, qui est entré en vigueur au début de cette année.

Er zijn twee mechanismen voor interdepartementale samenwerking in de Noordzee. Het Maritiem Informatiekruispunt – samengesteld uit FedPol, DG Scheepvaart, douane en marine – monitort de zee permanent en stuurt indien nodig patrouilles uit. Het andere mechanisme is de risicobeoordeling in het kader van het vernieuwde Scheepvaartwetboek, dat begin dit jaar in werking is getreden.

Le Carrefour de l'information maritime établira un rapport de sécurité concernant les menaces potentielles, les points faibles et les points d'amélioration. L'Autorité nationale de sûreté maritime devra approuver ce plan, qui sera actualisé tous les cinq ans. Les niveaux du Code international pour la sûreté des navires et des installations portuaires (ISPS) applicables aux ports seront adaptés. Les ports devront prendre des mesures de sécurité supplémentaires.

Het Maritiem Informatiekruispunt zal een veiligheidsbeoordeling van mogelijke dreigingen, zwakke plekken en verbeterpunten opstellen. De Nationale Autoriteit voor Maritieme Beveiliging moet dat plan goedkeuren. Het zal om de vijf jaar worden geactualiseerd. De niveaus van de Internationale Code voor de Beveiliging van Schepen en Havenfaciliteiten (ISPS) voor de havens worden aangepast. Zij moeten bijkomende veiligheidsmaatregelen nemen.

Le test de résistance fait partie du plan de sécurisation de l'exploitant des infrastructures critiques. Les services d'inspection sectoriels contrôlent ces plans. On peut considérer cette opération comme un test de résistance. Tous les secteurs cités plus haut sont aussi importants les uns que les autres. Les activités du Centre de crise sont également abordées suivant la même approche.

De stresstest zit vervat in het beveiligingsplan van de exploitant van de kritieke infrastructuren. De sectorale inspectiediensten controleren deze plannen. Dat kan worden omschreven als een stresstest. Alle voornoemde sectoren zijn even belangrijk. Ook de activiteiten van het Crisiscentrum worden zo benaderd.

L'exploitant est responsable du signalement des incidents au Centre de crise, la police est responsable du suivi de ces signalements et l'autorité sectorielle est responsable de l'inspection. L'OCAM est associé aux analyses ponctuelles et stratégiques de la menace. Le Centre de crise joue un rôle de supervision, de coordination et d'appui, notamment dans l'élaboration des plans nationaux de sécurité.

De exploitant is verantwoordelijk om incidenten te melden aan het Crisiscentrum, de politie is verantwoordelijk voor de opvolging ervan en de sectorale autoriteit is verantwoordelijk voor de inspectie. Het OCAD is betrokken bij de punctuele en strategische dreigingsanalyses. Het Crisiscentrum heeft een overkoepelende en coördinerende rol en een ondersteunende rol bij onder meer de opmaak van nationale veiligheidsplannen.

Si l'île énergétique est réalisée, nous devrons examiner si elle doit être qualifiée d'infrastructure critique. S'il ressort de l'analyse de l'autorité sectorielle qu'il ne s'agit pas d'une infrastructure critique, l'île sera protégée structurellement par l'Autorité nationale de sûreté maritime.

Als het energie-eiland gerealiseerd wordt, moeten we kijken of het als kritieke infrastructuur aangeduid moet worden. Als uit analyse van de sectorale overheid zou blijken dat het geen kritieke infrastructuur is, zal het eiland structureel beveiligd worden door de Nationale Autoriteit voor Maritieme Beveiliging.

01.13 **Ludivine Dedonder**, ministre *(en français)*: Si la Défense n'a pas de responsabilité explicite en matière de protection des infrastructures critiques,

01.13 Minister **Ludivine Dedonder** *(Frans)*: Defensie heeft geen expliciete verantwoordelijkheid op het vlak van de bescherming van kritieke

elle dispose de certaines capacités qui peuvent venir en appui ou contribuer aux missions des services civils qui en font la demande.

(En néerlandais) Ces capacités duales permettent à la Défense non seulement d'effectuer des missions de sécurité structurelle en Belgique, mais également de soutenir les services civils dans le cadre de la sécurisation des infrastructures critiques. Les missions du SEDEE s'inscrivent dans ce cadre.

(En français) La capacité CBRN spécialisée de la Défense contribue à la lutte contre la prolifération d'armes de destruction massive et au plan d'urgence national en cas d'accident majeur sur notre territoire. Elle est également engagée dans la lutte contre le terrorisme. Au travers de protocoles d'accord, des collaborations ont vu le jour dans le cadre du Centre de crise national et de son centre d'expertise CBRN fédéral, et dans le cadre du Plan d'urgence nucléaire sous la coordination de l'AFCN. La Défense met à contribution des hélicoptères A 109 équipés de gamma-spectromètres pour effectuer des contrôles radiologiques de zones sensibles.

Un accord de coopération entre la Composante Terre et le service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale permet des échanges d'expertise en CBRN.

(En néerlandais) Les laboratoires de la Défense jouent un rôle clé dans l'identification univoque des installations chimiques, biologiques, radiologiques ou nucléaires (CBRN). Le laboratoire fédéral d'orientation est le point de contact pour l'analyse des colis présentant un risque CBRN potentiel. Les spécialistes CBRN de la Défense possèdent un éventail de compétences, une expérience et une préparation en la matière que ne peuvent pas offrir nos partenaires civils.

(En français) Les cyberattaques d'envergure que nous avons pu contrer prouvent la pertinence de notre choix d'investir dans le domaine de la cybersécurité et la nécessité d'y investir encore.

(En néerlandais) En 2022, l'accent était porté sur le renforcement des capacités cyber opérationnelles du SGRS et sur le lancement de ce qui devrait devenir à terme la composante cyber de la Défense, à savoir le Cyber Command.

La plus grande menace aujourd'hui est bel et bien la cybernétique. Plus que jamais, nous devons nous

infrastructuur, maar het departement beschikt wel over de nodige capaciteit waarmee het bijstand kan verlenen of kan bijdragen aan de opdrachten van de civiele diensten die daarom vragen.

(Nederlands) Dankzij deze duale capaciteit kan Defensie niet alleen structurele veiligheidstaken in eigen land uitvoeren, maar ook civiele diensten ondersteunen bij de beveiliging van kritieke infrastructuur. De taken van DOVO maken daar deel van uit.

(Frans) De gespecialiseerde CBRN-capaciteit van Defensie werkt mee aan de bestrijding van de proliferatie van massavernietigingswapens en aan het nationaal noodplan in geval van een ernstig incident op ons grondgebied. Ze is ook betrokken bij terrorismebestrijding. Via protocolakkoorden zijn er samenwerkingverbanden opgezet in het kader van het Nationaal Crisiscentrum en zijn federale CBRNe-expertisecentrum en in het kader van het nucleair noodplan onder coördinatie van het FANC. Defensie stelt A109-helikopters ter beschikking die uitgerust zijn met gammaspectrometers voor het uitvoeren van stralingscontroles met betrekking tot gevoelige zones.

Er bestaat een samenwerkingsakkoord tussen de Landcomponent en de Dienst voor Brandbestrijding en Dringende Medische Hulp van het Brussels Hoofdstedelijk Gewest dat de uitwisseling van CBRN-expertise mogelijk maakt.

(Nederlands) De laboratoria van Defensie spelen een sleutelrol bij de eenduidige identificatie van chemische, biologische, radiologische of nucleaire (CBRN) installaties. Het federaal oriëntatielaboratorium is het meldpunt voor de behandeling van pakjes met een vermoedelijk CBRN-risico. De gespecialiseerde CBRN-capaciteit van Defensie bezit een waaier aan bekwaamheden, ervaring en voorbereiding op dergelijke zaken, die onze civiele partners niet kunnen bieden.

(Frans) De grootschalige cyberaanvallen die we hebben kunnen afslaan tonen aan dat onze keuze om te investeren in cyberbeveiliging de juiste was én dat verdere investeringen noodzakelijk blijven.

(Nederlands) In 2022 lag de focus op het versterken van de operationele cybercapaciteiten bij de ADIV en de opstart van wat op termijn de cybercomponent van Defensie moet worden, namelijk de Cyber Command.

De grootste bedreiging van vandaag is wel degelijk de cybernetics. Meer dan ooit moeten wij ons

prémunir contre ce danger. Il est clair que la capacité cyber est la capacité de l'avenir pour notre base industrielle.

(En français) Le développement des capacités cybernétiques de la Défense se poursuivra cette année.

L'ambition est de doubler le personnel dans ce domaine. Pour des raisons de sécurité, nous ne communiquons pas les moyens dédiés à cette capacité. Nous travaillons avec des partenaires publics et privés, pour arriver à un équilibre de deux tiers de civils et un tiers de militaires. Nous travaillons avec nos entreprises et engageons sous la réserve militaire, comprenant des personnes travaillant dans des entreprises de cybersécurité et à la Défense. Nous offrons aussi l'accès à des informations classifiées ou relatives aux opérations à l'étranger.

En collaboration avec le Centre de crise national, le CCB, la police fédérale et les Affaires étrangères, le nouveau Cyber Command participe à la protection des infrastructures critiques, comme le prévoient la stratégie nationale de sécurité et la stratégie cybersécurité Belgique 2.0.

Parallèlement au renforcement des capacités du Cyber Command et conformément aux mesures européennes, nous analyserons comment contribuer à la cybersécurité des entités critiques.

Concernant les capacités offensives, la loi a été adaptée pour permettre à la Défense de réagir en cas d'attaque. C'est le cas si la Défense, autre département ou une infrastructure critique d'intérêt national sont attaqués.

(En néerlandais) Outre ses propres infrastructures critiques, la Belgique accueille également les principales institutions de l'UE et de l'OTAN ainsi que de toute une série d'organisations internationales. Afin de consolider notre position de pays hôte et de préserver la sécurité de fonctionnement de nos infrastructures et institutions, la Belgique a renforcé ses capacités en matière d'antiterrorisme, d'espionnage, de subversion et de crime organisé par le biais du plan STAR. Le SGRS collecte des données et les transmet à l'OCAM, qui procède alors à une évaluation de la menace.

(En français) Avec la Belgian Pipeline Organization (BPO), la Défense maintient en l'état la partie belgo-

daartegen wapenen. Het is duidelijk dat cybercapaciteit de capaciteit van de toekomst is voor onze industriële basis.

(Frans) Ook dit jaar zal Defensie haar cybercapaciteit verder uitbouwen.

We streven naar een verdubbeling van het personeel van de cybercomponent. Om veiligheidsredenen communiceren we niet over de middelen voor die capaciteit. Samen met publieke en private partners werken we toe naar een evenwicht van twee derde burgerpersoneelsleden en een derde militairen. We werken samen met onze bedrijven en rekruteren personeelsleden via de militaire reserve, waaronder ook mensen die werken in cyberveiligheidsbedrijven en bij Defensie. We geven ook toegang tot geclassificeerde informatie en informatie over buitenlandse operaties.

In samenwerking met het Nationaal Crisiscentrum, het CCB, de federale politie en Buitenlandse Zaken neemt de nieuwe Cyber Command deel aan de beveiliging van kritieke infrastructuur, zoals vastgelegd in de nationale veiligheidsstrategie en de Cybersecurity Strategy Belgium 2.0.

Naast de versterking van de capaciteit van de Cyber Command en overeenkomstig de Europese maatregelen zullen we bekijken hoe we kunnen bijdragen aan de cyberveiligheid van kritieke instellingen.

Wat de offensieve capaciteit betreft, werd de wet gewijzigd, zodat Defensie op eventuele aanvallen kan reageren. Die mogelijkheid is er voortaan als Defensie, een ander departement of een kritieke infrastructuur van nationaal belang aangevallen worden.

(Nederlands) Naast de eigen kritieke infrastructuur herbergt België ook de belangrijkste instellingen van de EU, de NAVO en van een hele rist internationale organisaties. Om onze positie als gastland te bestendigen en om de veilige werking van onze infrastructuur en instellingen te vrijwaren, heeft België via het STAR-plan zijn capaciteiten op het gebied van antiterrorisme, spionage, subversie en georganiseerde misdaad versterkt. De ADIV verzamelt gegevens en stuurt die door naar het OCAD, dat dan de dreigingsevaluatie maakt.

(Frans) Met de Belgian Pipeline Organisation (BPO) staat Defensie in voor de bedrijfszekerheid van het

luxembourgeoise des pipelines d'Europe centrale qui approvisionnent en carburants des bases aériennes en France, en Allemagne et au Benelux.

Belgisch-Luxemburgse gedeelte van de pijpleidingen in Centraal-Europa voor de jetfuel- en gasolievoorziening van de luchtmachtbasissen in Frankrijk, Duitsland en de Benelux.

Ce dispositif dépassant les besoins militaires, l'excédent est à disposition de clients civils, dont de gros aéroports, pour assurer un entraînement optimal du personnel et une rotation des produits, et partager ses coûts.

De brandstofaanvoer is groter dan de militaire behoeften, en het overschot wordt daarom aangeboden aan burgerklanten, waaronder grote luchthavens. Op die manier kan een optimale training van het personeel gegarandeerd worden, is het voorraadverloop gegarandeerd en kunnen de kosten verdeeld worden.

(En néerlandais) Outre l'importance militaire évidente, l'importance économique de cette unité pour la Belgique ne doit pas être sous-estimée. Le carburant pour Brussels Airport, Luxembourg Airport et – dans une large mesure – pour l'aéroport de Bierset est fourni exclusivement par la Belgian Pipeline Organisation (BPO), qui est opérationnelle 24 h sur 24, 7 jours sur 7. En raison de sa position centrale dans le réseau, la BPO fait office de pivot de ce réseau, reliant les points d'accès de la zone Amsterdam-Rotterdam-Anvers aux clients nationaux et internationaux. La moitié du volume transporté est destinée aux organisations sœurs à l'étranger.

(Nederlands) Naast het evidente militaire belang mag ook het economische belang van deze eenheid voor België niet worden onderschat. Vliegtuigbrandstof voor Brussels Airport, voor Luxembourg Airport en – voor een belangrijk deel – voor Bierset wordt exclusief geleverd door de Belgian Pipeline Organisation (BPO), dat permanent operationeel is. Door de centrale ligging in het netwerk fungeert de BPO als spil in dit netwerk door de toegangspunten van de zone Amsterdam-Rotterdam-Antwerpen te verbinden met de klanten in binnen- en buitenland. De helft van het getransporteerde volume gaat naar zusterorganisaties in het buitenland.

(En français) L'OTAN définit la résilience de cette infrastructure face aux menaces. Sa protection s'effectue selon différents niveaux de responsabilité, en lien notamment avec des services de sécurité externes. En cas d'incident, une chaîne de notifications est prévue. Nous nous appuyons aussi sur les moyens de nos alliés pour l'échange d'informations, y compris satellitaires. Cette approche s'inscrit dans notre stratégie de résilience pour la protection des infrastructures critiques.

(Frans) De NAVO bepaalt in welke mate deze infrastructuur bestand is tegen de dreigingen. De bescherming ervan gebeurt volgens verschillende verantwoordelijkheidsniveaus, onder meer in samenwerking met externe veiligheidsdiensten. Wanneer er zich een incident voordoet, treedt er een keten van waarschuwingsberichten in werking. Voor de uitwisseling van informatie, ook via satellieten, steunen wij eveneens op de middelen van onze bondgenoten. Deze benadering past in het kader van onze weerbaarheidsstrategie voor de bescherming van kritieke infrastructuur.

La Défense joue un rôle dans la *Quick Reaction Alert* pour la mission de police aérienne dans le cadre de l'OTAN, y compris sur notre territoire. Des experts de la Défense interviennent au sein du *National Airspace Security Center* (NASC) où ils coopèrent avec le SPF Mobilité, la police fédérale et les douanes pour répondre efficacement en cas d'incident. Le NASC analyse et traite les informations sur les incidents liés à l'aviation et les retransmet à tous les services concernés.

Defensie speelt een rol in de Quick Reaction Alert in het kader van de luchtruimbewakingsopdracht van de NAVO, die zich ook over ons grondgebied uitstrekt. Experts van Defensie maken deel uit van het National Airspace Security Center (NASC), waar ze samenwerken met de FOD Mobiliteit, de federale politie en de douanediensten om in geval van een incident efficiënt te reageren. Het NASC analyseert en verwerkt de informatie over luchtvaartgerelateerde incidenten en stuurt ze door naar alle betrokken diensten.

Nonobstant la liste des infrastructures critiques, les opérateurs et la marine sécurisent évidemment les infrastructures en mer.

Niettegenstaande deze lijst met kritieke infrastructuur ligt het voor de hand dat de operatoren en de marine de infrastructuur op zee beveiligen.

C'est d'autant plus important avec le risque de sabotage lié à la guerre en Ukraine, notamment, de câbles sous-marins qui constituent des enjeux géostratégiques mondiaux pouvant bouleverser les télécommunications, l'économie ou l'approvisionnement énergétique. Les auteurs de sabotage peuvent être des organisations terroristes et criminelles ou des États hostiles, et leur dangerosité dépend de leur niveau technologique et de l'accessibilité de l'infrastructure.

Dat is des te belangrijker nu er sabotage dreigt door de oorlog in Oekraïne. Het gaat dan in het bijzonder over onderzeese kabels, die mondiale geografische uitdagingen vormen, aangezien sabotage van die kabels de telecommunicatie, de economie en de energievoorziening kan verstoren. De sabotage kan gepleegd worden door terroristische en criminele organisaties of vijandige staten. Het gevaar dat die potentiële daders vormen, hangt af van hun technologische knowhow en de toegankelijkheid van de infrastructuur.

(En néerlandais) Au niveau national, l'exploitant est responsable de l'infrastructure. La police fédérale exécute les mesures de protection. Pour sa part, la Défense conseille l'exploitant en matière de sécurité, y compris de cybersécurité, et peut le soutenir en cas de menace accrue, de même que la police fédérale.

(Nederlands) Op nationaal niveau is de exploitant verantwoordelijk voor de infrastructuur. De federale politie voert de beschermingsmaatregelen uit. Defensie van zijn kant adviseert de exploitant over veiligheid, inclusief cyberveiligheid, en staat klaar om hem te ondersteunen bij verhoogde dreiging, net als de federale politie.

La Défense consulte régulièrement l'industrie offshore et entretient des contacts avec des partenaires tels qu'Elia, Otary et Parkwind. Elle organise également des exercices conjoints au sein et à proximité des parcs éoliens. Le partage de moyens tels que des caméras fait aussi l'objet de concertations.

Defensie overlegt regelmatig met de offshore-industrie, onderhoudt contacten met partners als Elia, Otary en Parkwind en organiseert gezamenlijke oefeningen in en rond windmolenparken. Er is ook overleg over het delen van middelen, zoals bijvoorbeeld camera's.

(En français) La Marine participe à la sécurité des eaux belges, notamment la sécurisation des infrastructures critiques en mer, le contrôle de la pêche, la lutte contre les trafics, la préservation de l'environnement et l'appui lors de catastrophes.

(Frans) De Marinecomponent verzekert mee de veiligheid op de Belgische wateren, en staat met name in voor de beveiliging van de kritieke infrastructuur op zee, de controle op de visserij, de strijd tegen de illegale handel, de bescherming van het leefmilieu en de ondersteuning bij rampen.

Du personnel de la douane, de la police maritime et du SPF Mobilité a été intégré au commandement de la Marine dans le Carrefour de l'information maritime (CIM). Les quatre autorités ont leurs propres missions et disposent de bases de données sur toute la côte belge.

Personeelsleden van de douane, de scheepvaartpolitie en de FOD Mobiliteit maken deel uit van het commando van de marine in het Maritiem Informatie Kruispunt (MIK). De vier autoriteiten hebben hun eigen opdrachten en beschikken over gegevensbanken voor de hele Belgische kust.

(En néerlandais) Des informations sont collectées, analysées et partagées en permanence au Carrefour de l'information maritime. Afin d'optimiser la surveillance des eaux belges, des lignes d'approvisionnement maritimes et des infrastructures offshore, des pourparlers sont actuellement menés au sujet d'une coopération, notamment dans le cadre d'une future île énergétique. Une telle île conviendrait parfaitement à l'installation de capteurs et de dispositifs de communication, ainsi que comme site d'atterrissage pour drones.

(Nederlands) In het Maritiem Informatiekruispunt (MIK) verzamelt, analyseert en deelt men continu informatie. Om de bewaking van de Belgische wateren, de maritieme aanvoerlijnen en de offshore-infrastructuur te optimaliseren, lopen besprekingen over een samenwerking, onder andere in het kader van een toekomstig energie-eiland. Zo een eiland is zeer geschikt voor de installatie van sensoren en communicatiesystemen en als aanlegplaats voor drones.

(En français) La coopération interdépartementale dans le MIK peut intéresser les services de sécurité,

(Frans) De interdepartementale samenwerking in het MIK kan van belang zijn voor de

le Centre de crise national et le NASC lors d'opérations urgentes et de secours.

Des réunions périodiques sont organisées avec les partenaires européens et transatlantiques qui surveillent les transits des navires pouvant être une menace. Sans infraction flagrante, un État ne peut arraisonner un navire, mais l'exploitant et/ou la Marine peut analyser *a posteriori* les fonds marins et les éventuelles infrastructures critiques.

(En néerlandais) En ce qui concerne les eaux internationales, la Belgique a ratifié en 2015 la Convention pour la répression d'actes illicites contre la sécurité de la navigation maritime et le Protocole y relatif. Cette convention prévoit que les pays signataires peuvent prendre des mesures contre des navires qui commettent des infractions.

(En français) Les vulnérabilités des infrastructures critiques sont bien plus importantes en haute mer où prévaut la liberté de navigation et où la surveillance est plus compliquée de par les fonds marins et les moyens techniques nécessaires pour accroître la zone de surveillance. En dehors d'une zone économique exclusive, il est difficile d'attribuer une attaque ou un sabotage à un acteur hostile.

La Défense belge collabore avec le centre d'excellence de l'OTAN en Italie. Avec le plan STAR, nous avons une stratégie de développement technologique incluant le renforcement des partenariats avec les centres de recherche et des partenaires privés. L'investissement en recherche et développement se porte à 1,8 milliards d'euros. Notre volonté est de travailler avec nos entreprises de manière générale.

(En néerlandais) Plusieurs initiatives sont actuellement en cours pour développer de nouvelles technologies par le biais du programme DIANA et de l'Agence européenne de défense.

(En français) Les fonctionnalités "sécurisation" et "manutention non qualifiée" peuvent être fournies en appui d'autres services via la compagnie de protection territoriale. Il s'agit d'un détachement qui se tient prêt en tant que capacité d'intervention rapide en coordination avec les commandements militaires provinciaux, les autorités civiles et la police.

(En néerlandais) Le développement du hub logistique national prévu par le plan STAR contribuera à améliorer la mobilité militaire, y compris à l'échelle nationale, et donc la résilience

veiligheidsdiensten, het Nationaal Crisiscentrum en het NASC tijdens nood- en hulpoperaties.

Er worden periodieke vergaderingen georganiseerd met de Europese en trans-Atlantische partners die toezicht houden op de doorvaart van de schepen die een gevaar kunnen vormen. Zonder een op heterdaad vastgestelde inbreuk kan een Staat niet aan boord gaan van een schip, maar de exploitant en/of de marine kan de zeebodem en eventuele kritieke infrastructuren achteraf onderzoeken.

(Nederlands) Inzake de internationale wateren heeft België in 2015 het verdrag en het protocol geratificeerd tot bestrijding van wederrechtelijke gedragingen, gericht tegen de veiligheid van de zeevaart. Dat verdrag bepaalt dat de ondertekenende landen maatregelen kunnen nemen tegen vaartuigen die misdrijven plegen.

(Frans) De kwetsbaarheid van kritieke infrastructuur is veel groter in volle zee, waar vrijheid van scheepvaart geldt en het complexer is om toezicht uit te oefenen vanwege de zeebodem en de technische middelen die nodig zijn om het toezichtgebied te vergroten. Buiten de exclusieve economische zone van een land is het moeilijk om een aanval of sabotage aan een vijandige persoon, organisatie of mogendheid toe te schrijven.

De Belgische Defensie werkt samen met het *Centre of Excellence* van de NAVO in Italië. Met het STAR-plan hebben we een strategie voor technologische ontwikkeling die onder meer de uitbreiding van partnerschappen met onderzoekscentra en private partners omvat. Er wordt 1,8 miljard euro geïnvesteerd in onderzoek en ontwikkeling. We willen ook daarbuiten met onze Belgische bedrijven samenwerken.

(Nederlands) Via DIANA en het European Defence Agency lopen er momenteel verschillende initiatieven voor de ontwikkeling van nieuwe technologieën.

(Frans) De opdrachten inzake beveiliging en ongeschoold onderhoud kunnen uitgevoerd worden door PROTER (*protection territoriale*). PROTER is een detachement dat zich paraat houdt als snelle interventiecapaciteit, in coördinatie met de provinciale militaire commando-eenheden, de civiele overheden en de politie.

(Nederlands) De ontwikkeling van de nationale logistieke hub waarin het STAR-plan voorziet, zal bijdragen aan het verbeteren van de militaire mobiliteit, ook nationaal, en daarmee aan de

du pays. Ce hub agira comme un centre d'expertise pour la préparation et la projection d'équipements.

01.14 **Philippe Pivin** (MR): J'ai reçu un certain nombre de réponses, mais Madame Verlinden a beaucoup renvoyé aux compétences d'autres ministres. Je regrette dès lors que le champ de la discussion ait été limité à l'Intérieur et à la Défense, alors que d'autres collègues du gouvernement sont concernés par les infrastructures critiques.

Le renvoi à la responsabilité des opérateurs privés n'exonère pas le gouvernement de la sienne. Les opérateurs privés doivent élaborer des plans, mais le gouvernement doit s'assurer qu'ils répondent aux menaces. Des analyses sont-elles effectuées pour vérifier la qualité de ces plans? Des conclusions en ont-elles été tirées?

01.15 **Theo Francken** (N-VA): Moi aussi, j'ai été profondément choqué lorsque j'ai appris que le gazoduc Nord Stream 1 a été saboté à l'aide d'explosifs. J'ai été surpris que certains soient prêts à aller si loin dans le sabotage d'importantes infrastructures gazières. Apparemment, ces infrastructures sont de vraies cibles aujourd'hui. C'est pourquoi je me réjouis que de nombreuses initiatives aient été prises, notamment pour que l'opinion publique sache que la question nous préoccupe.

Nous déposerons une résolution à ce sujet qui pourra davantage alimenter le débat.

L'incident est clos.

La réunion publique de commission est levée à 16 h 12.

veerkracht van het land. Dit knooppunt zal fungeren als expertisecentrum inzake voorbereiding en projectie van uitrusting.

01.14 **Philippe Pivin** (MR): Ik heb een aantal antwoorden gekregen, maar mevrouw Verlinden heeft vaak verwezen naar de bevoegdheden van andere ministers. Ik betreur dan ook dat de scope van de discussie beperkt werd tot Binnenlandse Zaken en Defensie, terwijl andere collega's van de regering ook bevoegd zijn voor de kritieke infrastructuur.

Het is niet omdat de regering verwijst naar de verantwoordelijkheid van de privéoperatoren dat zij in dezen geen verantwoordelijkheid draagt. De privéoperatoren moeten de plannen opstellen, maar de regering moet zich ervan vergewissen dat die plannen het mogelijk maken aan de dreigingen het hoofd te bieden. Worden er analyses verricht om de kwaliteit van die plannen te toetsen? Werden er daaruit conclusies getrokken?

01.15 **Theo Francken** (N-VA): Ook ik was danig geschrokken toen Nord Stream 1 werd opgeblazen. Het verbaasde me dat men zo ver ging in het saboteren van belangrijke gasinfrastructuur. Blijkbaar zijn dat vandaag echte doelwitten. Daarom juich ik toe dat er heel wat initiatieven zijn genomen, ook al om aan de publieke opinie het signaal te geven dat we met de zaak bezig zijn.

We zullen hierover een resolutie indienen die het debat verder kan voeden.

Het incident is gesloten.

De openbare commissievergadering wordt gesloten om 16.12 uur.