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

_____

De openbare commissievergadering wordt geopend om 14.06 uur en voorgezeten door de heren Peter Buysrogge et Ortwin Depoortere.
La réunion publique de commission est ouverte à 14 h 06 et présidée par MM. Peter Buysrogge et Ortwin Depoortere.

De teksten die in cursief zijn opgenomen in het Integraal Verslag werden niet uitgesproken en steunen uitsluitend op de tekst die de spreker heeft ingediend.
Les textes figurant en italique dans le Compte rendu intégral n'ont pas été prononcés et sont la reproduction exacte des textes déposés par les auteurs.

Peter Buysrogge, voorzitter: Collega's, ik open samen met mijn collega-commissievoorzitter van de commissie voor Binnenlandse Zaken de gezamenlijke commissie voor Landsverdediging en Binnenlandse Zaken. Op de agenda van vandaag staat een gedachtewisseling met de ministers van Binnenlandse Zaken en Defensie over de kritieke infrastructuur. De aanleiding voor het debat was het moment waarop de Nord Stream 2-pijpleiding ontplofte en er vragen rezen over de manier waarop ons land is georganiseerd op het vlak van onze kritieke infrastructuur. De vraag om daarover een gedachtewisseling te kunnen organiseren, was gesteld door Theo Francken. Wij zijn erin geslaagd om hier vandaag samen te komen – wat geen evidentie is – om de gedachtewisseling te kunnen organiseren.

Voor de orde der werkzaamheden stel ik voor dat wij eerste beide ministers de kans geven een introductie of inleiding te geven. Zij hebben ook op voorhand de verschillende ingediende vragen gekregen. Ik ga er dus van uit dat zij in hun antwoorden daarnaar al zullen verwijzen en er in de mate van het mogelijke een antwoord op zullen geven. Vervolgens zullen wij een rondvragenrepliek openen, waarvoor ik voorstel te werken in de volgorde van de grootte van de fracties. Iedereen die een vraag heeft ingediend, moet dan maar verwijzen naar zijn of haar vraag, indien die vraag onvoldoende werd beantwoord.

Gaat iedereen akkoord dat wij op die manier werken? *(Instemming.)*

Ik geef ook nog mee dat een vraag was ingediend door de heer Ducarme. Hij heeft echter gevraagd zijn vraag in te trekken. Ze is van de agenda gehaald teneinde die vraag te kunnen behandelen in de commissie voor Defensie zelf, tijdens een volgende commissievergadering. Ze zal dus nog apart worden behandeld in de commissie voor Defensie.

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 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 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 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 **Ludivine Dedonder**, ministre: Monsieur le président, nous avions prévu une courte introduction, suivie des questions et, pour terminer, les réponses aux questions.

Peter Buysrogge, voorzitter: U mag beginnen, mevrouw de minister. Vervolgens zullen de leden repliceren, waarna u de kans krijgt om eventueel aanvullingen te doen. Het Parlement heeft uiteindelijk wel het laatste woord om al dan niet nog iets toe te voegen.

01.02 Minister **Annelies Verlinden**: Beste voorzitters, beste leden, ik zal vandaag ingaan op de rol van Binnenlandse Zaken bij de bescherming van de kritieke infrastructuren. In het bijzonder zal ik toelichten welke acties ondernomen werden door de diensten van Binnenlandse Zaken naar aanleiding van de lekken in Nord Stream 1 en Nord Stream 2.

Conformément à la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, le Centre de crise national (NCCN) coordonne la politique nationale en matière d'infrastructures critiques en Belgique.

Dans les secteurs critiques définis par ladite loi, à savoir l'énergie, les transports, les finances, les télécommunications, les infrastructures numériques, la santé, l'eau potable et le secteur spatial, les infrastructures critiques peuvent être identifiées après une analyse menée par les autorités sectorielles et en coopération et concertation avec le NCCN.

Les autorités sectorielles sont chargées de désigner formellement ces infrastructures critiques après avis du NCCN et sont également responsables des inspections des plans et mesures de sécurité de l'exploitant. Les obligations à respecter s'il s'agit d'une infrastructure critique concernent des aspects de sécurité interne, d'une part, et de protection externe, d'autre part.

Voor de interne beveiliging maakt de exploitant van kritieke infrastructuur, na de aanduiding als kritieke infrastructuur, het beveiligingsplan van de exploitant, het zogenaamde BPE. De maatregelen worden

opgesteld op basis van een risicoanalyse die door de exploitant wordt uitgevoerd. Aan die risicoanalyse worden dan permanente en graduele beveiligingsmaatregelen gekoppeld. Terwijl de eerste beveiligingsmaatregelen permanent zijn – het woord zegt het zelf –, kunnen de graduele maatregelen door de exploitant worden genomen in het geval van een verhoogde dreiging op basis van een dreigingsanalyse van het OCAD. Die punctuele analyse wordt opgesteld wanneer het OCAD weet heeft van een concrete of plausibele dreiging tegen een kritieke infrastructuur, om zo tot een concreet dreigingniveau voor die infrastructuur te komen. De exploitant is er ook aan gehouden om oefeningen met betrekking tot het BPE uit te voeren en het BPE, indien nodig, aan te passen.

De sectorale overheid heeft de verplichting om minstens één keer om de vijf jaar na te gaan of de lijst met geïdentificeerde kritieke infrastructuren nog actueel is. Zo vond voor de telecom- en de energiesector in de eerste helft van 2022 een herziening plaats.

Het OCAD is verantwoordelijk voor de opmaak van de strategische dreigingsanalyses per subsector of sector en voert die dreigingsanalyse ten minste elke vijf jaar uit. De strategische analyse voor elke kritieke infrastructuur wordt op basis van de input van de betrokken steundiensten bij het OCAD uitgevoerd. In die analyse kijkt men niet alleen naar de dreiging van extremisme en terrorisme, maar ook naar die van activisme, spionage, inmenging en georganiseerde misdaad. Het OCAD gaat dan na of er actuele dreigingen zijn en bekijkt ook antecedenten in binnenland en buitenland, alsook nieuwe modi operandi. Op basis daarvan worden de meest plausibele dreigingscenario's naar voren geschoven. Die scenario's helpen de exploitant om het veiligheidsplan te optimaliseren.

De exploitant is eveneens verplicht om een beveiligingscontactpunt dat de klok rond functioneert te communiceren aan de sectorale overheid, het crisiscentrum en de politiediensten.

En ce qui concerne la protection externe, les mesures pour la protection externe des infrastructures critiques sont déterminées par le Centre de crise sur la base d'une menace accrue concrète.

La base juridique permettant au Centre de crise de prendre de telles mesures figure dans la directive ministérielle MFO-5 relative aux missions à caractère fédéral à exécuter par la police locale lors des missions de protection spéciale des personnes et des biens mobiliers et immobiliers du 23 décembre 2002. Cette directive stipule que le Centre de crise peut imposer des mesures pour la protection des installations critiques, vitales et sensibles des bâtiments abritant une activité régulière ou ponctuelle de type politique, culturel, religieux ou autres qui font l'objet de menaces.

Pour déterminer ces mesures, le Centre de crise utilise divers outils et recourt aux connaissances et à l'expertise de différents services partenaires. Le Centre de crise s'appuie, entre autres, sur les analyses de la menace de l'OCAM. D'une part, des évaluations sont demandées à intervalles réguliers pour les infrastructures critiques et certaines infrastructures sensibles. D'autre part, le Centre de crise demande également des évaluations à la suite d'incidents concrets survenus en Belgique mais également à l'étranger.

Les informations issues de ces analyses de la menace sont intégrées dans des analyses de risque établies par le Centre de crise. Ces analyses constituent la base finale pour l'adaptation de certaines mesures de protection, policières y incluses. La mise en œuvre est assurée par la police locale avec éventuellement le soutien de la police fédérale.

Lorsqu'un incident grave se produit, le Centre de crise organise une réunion de coordination avec tous les services partenaires concernés comme la zone de police locale, les différents services de la police fédérale, les services de renseignement, les partenaires privés éventuels, etc.

Lors de cette réunion de coordination, un état des lieux est dressé et la décision est prise d'adopter certaines mesures de protection. Ces mesures peuvent être imposées également par le Centre de crise. D'autres sont initiées par les services partenaires eux-mêmes sur une base volontaire.

Wat het incident van 26 september 2022 betreft, de oorlog in Oekraïne heeft duidelijk een grote impact op ons land. Vandaag is met de helikoptercrash in Kiev, waarbij mijn collega-minister van Binnenlandse Zaken van Oekraïne is omgekomen, opnieuw gebleken hoe dramatisch de situatie ter plaatse blijft. Het is goed om daar even bij stil te staan.

Zoals ik al heb uiteengezet, maakt het OCAD de dreigingsanalyses op voor de kritieke infrastructuur, waarbij

het kan rekenen op de informatie en inlichtingen van alle steun- en partnerdiensten. Daarnaast heeft de Nationale Veiligheidsraad naar aanleiding van de oorlog in Oekraïne vorig jaar ook beslist om het mandaat van het OCAD uit te breiden naar dreigingen die interstatelijk kunnen zijn. Naast de dreigingen voor terrorisme en extremisme moet het OCAD dus ook de interstatelijke dreigingen opvolgen. Dat wordt nader uitgewerkt in het Coördinatiecomité voor Inlichting en Veiligheid (CCIV), waaraan het OCAD uiteraard ook deelneemt.

Vorig jaar waren er in september lekken in de pijpleidingen Nord Stream 1 en 2. Ook al zijn de bevoegdheden van mijn diensten Binnenlandse Zaken inzake gasbevoorrading beperkt, het Crisiscentrum heeft meteen actie ondernomen toen het nieuws bekend raakte. Zo is er dadelijk contact opgenomen met de algemene directie Energie van de FOD Economie, waarbij werd bevestigd dat er geen onmiddellijke impact was op de bevoorradingszekerheid van de Europese Unie. Sinds 31 augustus 2022 werden er namelijk geen volumes via Nord Stream 1 meer doorgevoerd en Nord Stream 2 is nooit in gebruik genomen.

Het Crisiscentrum heeft dan ook verschillende acties ondernomen. In de eerste plaats is aan het OCAD een evaluatie gevraagd van de interstatelijke dreiging tegen de Belgische gasinfrastructuur. Voorts zijn er meerdere vergaderingen georganiseerd om de situatie te bespreken met de betrokken partnerdiensten, zoals de inlichtingendiensten en het OCAD.

Daarnaast is vanuit het Crisiscentrum een waarschuwing verstuurd naar de exploitanten van kritieke infrastructuur in alle sectoren, met de vraag om de levering van hun essentiële diensten te blijven verzekeren, extra waakzaam te zijn en de al geïmplementeerde maatregelen te allen tijde strikt na te leven.

Ten slotte is aan de inlichtingen- en veiligheidsdiensten gevraagd om een update te maken van alle dreigingsniveaus. Het besluit van die analyses was dat de incidenten geen aanleiding gaven tot een verhoging van de dreigingsniveaus.

01.03 Minister **Ludivine Dedonder**: Zoals mevrouw Verlinden al heeft aangehaald, is het essentieel om onze kritieke infrastructuren te beschermen. Bij wijze van korte inleiding wil ik er ook aan herinneren dat die bij wet zijn gedefinieerd, elektriciteitsnetwerken, transportsystemen, communicatie-infrastructuren en financiële systemen omvatten en essentieel zijn voor ons dagelijkse leven en onze economie. Het gaat om de veiligheid van ons allemaal en om de welvaart van onze Staat.

Malheureusement, ces infrastructures sont de plus en plus exposées aux menaces de perturbation naturelle ainsi qu'aux cyberattaques, au terrorisme ou encore au sabotage, comme le démontre trop souvent l'actualité. Outre des cyberattaques à l'encontre des services de l'Intérieur, de la Défense et d'autres services de l'État, voire d'hôpitaux dans notre pays, qui ont toutes été contrées, je pense notamment aux explosions – à des fins de sabotage – qui ont touché en septembre dernier les gazoducs Nord Stream 1 et Nord Stream 2 en mer Baltique, construits pour acheminer le gaz russe en Europe.

Als onze kritieke infrastructuur wordt aangetast, zijn de gevolgen per definitie ernstig en langdurig. Vandaar het cruciale belang om ze steeds beter te beschermen en zo een grote impact op ons land en mogelijk ook onze buurlanden te vermijden.

Defensie is verantwoordelijk voor specifieke kritieke infrastructuur in haar patrimonium. Bij Defensie is de ADIV specifiek bevoegd om toezicht te houden op die infrastructuur, in coördinatie met de staf.

En ce qui concerne la protection des infrastructures critiques en général, la responsabilité incombe d'abord et avant tout aux propriétaires et aux exploitants, surtout si ces infrastructures se trouvent en haute mer. La Défense n'a pas de responsabilité explicite à cet égard, mais elle dispose d'un certain nombre de capacités qui, lorsque ses ressources le permettent, peuvent venir en appui ou contribuer aux missions des services civils concernés quand ils en font la demande.

L'ensemble de ces capacités dites duales, qui sont utiles à cet effet, sont assurées par le Plan STAR et par la loi de programmation militaire 2023-2030. Dans le cas de la protection des infrastructures critiques, elle concerne plus spécifiquement les domaines de la marine, du cyber et de la BPO (Belgian Pipeline Organisation).

La Défense met également à profit son expertise et ses capacités dans le cadre d'incidents, menaces ou attaques CBRN, c'est-à-dire en lien avec des produits chimiques, biologiques, radiologiques et nucléaires.

Elle intervient en plus notamment dans des missions de police aérienne.

Defensie draagt daarmee bij aan de versterking van de beveiliging van onze kritieke infrastructuren op nationaal niveau. Naast investeringen in veiligheidstechnologie omvat haar bijdrage uiteraard ook de vorming van het personeel en een interdepartementale samenwerking.

Tot slot wordt het vermogen van Defensie en van ons land om snel en effectief te reageren op eventuele bedreigingen, ook versterkt door onze nauwe samenwerking met onze strategische partners in de Europese Unie en de NAVO.

Voilà, brièvement, quelques mots d'introduction que je voulais rappeler avant de répondre à vos questions et de revenir plus en détail sur les points relatifs aux missions et aux tâches de la Défense en matière de protection de nos infrastructures militaires et critiques.

01.04 **Yngvild Ingels** (N-VA): Ik dank de ministers voor hun toelichting, ook al heb ik niet veel nieuws gehoord.

In het kader van onze gedachtewisseling heb ik een eerste vraag, namelijk over een multirisicoaanpak. Iedereen heeft wel een rol te spelen in de analyse van de dreiging voor kritieke infrastructuren. Ook door een calamiteit zoals een overstroming of aardbeving kan de kritieke infrastructuur out zijn. In Europa is men nu elf nieuwe risicogebieden aan het bekijken, waaronder natuurrampen.

Is men in België al bezig met het nemen van maatregelen in het kader van een multirisicoaanpak? Ik herinner mij bijvoorbeeld dat er een kritieke infrastructuur in de sector energie werd aangeduid die niet alleen in een overstromingsgebied lag, maar ook nog eens onder een landingszone van vliegtuigen, vlakbij de luchthaven van Zaventem. Ook met die risico's moet rekening worden gehouden, want naast risico's als terreurdreiging en sabotage kunnen die factoren ook een impact hebben.

Hoever staat het met de multimodale risicoaanpak in België, in het licht van de aanpak die nu in Europa tot ontwikkeling wordt gebracht? Wat is er op dat vlak al gebeurd?

Ten tweede, naar aanleiding van de sabotage van de Nord Stream heeft von der Leyen ook verwezen naar het gebruik van satellieten om de zaak beter op te volgen. Men zou dat doen in coördinatie met de NAVO. Welke rol speelt België daarin? Nemen wij daaraan deel? Zijn wij ook actief in de monitoring met satellieten?

Ten derde, onze eerste minister heeft in het begin van de oorlog in Oekraïne ook gezegd dat er jaarlijks 1,2 miljoen euro extra zou worden vrijgemaakt om België beter te wapenen tegen vooral cyberaanvallen op onze kritieke energie-infrastructuur.

Daarvoor zouden achttien specialisten worden aangeworven. Wat is er met de centen gebeurd? Zijn de analisten er? Lopen de aanwervingen? Over welke uitbatingen gaat het juist? Worden er ook gelijkaardige inspanningen geleverd voor andere sectoren dan de energiesector?

Ten vierde, de sectoraanpak, met sectorale verantwoordelijkheid, die in België al tientallen jaren wordt gehanteerd, is mijns inziens de juiste. Wij mogen evenwel niet vergeten dat er ook intersectorale invloeden mogen zijn. Het is goed de zaken per sector te bekijken, maar iemand moet ook het overzicht houden, zodat wij niet in silo's beginnen te denken. Er kan ook een risico bestaan als er intersectoraal zaken gebeuren.

Ten vijfde, ik heb nog een vraag over de Directie beveiliging (DAB). Hoe wordt zij nu nog ingezet voor de bewaking van de kritieke infrastructuur? Zijn er nog permanente bewakingen bezig of is dat meer ad hoc? Hoe zal dat verder worden uitgerold?

01.05 **Éric Thiébaut** (PS): Madame la ministre de l'Intérieur, dans votre note de politique générale 2023, vous indiquiez que les effectifs de la DAB seront élargis durant les prochains mois tout en nous informant qu'une augmentation du nombre d'agents de 1 343 personnes sur les 1 600 prévues initialement avait vu le jour en 2022.

Déjà en septembre dernier, nous vous interrogions sur ce manque d'effectifs qui s'élève à 250 ETP au sein du corps de police fédérale, alors que les tâches de sécurisation s'intensifiaient autour de la tenue du procès des attentats terroristes.

Nous évoquions aussi la protection de nos infrastructures critiques. Comme annoncé précédemment, votre note réaffirmait la reprise des missions de sécurisation des sites nucléaires assurées auparavant par la Défense, sites situés en Flandre (Doel, Mol, Geel, Dessel), depuis ce 1er janvier.

À cet égard, madame la ministre, permettez-moi de vous interroger. Quelles sont vos ambitions concernant l'augmentation des effectifs de la DAB pour 2023? Comment remplirez-vous ces objectifs? Qu'en est-il de la concertation sociale face à ce manque de personnel?

Quelle sera la répartition des effectifs mis à la disposition de la DAB pour la sécurisation de chacun des sites nucléaires du pays ainsi que du nombre de ces derniers dédiés à la sécurisation du procès des attentats terroristes?

La DAB est-elle déployée ou le sera-t-elle prochainement dans la protection d'autres infrastructures critiques? Dans l'affirmative, lesquelles?

Enfin, un renforcement des missions et formations de la DAB dans la protection de nos infrastructures critiques est-elle prévue au regard de l'actualité?

01.06 **Steven Creyelman** (VB): De beveiliging en bescherming van onze kritieke infrastructuur is een pertinent thema. Niemand zal daarvan het belang ontkennen, dat hoop ik tenminste.

Mijn eerste vraag gaat over de definitie van die kritieke infrastructuur. U verwijst beiden naar wat de regelgeving daarover bepaalt en daar kan ik u geen ongelijk in geven. Wat beschouwt u als kritieke infrastructuur, zowel op materieel als immaterieel vlak? Bestaat er bijvoorbeeld een duidelijke lijst, zonder al te brede sectoren te definiëren? En is die lijst dynamisch? Minister Verlinden heeft dat echter al goed geschetst in haar inleiding.

Wordt die lijst regelmatig up-to-date gehouden? Dat zou om de vijf jaar gebeuren, heb ik begrepen. Welke parameters worden er gebruikt om een bepaalde infrastructuur toe te voegen of te schrappen? Ook die vraag is al deels beantwoord door mevrouw Verlinden. Graag krijg ik toch wat meer uitleg en toelichting over de gebruikte parameters.

Ik ga ook even dieper in op het zogenaamde immateriële, niet-fysieke onderdeel. Het gaat vaak over de beveiliging van bepaalde militaire of burgerlijke infrastructuur, maar daar is ook een cybercomponent aan verbonden. Ik trap een open deur in: die component is natuurlijk inherent aan onze maatschappij. Cyberveiligheid is een onderdeel van een goed veiligheidsbeleid, en die kan en mag niet onderschat worden. Een goed uitgevoerde, grootschalige cyberaanval kan data compromitteren, communicatienetwerken platleggen, energienetwerken verstoren, enzovoort. Ik hoef niet te verwijzen naar wat er in de aanloop naar de Russische inval in Oekraïne is gebeurd.

Er moet dus op een holistische manier worden omgegaan met die veiligheid van onze kritieke infrastructuur.

Daarom denk ik dat het goed is dat we vandaag samenzitten met de departementen van Binnenlandse Zaken, Veiligheid en Defensie. Van de beide ministers heb ik gehoord hoe zij daaraan werken in hun eigen departementen. Kunt u toelichten hoe uw beide departementen samenwerken om onze veiligheid te garanderen?

Collega's, er zijn de laatste tijd heel wat alarmbellen afgegaan met betrekking tot onze cyberveiligheid. Daarmee trap ik nogmaals een open deur in. We kregen in 2022 te kampen met een aantal grootschalige cyberaanvallen. Zo werd in Frankrijk een aantal zorginstellingen geviseerd. Ook uw beide departementen weten waarover ik spreek. Ze werden immers beide het slachtoffer van cyberaanvallen die kunnen worden toegeschreven aan Chinese hackerscollectieven.

De reactie van onze overheid op deze Chinese aanvallen kwam er via het kabinet Buitenlandse Zaken en stelde dat China zijn grondgebied niet mag laten gebruiken voor kwaadaardige cyberactiviteiten. Ons land riep China zelfs op om alle gepaste en mogelijke maatregelen te nemen om de situatie te detecteren, te onderzoeken en aan te pakken. Ik kan mij inbeelden dat de Chinezen daar nog steeds niet van bekomen zijn en dat ze nog steeds zitten te bibberen bij de psycholoog na een dergelijke reactie.

Sta mij toe om dat een naïeve houding te vinden ten aanzien van onze vrienden in Peking. Het is een publiek geheim dat deze hackersgroepen verantwoording afleggen aan de Chinese communistische partij. De Chinese overheid is de opdrachtgever. Dus waarom zou China in godsnaam maatregelen nemen tegen zijn eigen hackers? Dat is eigenlijk geen vraag, want ze stellen is ze al gedeeltelijk beantwoorden.

Ik heb wel een concrete vraag met betrekking tot de aanvallen. Bent u door de Chinese instanties al op de hoogte gebracht van de stappen die zij hebben gezet tegen de hackersgroepen die achter de cyberaanvallen en de dreiging tegen ons land zaten en waarschijnlijk nog steeds zitten?

Welke maatregelen hebben wij ondertussen genomen om onze infrastructuur beter te beveiligen tegen buitenlandse hackers? Zijn er bijkomende maatregelen genomen? Bent u van mening dat de huidige veiligheidsmaatregelen voldoende zijn?

Een punt dat de collega's misschien niet zullen aanhalen is het debat over de attributie van die cyberaanvallen. Ook het debat over het beleid dat we ter zake ontwikkelen woedt nog volop. Collega Michael Freilich heeft in een niet zo ver verleden daarover nog een voorstel van resolutie ingediend. Ook het internationaal recht omtrent cyberaanvallen is nog in volle ontwikkeling. De vraag blijft of dit soort van hybride oorlogsvoering als een gewapende aanval kan of moet worden beschouwd, waarna dan een proportionele reactie van zelfverdediging gewettigd is. Ik had graag de visie daarop van de dames ministers gehoord.

Volgens ons moet een cyberaanval tegen kritieke infrastructuur krachtdadig kunnen worden beantwoord. Ons cyberveiligheidsbeleid moet dus niet alleen over defensieve capaciteit beschikken maar ook over offensieve. Als ik mevrouw Dedonder in het verleden goed heb begrepen, heeft zij ook plannen in die richting. Dat is een goede zaak.

Wanneer we met relatief grote zekerheid weten dat staten als China en Rusland ons bestoken met cyberaanvallen, moeten we met gelijke wapens kunnen reageren. Een van de voorwaarden is natuurlijk dat een cyberaanval met aan zekerheid grenzende waarschijnlijkheid aan een bepaalde actor of staat moet kunnen worden toegewezen. Het is moeilijk om te bewijzen dat een statelijke actor achter een bepaalde cyberaanval zit, niet het minst omdat China altijd zegt dat het om private initiatieven gaat. Ik hoef u natuurlijk niet uit te leggen hoe de vork daar aan de steel zit.

Hoe staat het met de uitrol van die toewijzingsprocedure voor cyberaanvallen? Welke parameters neemt u in overweging voor de attributie van die cyberaanvallen?

Mevrouw Dedonder, mijn volgende vraag voelde u wellicht al aankomen. Ik peil graag nog eens naar de uitbouw van de cybercomponent, waarvoor de ADIV de algemene instelling wordt. Hoe staat het met die cybercomponent, bijvoorbeeld inzake personeelswerving? Kunt u voldoende bekwame IT'ers aantrekken? Ik zal maar niet weer uitweiden over de verloning, die in de privésector toch net iets anders is dan wat Defensie kan bieden. Bent u nog altijd zinnens om uitdagende opleidingen aan te bieden aan die IT'ers om hun talenten binnen Defensie te kunnen ontplooien?

Ik weet dat u zeker zult antwoorden dat Defensie die cybercomponent aanprijst met het argument dat men voor Defensie wel zaken zal mogen doen die elders verboden zijn. In welke mate heeft dat al tot concrete resultaten geleid?

Hoe staat het met de veiligheid van onze energie-infrastructuur? Zijn er extra beveiligingsmaatregelen getroffen na de sabotage van de Nord Stream-pijpleiding om onze kritieke infrastructuur beter te beschermen, afgezien van het reeds vermelde overleg waar minister Verlinden over sprak?

Ik wil ook nog even terugkomen op de cyberaanval op de diensten van de stad Antwerpen, die niet als een kleinschalige operatie kan worden aangemerkt, integendeel zelfs. We hebben vastgesteld dat de stat Antwerpen in een soort digitale lockdown is moeten gaan. Het zou nog tot het einde van deze maand duren om de gevolgen ervan weg te werken. Welke samenwerking was en is er tussen de stad Antwerpen en uw respectievelijke departementen? Is er regelmatig overleg tussen de verschillende beleidsniveaus bij dit soort cyberaanvallen? Is er al enige synergie voortgevloeid uit dat overleg?

Als afsluiter heb ik nog een paar vragen over de incidenten in de steden en gemeenten Antwerpen, Zwijndrecht en Diest. Hebben uw departementen een draaiboek cybercrime voor de bescherming van

kritieke infrastructuur tegen cyberaanvallen, ook voor die lokale en lagere overheden? Ik had begrepen dat dat het geval was. Begeleidt u de geviseerde infrastructuur structureel? Bestaan er impactanalyses per sector, per zorginstelling, als ik dat zo mag noemen? Zijn er continuïteitsplannen voorzien waarmee die kritieke processen in kaart gebracht kunnen worden? Wordt er bepaald binnen welke termijn die kritieke processen heropgestart moeten kunnen worden en welke stappen daartoe moeten worden ondernomen?

Mijn laatste vraag gaat over iets waaraan het overheden vaak ontbreekt, namelijk een duidelijk communicatieplan voor het geval er zich een calamiteit op dat vlak voordoet. Is er een communicatieplan dat bepaalt wat er gecommuniceerd wordt, wanneer en hoe dat gebeurt, door wie en met wie? Als we de doelgroepen, de communicatiekanalen en de mogelijke boodschappen op voorhand in kaart brengen, dan komt dat een sterke en duidelijke crisiscommunicatie alleen ten goede. Daar kunnen we het allemaal over eens zijn volgens mij. Graag kreeg ik ook daarover wat meer toelichting.

01.07 **Philippe Pivin** (MR): Monsieur le président, madame la ministre, je pense que chacun s'accordera à dire que la nécessité de garantir une capacité de sécurisation suffisante des infrastructures et des services critiques, c'est une évidence et ce, depuis quelques années déjà. Mais il faut quand même se souvenir que ce n'était pas tout aussi évident avant 2014.

Chacun se rappellera aussi qu'à l'époque des attentats à Maelbeek et à Zaventem, on avait fait le constat d'une absence complète de plan d'urgence en cas d'attentat terroriste. Plus récemment, chacun se souviendra du manque de moyens et de l'absence de culture du risque constatés après les inondations de l'été 2021. Je pointe ici deux situations très différentes qu'on doit redouter car les menaces sont réelles dans un cas comme dans l'autre et qui montrent que ce sont des dossiers qu'on ne doit pas traiter comme le commun des dossiers en commission de l'Intérieur ou en commission de la Défense. Je crois que, pour ces dossiers, on doit s'assurer qu'il y a une gestion suffisamment efficace en amont pour éviter de devoir faire des constats de carence ou de lacune en aval, même si la difficulté de l'exercice réside dans le fait que, généralement, on ne vérifie que tout a bien été prévu qu'en cas de catastrophe avérée. Il importe, toutefois, de s'assurer d'une bonne gestion en la matière.

J'ai posé un certain nombre de questions à l'attention principalement, si pas exclusivement, de la ministre de l'Intérieur, catégorisées par secteur, (énergie, eau, etc.) ainsi que des questions plus générales. Je les ai déposées comme cela avait été demandé et je m'y réfère pour permettre à d'autres collègues de s'exprimer.

Les réseaux informatiques:
Ces menaces sont évidemment importantes et denses en quantité. Il apparaît cependant que des moyens supplémentaires peuvent être apportés?
Quelles mesures nouvelles et investissements nouveaux ont-ils été décidés pour protéger les systèmes numériques de gestion des opérateurs des services essentiels du pays, les infrastructures critiques et notamment les installations privées essentielles comme les établissements hospitaliers?

Secteur de la santé:
Précisément, quelles normes sont-elles en vigueur en matière de protection des données médicales? De protection des systèmes informatiques des établissements hospitaliers?
Quel soutien spécifique est-il apporté aux hôpitaux dans ce cadre? Quel point de contact existe ou doit exister dans les établissements publics et privés et le Centre de Crise?

Etablissements pénitentiaires et lieux de Justice:
Alors que le serveur central du SPF Intérieur avait été piraté il y a deux ans, quelles mesures spécifiques de protection existent au niveau des systèmes numériques qui gèrent les données et espaces internes des prisons? De quelle façon des lieux de Justice sont-ils désignés infrastructures critiques et sécurisés dans notre pays?

Stockages armement Police et Défense:
Compte tenu de la gestion constatée des stocks d'armes à feu, pourriez-vous m'indiquer comment sont sécurisés les stocks d'armements de la police d'une part, et de la Défense d'autre part avec le soutien de la police?
Pouvez-vous m'indiquer quelles mesures nouvelles ont été prises depuis 2021 pour sécuriser ces lieux?

Globalement:

Comment sont évalués les systèmes de sécurité de ces infrastructures? Des procédures différentes existent-elles entre les contrôles et audits en fonction du caractère public, semi-public et privé des infrastructures?

Des rapports du Centre pour la Cybersécurité Belgique concernant les secteurs vitaux font-ils état de la nécessité de moyens supplémentaires de protection et de sécurisation à apporter pour certains lieux? Si oui quels sont-ils et quelles sont les mesures planifiées en 2023 et 2024?

Combien de signalements d'incidents de sécurité ont-ils été communiqués au Centre de crise, ces trois dernières années, par des infrastructures critiques et pour quelles infrastructures et quelles atteintes ou menaces?

Combien d'intrusions physiques ont-elles été constatées au sein des infrastructures critiques, chaque année, depuis 2019? Quelles sont les infrastructures qui en ont été ainsi victimes?

Combien de piratages ont-ils été décelés dans les systèmes numériques des services essentiels et des infrastructures critiques depuis 2019?

Combien y a-t-il à ce jour d'opérateurs de services essentiels dans le pays, identifiés par le Centre pour la Cybersécurité?

Quels lieux stratégiques sont sécurités par la DAB? Quel effectif global est-il en charge de la sécurisation de l'ensemble des infrastructures critiques et OSE actuellement? Quelle en est l'évolution depuis 2019? Quels services et infrastructures stratégiques et critiques sont-ils sécurisés par des sociétés privées de gardiennage? Avec quelle régularité un screening des agents travaillant à la sécurisation des OSE et infrastructures critiques est-il réalisé?

Combien de mesures de protection externes nouvelles ont-elles dû être décidées par le Centre de crise ces dernières années à la suite d'évaluations de la menace?

Quelles autorités sectorielles ont déterminé des nouvelles mesures internes de protection et quelles nouvelles désignations de « statut » d'infrastructures critiques ont été décidées depuis 2019?

Enfin, concernant l'évaluation des risques à grande échelle portant sur la période 2018-2023 sur les probabilités de risques et précisément les scénarios soumis au changement climatique, pouvez-vous nous indiquer ce qui avait été analysé et déterminé par les experts au niveau des infrastructures publiques de gestion des risques d'inondation? Et précisément dans le Limbourg et la province de Liège? A cet égard, quel nouveau Belgian National Risk Assessment est-il conçu pour les prochaines années? Je vous remercie.

01.08 **Franky Demon** (cd&v): Ministers, door Poetins vreselijke oorlog in Oekraïne kregen we het afgelopen jaar ook intern te maken met een gewijzigde veiligheidscontext. We zijn ons meer dan ooit bewust van onze strategische onafhankelijkheid, zeker ook wat onze energiebevoorrading betreft. Het incident in september met de Nord Stream-gaspijpleiding is in dat kader tekenend. Het is dan ook naar aanleiding daarvan dat we onze gedachtewisseling houden.

Ik heb enkele zaken op voorhand schriftelijk ingediend en zal deze hier niet allemaal herhalen.

De beleidsnota van Binnenlandse Zaken voor 2023 ging uitgebreid in op de bescherming van onze kritieke infrastructuren. Ze gaf ook de belangrijke vaststelling mee dat bepaalde deadlines inzake de dreigingsanalyses niet werden gehaald door een capaciteitstekort bij het OCAD en de gebrekkige informatiedoorstroming met sommige partnerdiensten. In de nota gaf u, mevrouw de minister, eveneens aan dat het OCAD in het najaar van 2022 zou worden versterkt met bijkomend personeel en dat er overleg zou volgen om het gebrek aan informatiedoorstroming aan te pakken.

Dat zijn allebei noodzakelijke en belangrijke stappen. De internationale situatie toont duidelijk aan dat wij op dit moment niets aan het toeval mogen overlaten. We rekenen op u om te bewerkstelligen dat de dreiging ten opzichte van onze kritieke infrastructuren regelmatig en tijdig wordt geëvalueerd.

Zoals gezegd is de aanleiding van deze gedachtewisseling het incident met de gaspijpleiding. Onze energie-infrastructuur verdient, gezien de huidige context, dan ook zeker de nodige prioriteiten. Desalniettemin mogen we ook de andere sectoren niet uit het oog verliezen, zelfs sectoren die vandaag nog niet als kritiek

worden beschouwd.

Ik stelde u rond deze tijd vorig jaar reeds vragen rond de erkenning van de distributiecentra van supermarkten als kritieke infrastructuur. Onze voedselbevoorrading is dan ook een cruciaal element in tijden van crisis. Uit overleg met Comeos onthoud ik de dringende vraag van de voedseldistributiesector om opgenomen te worden op de lijst met kritieke infrastructuren.

Een van de belangrijkste redenen waarom ze deze vraag stellen zijn de mogelijke gevolgen die een eventueel stroomtekort met zich zou kunnen meebrengen. Ik vraag u daarom nogmaals om te heroverwegen om deze sector aan de lijst met kritieke infrastructuren toe te voegen.

Een goede beveiliging van onze kritieke infrastructuur is cruciaal. Binnen de federale politie komt die bevoegdheid in principe toe aan de DAB. In de afgelopen jaren hebt u ingezet op een versterking van die dienst en de opvulling van het personeelskader. In 2022 bent u gekomen tot 1.343 personeelsleden op een voorzien aantal van 1.600. U hebt al aangekondigd dit jaar de capaciteit verder te willen verhogen. Met cd&v geloven wij in het belang van die versterking, zodanig dat wij optimaal kunnen instaan voor de bescherming van onze kritieke infrastructuren. Er ligt hier dus ons inziens een belangrijke taak weggelegd.

01.09 **Tim Vandenput** (Open Vld): Heren voorzitters, dames ministers, bedankt voor uw korte toelichting. Er zijn al veel vragen gesteld, dus ik zal het kort houden.

Als mogelijk probleem wordt er vaak verwezen naar het kluwen van verschillende instanties en bevoegdheden. De minister van Justitie zette bijvoorbeeld al stappen voorwaarts met een nieuwe wet inzake maritieme beveiliging die biometrische toegangscontroles voorziet in de havens, waardoor schepen beter gecontroleerd worden. Ook de kritieke infrastructuur op de Noordzee wordt beter beschermd door de realisatie van het Maritiem Informatiekruispunt.

Hoe verloopt volgens jullie de samenwerking op andere domeinen? Worden er gelijkaardige stappen gezet naar een betere beveiliging?

Is de tijd niet rijp om inzake de veiligheid van alle kritieke infrastructuur naar een eenheid van commando te streven, *one command*, zodat op mogelijke dreigingen efficiënter kan worden gereageerd?

België is een import- en exportland, er komen en gaan veel goederen en ook veel diensten binnen en buiten. Naast de energiebevoorrading behoren daarom de zeehavens en luchthavens tot de kritieke infrastructuur. Bij de luchthavens reken ik ook de militaire luchthavens, want als de militaire luchthavens niet meer functioneren, kunnen wij ons in de lucht niet meer verdedigen. In 2016 lag de luchthaven van Zaventem, de tweede economische poort van ons land, ook weken uit.

Er worden stresstests gedaan, maar is het volgens jullie opinie en ervaring nodig om meer stresstests te doen in de economische poorten en op andere vlakken? De vraag is dus of wij meer oefeningen en stresstests moeten doen om beter voorbereid te zijn op eventuele calamiteiten.

Ten derde, ik heb net zoals twee andere leden een vraag over de DAB, die onder andere instaat voor de beveiliging van de kritieke infrastructuur. Die dienst kampt al jaren met een personeelstekort van ongeveer 250 politiemensen. Wat is de huidige bezetting van de DAB? Hoeveel mensen worden dagelijks ingezet om de beveiliging van de kritieke infrastructuur te verzorgen?

01.10 **Kris Verduyckt** (Vooruit): Mijnheer de voorzitter, mevrouw de minister van Defensie en mevrouw de minister van Binnenlandse Zaken, ik dank jullie alvast voor de inleiding.

De oorlog in Oekraïne heeft ons inderdaad met de neus op de feiten gedrukt. De belangrijkste lessen die wij daaruit leren zijn enerzijds de waarde van energie en anderzijds dat bij dat specifieke thema de kritieke infrastructuur belangrijk is. Eigenlijk zijn beide ook gelinkt aan elkaar. Wanneer wij zien welke installaties bijvoorbeeld al het doelwit waren van aanslagen, wordt enerzijds duidelijk dat die aanslagen worden gepleegd om de zaak te destabiliseren, door de productie of het vervoer aan te vallen. Anderzijds zitten wij in Oekraïne voor de eerste keer in de geschiedenis met een strijdperk waar er ook kerncentrales aanwezig zijn. Qua veiligheid is ook die aanwezigheid een probleem.

Het goede nieuws over energie is dat wij naar een steeds meer decentrale energieproductie zullen gaan in

dit land. Decentraliteit zal de toekomst zijn in de energieproductie. Op dat vlak is een en ander een voordeel. Wij zullen in ons land echter wel een aantal centrale plekken blijven hebben. De kerncentrales die langer openblijven zijn daarvan een voorbeeld. Ook het streven naar een energie-eiland op de Noordzee levert mogelijks een interessant doelwit op voor zij die het slecht voorhebben met onze Staat.

Ik heb nog twee vragen. De andere vragen zijn ondertussen immers al gesteld.

Ten eerste, kunt u op dat laatste, dus het energie-eiland, inzoomen en aangeven op welke manier volgens u beide zich daar mogelijkheden aandienen of waarop ter zake de focus moet liggen om aan dat eiland een redelijke bescherming te kunnen geven?

Ten tweede, mijn tweede vraag gaat in op wat mevrouw Ingels uiteenzette over de satellieten. Observatie is inderdaad een heel belangrijk gegeven. Wij kopen vandaag op dat vlak de dure capaciteit in, hoewel wij op ons grondgebied instellingen hebben die perfect in staat zijn om die observatiecapaciteit te ontwikkelen. Denkt de regering aan een dergelijke piste of blijven we ons daarvoor beroepen op andere naties?

01.11 **Theo Francken** (N-VA): Beste wensen aan mevrouw Verlinden. Ik wens haar veel loopplezier, dat is een goede manier om het hoofd fris te houden. Veel succes ook met de uitdagingen voor 2023.

Frankrijk is in deze problematiek een voorloper. Ik ben niet de grootste fan van het Franse militaire apparaat, dat weten jullie, ik sta meer aan de NAVO-kant. Maar ik volg de Fransen wel van nabij. Ze zijn nu eenmaal onze krachtigste militaire buur, het land is ook een kernmogendheid en het heeft een prachtige defensie. In de parlementaire assemblee van de NAVO heb ik vaak gesprekken met de Franse collega's van de belangrijke commissie Defensie. Die vergadert wekelijks en de persbelangstelling is altijd massaal. Hier is dat iets minder, maar de pers volgt onze vergadering ongetwijfeld online.

De Fransen hebben een grote traditie op het vlak van oorlogsvoering en de opbouw van een verdediging, en daar heb ik veel respect voor. Bijna een jaar geleden, in februari 2022, heeft Frankrijk als eerste natie binnen de NAVO een nationale strategie voor zeebodemoorlogvoering ingevoerd. Ik beveel de minister van Defensie aan om die tekst eens te lezen, om te zien hoe zij dat aanpakken.

In Oostende is het NATO Centre of Excellence voor mijnenbestrijding gevestigd, dat zeker een bezoek waard is. Een paar jaar geleden was niemand daarin geïnteresseerd. Ons land heeft dat binnengehaald en het heeft nu een enorm goede reputatie. Waarom zouden we dat niet uitbreiden naar een NATO Centre of Excellence voor zeebodemoorlogvoering?

Op het gebied van mijnenbestrijding hebben we een zeer goede reputatie. We hebben ook nieuwe schepen aangekocht, die eraan komen. We staan eveneens goed op het vlak van onderwaterdrones. Er is immers een fabriek in Oostende, waar u misschien al geweest bent, ECA, die *unmanned underwater vehicles* (UUV's) produceert.

We hebben dus een enorme expertise in ons land. Het NATO Centre of Excellence hebben we ook al. Mevrouw Dedonder, dit is dus een enorme opportuniteit voor uw industriële defensieraad. U gaat daarmee dit jaar volop aan de slag en misschien kan dat geagendeerd worden. Misschien kunnen wij de *leading force* van de NAVO worden op het gebied van zeebodemoorlogvoering en de bescherming van kritieke infrastructuur. We hebben immers de industrie, het NATO Centre of Excellence, de reputatie en de ervaring. Ik zie hier dus een enorme opportuniteit voor Vlaanderen – of laat ons België zeggen, want ik wil er geen communautair debat van maken, hoewel de Noordzee ligt waar ze ligt – en voor onze economie, Defensie en industrie.

Ik wil ook nog graag een tweede anekdote vertellen.

In totaal hebben we 807.000 mijl onderzeese kabels die we moeten beschermen binnen het NAVO-bondgenootschap. Dat is bijna 1 miljoen mijl aan gasleidingen, kabels en dergelijke. Dat zijn allemaal zaken die we het beste goed bewaken. We hebben immers heel veel vrienden bij de NAVO, maar ook heel veel vijanden, die de laatste tijd redelijk assertief zijn. We moeten daar sowieso naar kijken.

Misschien kunnen we wel iets leren van de Italianen. De Italiaanse marine doet actief aan het beveiligen van heel hun kabelnetwerk in de Middellandse Zee en de Adriatische Zee. Zij hebben daarvoor een akkoord gesloten met het IT-bedrijf Sparkle. Zij zeggen dat ze hun Italiaanse kabels zullen bewaken, beschermen, in

ruil voor toegang tot de kabels. Die kabels detecteren bijvoorbeeld alles wat er beweegt op het vlak van drones en schepen. Die data gaan nu rechtstreeks naar de Italiaanse defensie, die die gegevens permanent analyseert. De Italianen hebben op dit moment een zeer performante kennis van wat er juist reilt, zeilt en vaart op de Middellandse Zee en op de Adriatische Zee, door dat akkoord dat ze hebben gesloten met dat kabelbedrijf.

Zowel u als wij zijn de overheid. Wij zijn de wetgevende macht, u bent de uitvoerende macht. Misschien kunt u wel een akkoord sluiten met een aantal van die privébedrijven, met bescherming van de infrastructuur in ruil voor iets anders. Laten we ook eens naar het Italiaanse model kijken. Laten we ook kijken naar de Franse nationale strategie voor zeebodemoorlogvoering. Laten we dat bundelen in iets waarin we echt kunnen excelleren. We zijn maar een klein land. We zijn niet de beste leerling van de klas als het gaat over NAVO-bijdragen en onze job doen. Dat weten we allemaal en dat is soms ook heel pijnlijk op internationale vergaderingen. Laten we er wel voor zorgen dat we net in die niches heel sterk staan.

Minister Verlinden, maar vooral minister Dedonder, wat vindt u daarvan? Hebt u plannen in dat opzicht?

Ik kondig ook graag 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 de heer Buysrogge, mevrouw Ingels en enkele andere parlementsleden in de Kamer indienen.

01.12 **Yngvild Ingels** (N-VA): Mevrouw de minister, ik was nog één belangrijk element vergeten. Het verbaast me trouwens dat u het zelf niet hebt vermeld. Het Crisiscentrum stelt een globale strategie op om de weerbaarheid van onze samenleving te verhogen. De bescherming van kritieke infrastructuur speelt daarin volgens mij ook een rol. Kunt u daarover wat meer uitleg verschaffen? Wat is de stand van zaken daarvan?

Peter Buysrogge, voorzitter: Als niemand nog het woord vraagt, sluit ik deze vragenronde af en geef ik het woord aan minister Verlinden.

01.13 Minister **Annelies Verlinden**: Mevrouw Ingels, u vroeg in de eerste plaats naar de multirisicoaanpak en hoe we ons voorbereiden op een calamiteit, bijvoorbeeld een overstroming, terwijl er ook nog andere crisissen zijn.

De huidige wetgeving is gebaseerd op de wet van 1 juli 2011, die vooral focust op de *man-made* risico's. Dat betekent natuurlijk niet dat met andere risico's geen rekening wordt gehouden bij de vaststelling van veiligheidsmaatregelen, in het bijzonder door de exploitant in zijn bedrijfsveiligheidsplan. De Critical Entities Resilience-richtlijn zal na omzetting in de Belgische regelgeving er ook 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 wettelijke basis.

U stelt terecht dat die multirisicobenadering deel uitmaakt van de nationale weerbaarheidsstrategie die in opmaak is. Ze wordt gecoördineerd door het Crisiscentrum, dat uiteraard samenwerkt met alle betrokken partners. Het Crisiscentrum vervult veeleer de rol van coördinator dan die van auteur van die technische sectorgebonden aanpak.

Centraal daarbij is een transparante beoordeling van de risico's en de bedreigingen waarmee ons land en de verschillende sectoren en subsectoren kunnen worden geconfronteerd. In de eerste plaats wordt natuurlijk uitgegaan van de erkenning van het bestaan van die risico's. Soms gaat het om de voortdurende aanwezigheid van bepaalde risico's.

Als de oorlog voorbij is verdwijnen sommige risico's, maar andere blijven actueel. De weerbaarheidsstrategie, met de multiriskbenadering gaat dan ook 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. Vanuit dat perspectief wordt ook verder gebouwd op de nationale risicoanalyse BNRA, die geldt om dat te kunnen voorbereiden. Daarbij vertrekken we niet van iets nieuws, maar werken we op basis van de bestaande expertise en benaderingen die we al kennen, om daar verder uit te leren.

Bovendien is het volgens mij erg belangrijk dat de nationale weerbaarheidsstrategie ook rekening houdt met de internationale context en de internationale initiatieven die daar worden genomen, zowel door de NAVO

als door de EU. De NATO *resilience*, met de zeven uitgangspunten, is ook voor ons en voor het Crisiscentrum richtinggevend om de weerbaarheidsstrategie en de multiriskbenadering aan te pakken.

In de context van energie hebben bedrijven ook een intern noodplan dat bij een noodsituatie afgekondigd kan worden. Als Elia, de beheerder van hoogspanningslijnen, een incident zou vaststellen, kan het een intern noodplan afkondigen. Uiteraard is er daarvoor ook overleg met het Crisiscentrum en de andere sectorale overheden, zoals de AD Energie.

Zelfs wanneer ze enkel dat interne noodplan afkondigen, worden de externe partners alsnog voor hen gecontacteerd. Dan zal het Crisiscentrum samen met de betrokken partner en de AD Energie bekijken hoe ernstig het incident is. In functie daarvan worden andere partijen mogelijk op de hoogte gebracht en zullen er afspraken worden gemaakt over de maatregelen die getroffen moeten worden, maar ook over crisiscellen van andere sectoren en departementen die samengeroepen moeten worden om de crisis de baas te kunnen. In het meest extreme geval zou dat dan ook kunnen leiden tot de afkondiging van een federale fase als dat nodig is, met name wanneer er vele actoren over de provinciegrenzen heen bij betrokken zijn.

Wanneer Elia zou vaststellen dat bepaalde infrastructuur moet worden uitgeschakeld, zoals bij het voorbeeld van de overstromingen dat u aanhaalt, dan zal het dat uiteraard ook doen. Dat is trouwens ook de analyse die het maakte in de zomer van 2021.

Bij een noodgeval waarin de gasvoorziening geraakt wordt, is voorzien in de mogelijkheid om de elektriciteitscentrales zoveel mogelijk te vrijwaren van storingen of schokken, om ervoor te zorgen dat de gevolgen van de gasschaarste worden opgevangen in het elektriciteitsnetwerk. In geval van een incident op het gasnetwerk wordt natuurlijk ook getracht om die zo lang mogelijk actief te houden, om in het kader van het afschakelplan te bekijken welke sectoren, domeinen en regio's gevrijwaard kunnen blijven.

Op basis van de ervaringen die wij hebben, kunnen wij ook zeggen dat er in de oefeningen die georganiseerd worden en in de planning veel meer bewust wordt omgegaan met die multirisicobenadering en -aanpak. In de mate van het mogelijke worden meerdere incidenten gecombineerd bij een oefening, bijvoorbeeld terro samen met CBRNe. Op die manier – en dat is iets dat in de praktijk het best werkt – worden mensen geoefend in het omgaan met die risico's. De lijnen worden bijzonder kort wanneer ze dat al eens doorlopen hebben, weliswaar in een *dry run*, maar dan zo realistisch mogelijk.

Dat is ook een van de redenen waarom ik pleit om nog veel meer te oefenen, op elk niveau. Ik heb het hier reeds een paar keer gezegd, onder meer naar aanleiding van de explosies die we hebben gehad en de instorting van de school in Antwerpen. Wij hebben toen in de provincie Antwerpen echt kunnen vaststellen dat men bij de latere incidenten zeer goed geoefend was, helaas door levensechte incidenten. Die kan men echter in grote mate benaderen met oefeningen. Er gebeurt trouwens ook een ronde, soms onder de auspiciën van de gouverneur. Er wordt dan overal rondgegaan en bekeken welke oefeningen, desktop of reallife, kunnen gebeuren.

Uw tweede vraag ging over de monitoring van de satellieten. Dat is in de eerste plaats een vraag voor Defensie. Ter ondersteuning van Defensie kan het Crisiscentrum, via het Emergency Response Coordination Centre, satellietbeelden opvragen en ter beschikking stellen. Dat gebeurt via de eigen kanalen, het eigen netwerk van het Crisiscentrum. Het Crisiscentrum is immers in België de enige *authorised user*. Het zal dat op dat moment doen ter ondersteuning van Defensie.

Andere diensten kunnen ook gebruikmaken van die diensten van het Crisiscentrum, telkens door de vraag te stellen aan het Crisiscentrum. Dat heeft wellicht te maken met licenties en abonnementen. De gouverneurs kunnen die vraag stellen, maar ook de betrokken regionale diensten, via de regionale crisiscentra. Wij proberen ook om die zoveel mogelijk te integreren in de dagelijkse maar ook in de incidentgedreven werking van het Crisiscentrum. Dus ook op dat moment kan die vraag worden gesteld.

De beelden verkregen via het Emergency Response Coordination Centre kunnen dan dienen voor de beeldvorming en het besluitvormingsproces, onder meer binnen Defensie. Zij kunnen echter ook worden gebruikt door de crisiscellen van de verschillende departementen of bij het ondersteunen van een eventuele federale fase. Het Nationaal Crisiscentrum bekijkt momenteel nog de mogelijkheden van de Starlinksatellieten, om ze mee te integreren in de beeldvorming.

U had ook vragen over de verhoging van het budget voor cyberveiligheid. Die vragen stelt u het best aan de

eerste minister – dat geldt ook voor uw vragen, mijnheer Verduyckt – omdat cybersecurity onder zijn bevoegdheid valt.

Een aantal collega's had vragen over de DAB. Ik probeer gegroepeerd uw vragen, mevrouw Ingels, en die van de heren Thiébaut, Demon, Vandenput en Pivin te beantwoorden. 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. Dat weet u, want het stond in de vooropgestelde planning. Daarmee heeft de DAB alle wettelijke verplichtingen inzake nucleaire beveiligingsopdrachten overgenomen van Defensie. Ik dank Defensie voor de uitgevoerde diensten en wens veel goede moed en spreek mijn dank uit aan de politiediensten die dat willen overnemen. Dat is op zich goed verlopen.

Het is zeker geen geheim dat wij de DAB moeten en willen versterken. Om dat initiatief te ondersteunen en om de personeelscapaciteit te versterken, zullen door de Nationale Politieacademie volgend jaar in principe zeven klassen worden georganiseerd om de beveiligingsagenten van de politie op te leiden. De ambitie is om 168 beveiligingsagenten op te leiden. Het gaat over vier Nederlandstalige en drie Franstalige klassen. Zoals in elke sector en elk publiek en privébedrijf moet uiteraard bij de rekrutering en de berekening van de nettotoename rekening worden gehouden met de vertrekkers. Bij de DAB waren er dit jaar achttien natuurlijke vertrekkers. Daarnaast – dat is goed en slecht nieuws tegelijkertijd – zijn er 79 personeelsleden die zijn gestart met de opleiding tot inspecteur of dat nog zullen doen vanaf 1 maart 2023, en die dus ook zullen vertrekken als beveiligingsagent. Op zich is het goed dat mensen hun carrière kunnen ontwikkelen binnen de politie, maar dat betekent natuurlijk ook dat wij moeten blijven werken aan de instroom.

En ce qui concerne le renforcement et le recrutement du service DAB, il est un fait que ce dernier travaille en étroite collaboration avec les directions au sein de la police intégrée: la direction du personnel, du recrutement et de la sélection, pour assurer le suivi du recrutement des futurs agents de sécurisation de police. Il y a aussi des contacts réguliers avec les syndicats pour améliorer les procédures et les fluidifier.

La répartition des effectifs sur l'ensemble des sites et des centrales nucléaires sécurisées par la DAB ne peut pas être communiquée. On ne l'a jamais fait, je crois, et ce pour des raisons de sécurité. Je peux vous communiquer que le dispositif de la DAB pour la sécurisation du procès des attentats terroristes comprend environ 70 membres du personnel mobilisés chaque jour et cela en plus des autres membres de la police intégrée et de la police locale Bruxelles-Nord-Ixelles qui envoie, elle aussi, des agents.

Il n'est actuellement pas prévu que la DAB reprenne d'autres responsabilités, d'autres tâches et d'autres sites pour sécuriser d'autres infrastructures critiques. Je ne pense pas devoir vous détailler les sites ou les activités pour lesquelles la DAB peut être appelée puisque la loi sur la fonction de police les énumère (palais royaux, etc.).

Mais pour être claire, la sécurisation des palais royaux, des infrastructures du SHAPE et de l'OTAN est actuellement assurée par une autre direction de la DG de la police administrative, en attendant que la DAB puisse reprendre ses missions. De cette manière, les responsabilités ont été partagées.

Le calendrier de reprise par la DAB de la sécurisation des activités ou des lieux à la suite de la Défense – à l'époque des attentats de 2016 – est connu et je ne dois pas y revenir.

Je terminerai en donnant quelques détails à propos de la DAB. Je peux vous confirmer que la nomination du personnel de sécurité relève de la responsabilité de l'exploitant d'une infrastructure critique. Des vérifications peuvent être faites à la demande de l'autorité sectorielle sur la base de la loi du 11 décembre 1998 relative à la classification et aux habilitations. Les résultats de ces vérifications sont valables pour une durée de cinq ans. Normalement, l'initiative vient de l'exploitant puis des vérifications sont faites par l'autorité sectorielle, conformément à la législation applicable. Je crois avoir également répondu ou au moins fourni un début de réponse aux questions de M. Thiébaut.

Dan kom ik tot de vragen van de heer Creyelman. Wij geven geen exacte details over de identificatie van de beschermde infrastructuren omwille van de redenen die ik daarnet aangaf, inzonderheid de veiligheid van alle betrokkenen. Het OCAD en het Crisiscentrum maken vertrouwelijke rapporten en dreigingsanalyses op en op basis daarvan worden dan de juiste politiemaatregelen bepaald.

Ik heb tijdens mijn introductie al de definitie van kritieke infrastructuur gegeven. Aan de hand van die parameters worden die infrastructuren aangeduid door de sectorale overheden conform de wet van

1 juli 2011. Dat is de handleiding om te bepalen wat een kritieke infrastructuur is. De precieze identificatie van de kritieke infrastructuren gebeurt aan de hand van parameters en interne sectorale criteria, waarbij de sectoraal bevoegde overheid tijdens het identificatieproces de sectorale criteria zal bepalen waaraan die infrastructuren moeten voldoen en moeten beantwoorden, rekening houdend met de bijzondere eigenschappen van de sector. Het gaat dan onder meer over het aantal potentiële doden of gewonden als gevolg van incidenten met die infrastructuur en de potentiële economische weerslag, zoals de economische verliezen en de kwaliteitsvermindering van producten of diensten. In de analyse van die identificatie wordt ook de weerslag op het milieu opgenomen. Ruimer wordt ook de potentiële weerslag van een aanval op de infrastructuur op de hele bevolking bekeken. Het gaat dan over het vertrouwen van de bevolking, het fysieke lijden, de verstoring van het dagelijkse leven en het uitvallen van essentiële diensten. Men hanteert daarbij door de sectorale overheid berekende drempelwaarden voor de economische verliezen.

De sectorale overheden actualiseren de lijst van kritieke infrastructuren vijfjaarlijks en telkens het nodig is bij evidente wijzigingen. Zij beslissen daartoe voor de sector, met de steun van het Crisiscentrum, dat expertise, mogelijk uit andere sectoren, biedt bij de analyse en de eventuele identificatie van de parameters.

De lijst wordt beheerd door de sectorale overheid. Het spreekt voor zich dat het Crisiscentrum een lijst heeft van de kritieke infrastructuren uit de betrokken sectoren, zodat er contact kan worden genomen met de verschillende partijen bij een multiriskincident.

U had het ook over de cyberaanvallen. Ik heb daarover al kort iets gezegd. De Nationale Veiligheidsraad heeft alvast een procedure voor de attributie van cyberaanvallen uitgewerkt en die hebben we al een paar keer toegepast, onder meer voor de cyberaanval op de FOD Binnenlandse Zaken. Naar aanleiding daarvan heb ik inderdaad in mei 2021 een attributieprocedure bij de minister van Buitenlandse Zaken opgestart, waarna de aanval nader werd onderzocht door het Coördinatiecomité voor Inlichting en Veiligheid en Buitenlandse Zaken communiceerde over de inmenging van een buitenlandse actor uit China. U bevraagt wellicht het beste Buitenlandse Zaken over de specifieke acties die werden ondernomen na de aanmelding van de attributie bij Buitenlandse Zaken. Voor uw vragen met betrekking tot de cyberaanval in Antwerpen moet ik u ook doorverwijzen naar het CCB, dat het dossier opvolgt.

Voorts vroeg u samen met collega Demon welke initiatieven we hebben genomen in het dossier betreffende Nord Stream. In de eerste plaats heb ik gevraagd naar een evaluatie door het OCAD van wat er precies gebeurd was en de interstatelijke dreiging voor de gasinfrastructuur. Er moest gelukkig niet worden besloten tot een verhoging van het dreigingsniveau voor de gasinfrastructuur. De risico's ter zake worden continu opgevolgd en niet enkel naar aanleiding van dat incident.

Voorts hebben we vergaderingen belegd met alle betrokken partnerdiensten en een alert verstuurd naar de exploitanten van kritieke infrastructuren die zouden kunnen worden geraakt, opdat zij hun essentiële diensten zouden kunnen blijven leveren. Ik heb u dat daarstraks al in detail toegelicht.

Daarnaast werden er noodzakelijke permanente beveiligingsmaatregelen in plaats gesteld naar aanleiding van het incident. Het gaat dan om een actualisatie van de beveiligingsplannen en een inspectie door de sectorale overheden en het OCAD, dat een dreigingsanalyse heeft uitgevoerd op de kritieke infrastructuren.

Als er zich incidenten in andere sectoren voordoen, vragen wij om die zo snel mogelijk te melden aan de betrokken overheden en aan het Crisiscentrum.

J'en viens aux questions de M. Pivin dont certaines m'avaient déjà été adressées par écrit avant cette réunion.

Pour ce qui est du *screening* des travailleurs portuaires, je ne peux bien évidemment pas m'exprimer sur les sujets qui relèvent entre autres de la compétence de mon collègue, le ministre de la Justice. Lorsqu'une question est liée aux responsabilités d'un de mes collègues, je dois faire référence au ministre concerné. Le processus d'approbation pour permettre le *screening* des travailleurs portuaires est dans sa phase de finalisation.

Quant à savoir si une infrastructure a été désignée comme infrastructure critique ou non, il m'est impossible de communiquer, dans l'intérêt de la sécurité. Il est donc préférable d'adresser ces questions à l'autorité sectorielle concernée.

Pour ce qui a trait à la distribution de l'eau, je vous renvoie également à l'autorité sectorielle établie en application de l'arrêté royal du 31 juillet 2020 portant création et organisation du Comité national de sécurité pour la fourniture et la distribution d'eau potable. Ce Comité est composé d'entités fédérées et régionales, à savoir deux représentants et deux suppléants nommés par le ministre fédéral en charge de la Sécurité alimentaire, deux représentants et deux suppléants nommés par la Région flamande, deux représentants et deux suppléants nommés par la Région wallonne et, enfin, deux représentants et deux suppléants nommés par la Région de Bruxelles-Capitale.

Quant à votre question sur la police de la navigation (SPN), l'effectif actuel de la police de la navigation s'élève à environ 350 personnes au total. Son activité s'étend à différents domaines (police des voies navigables, contrôle des frontières et police portuaire). Environ 130 membres de la SPN travaillent à la côte belge. À Anvers, ce chiffre s'élève à 93 personnes auxquelles s'ajoutent une vingtaine de détachés de longue durée. À Gand, il faut compter environ une cinquantaine de personnes actives dans le port. Á l'heure actuelle, il n'y a pas de portique de sécurité sous la responsabilité de la SPN.

Concernant la collaboration avec les services des douanes, il m'est impossible de communiquer des chiffres dans un aussi bref délai mais je peux préciser qu'un accord de coopération entre les douanes et la SPN a été signé en juin 2022.

Quant à la protection des réseaux informatiques qui sont gérés par les opérateurs essentiels et les exploitants de l'infrastructure critique, celle-ci est également coordonnée par le Centre pour la Cybersécurité Belgique (CCB).

Je dois ici à nouveau me référer au premier ministre qui a la tutelle sur le CCB.

Concernant les questions relatives aux acteurs du secteur de la santé publique, je vous renvoie à mon collègue, le ministre de la Santé pour obtenir de plus amples informations quant au cadre légal réglementant ces matières.

Pour ce qui concerne les mesures de protection mises en œuvre spécifiquement pour les réseaux des prisons et des établissements de justice, je vous renvoie à mon collègue, le ministre de la Justice.

Je rappelle que la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques vise uniquement les transports, l'énergie, les finances, la santé publique, les communications électroniques, les infrastructures numériques, l'eau potable et le secteur de l'espace. Les autorités et les services publics n'y figurent pas. Ils ne sont donc pas concernés par cette législation.

Vous avez également posé une question sur la Regional Computer Crime Unit (RCCU) et la Federal Computer Crime Unit (FCCU) qui contribuent à la *quick reaction force*. Cette initiative vise à répondre au rôle joué par la police dans le cadre du plan d'urgence cyber du CCB afin d'apporter une réponse opérationnelle rapide aux crises et incidents de cybersécurité, notamment aux attaques visant des infrastructures critiques ou des secteurs vitaux. À cette fin, un groupe de collaborateurs de différents services CCU ayant les compétences nécessaires pour enquêter sur la cybercriminalité dans les environnements de réseaux complexes a été créé.

Pour ce qui concerne le stockage des armements policiers, comme je l'ai dit à votre collègue, Mme Caroline Taquin, à l'occasion de ma réponse à une précédente question parlementaire sur ce thème, la circulaire ministérielle GPI 62 reprend d'ores et déjà une série de mesures relatives à la sécurisation des locaux d'entreposage des armes. J'ai demandé à ce que soit préparé un arrêté royal relatif à la sécurisation des bâtiments et complexes de bâtiments policiers. Cet arrêté aura pour vocation de renforcer les conseils de sécurité (membres du personnel, matériel, informations sensibles).

Je soumettrai prochainement ce projet d'arrêté royal en vue de sa publication dans le courant de cette année.

Dans l'intervalle, la police fédérale procède déjà à des investissements sur fonds propres ou via la Régie des Bâtiments pour la mise en conformité des locaux le nécessitant. Je confirme que les projets repris dans les différents plans directeurs de la Régie de rénovation ou de construction menés et en cours de développement comprennent systématiquement une mise à niveau de ces locaux.

Monsieur Pivin, la définition des mesures de sécurité incombe à l'exploitant. Il doit l'élaborer dans son plan de sécurité et décrire les mesures qui seront prises. L'autorité sectorielle peut superviser et contrôler ces plans pour les infrastructures critiques désignées par l'autorité sectorielle. Le champ d'application de la législation sur les infrastructures critiques n'implique pas actuellement le secteur public.

Les mesures de cybersécurité imposées par la loi NIS prévoient une protection approfondie du réseau et des systèmes d'information des fournisseurs de services essentiels. Pour plus d'informations, je vous enjoins de poser la question au CCB.

Quant aux éléments désignant les infrastructures critiques, je ne peux les divulguer. En règle générale, la loi exige que les incidents de nature à menacer le fonctionnement d'une infrastructure soient d'office signalés par l'exploitant d'une infrastructure critique aux services de police, à l'autorité sectorielle et au Centre de crise national. De la même manière, les incidents pris en compte par la loi NIS doivent également être signalés aux autorités compétentes.

Comme mentionné, l'évaluation nationale des risques de la Belgique est une analyse des risques au niveau national et ne fournit pas d'information concrète sur la vulnérabilité d'infrastructures spécifiques ou de territoires belges.

Les résultats de la dernière itération 2018-2023 ont été mis à disposition sur le site web www.risk-info.be et peuvent être utilisés par les différents niveaux de pouvoir, y compris les pouvoirs locaux, pour aider à réaliser les étapes suivantes du cycle du risque.

La prochaine itération de l'évaluation nationale des risques pour la Belgique est actuellement en cours et sera valable pour la période de 2023 à 2026. Cette évaluation des risques est cyclique et doit être reconduite tous les trois ans.

J'en arrive ainsi à votre dernière question, monsieur Pivin, sur les risques d'inondation. Selon l'article 3 de l'arrêté royal de 2019 relatif à la planification d'urgence, l'identification et l'analyse des risques sur son territoire est une responsabilité de l'autorité compétente. Dans le cas présent, il s'agit du gouverneur de la province de Limbourg et du gouverneur de la province de Liège. En principe, cette analyse n'est pas rattachée au plan national.

Sur cette base, il peut être décidé d'établir un plan d'intervention pour les risques pour lesquels l'autorité compétente l'estime nécessaire. Dans le Limbourg par exemple, c'est le cas pour les inondations au niveau des bassins de la Meuse et du Demer. Le risque de tempête est quant à lui couvert par le plan.

Pour la province de Liège, le plan reprend le risque d'inondation dans son annexe 49, qui sert comme plan d'intervention et comme fiche de référence.

Pour les risques Seveso, les exploitants des établissements concernés doivent établir un rapport de sécurité dont le chapitre consacré à la présentation de l'environnement de l'établissement comprend une analyse des risques liés à l'environnement de l'établissement et qui doit prendre en compte le risque d'inondation.

Les services d'évaluation, dont le Centre de crise, évaluent chacun pour ce qui les concerne ces rapports de sécurité et peuvent les approuver ou non.

De vragen van collega Demon over Nord Stream heb ik beantwoord naar aanleiding van de vragen van collega Creyelman.

Ik kom tot de vraag van collega Demon over de voedingssector en de voedseldistributie. Vandaag wordt de sector van de voedseldistributie niet gedefinieerd als een sector met kritieke infrastructuren. Dat houdt dus ook in dat er geen dreigingsanalyse bestaat voor de sector op grond van artikel 10 van de wet van 2011. Dat zal in de toekomst wel veranderen gelet op de recent gepubliceerde richtlijn betreffende de veerkracht van kritieke entiteiten, waarmee een uitbreiding wordt beoogd van de kritieke sectoren op Europees vlak en die sector wordt meegenomen als kritieke sector.

In 2022 ondersteunde het Crisiscentrum de FOD Economie bij de uitwerking van een voorstel van voedselcrisisplan. Ook andere partners, zoals de FOD Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu en de gewesten, hebben meegewerkt aan dat plan. Dat plan heeft tot doel om België zo goed

mogelijk voor te bereiden op crises of incidenten die niet alleen de distributiecentra kunnen beïnvloeden of destabiliseren, maar ook de nationale voedselvoorzieningsketen en zijn sociaal-economische werking kunnen bedreigen.

Voor de opmaak van het plan werden twee studies uitgevoerd. De eerste bestond uit een analyse van de verschillende risico's die de voedselketen zouden kunnen verstoren, alsook een identificatie van de meest kwetsbare personen en groepen en maatregelen die genomen zouden kunnen worden om hen te beschermen. De tweede studie ter voorbereiding van het plan betrof de agrovoedingssector en meer bepaald de kwetsbaarheden en het gerelateerde crisisbeheer in twee buurlanden met vergelijkbare kenmerken als België, namelijk Denemarken en Duitsland.

Die studie heeft gebieden naar voren gebracht waarin België vooropliep, maar ook waar België nog kan inhalen. De eerste versie van het plan ligt momenteel bij de FOD Economie. Daarin zijn de belangrijkste richtlijnen en maatregelen opgenomen die de bevoegde autoriteit in staat zouden moeten stellen om elke situatie met nadelige gevolgen, elke gebeurtenis en elk incident zo goed mogelijk te beheersen en vooral ook te herstellen om de voedingsketen en de bevoorrading te verzekeren en daarnaast de bevolking te informeren. Alle actoren die inherent zijn aan het beheer van die noodsituaties, moeten de afgesproken maatregelen operationaliseren zodra het voedselcrisisplan definitief is.

In het kader van de zeven *baseline requirements* van de NAVO, waaronder ook de weerbaarheid van de voedselketen valt, voert het Crisiscentrum met de partners ook een *gap analysis* uit die het mogelijk moet maken om kritieke lacunes te identificeren in het belang van die voedselketen. Die *gap analysis* moet tegen februari 2023 klaar zijn en aansluitend zal op sectoraal niveau worden bekeken welke maatregelen genomen moeten worden en welke implementatieplannen voor die maatregelen gemaakt moeten worden.

Vandaag heeft het OCAD, op basis van de informatie die ik heb, geen weet van dreigingen tegen distributiecentra, ook niet in het kader van de oorlog in Oekraïne. In het geval van een dreiging zal het OCAD uiteraard niet nalaten om een dreigingsanalyse op te stellen om het Crisiscentrum toe te laten de nodige beschermingsmaatregelen te nemen.

U hebt ook een vraag gesteld over het OCAD en de analyse van de kritieke infrastructuur. Momenteel is er een kleine achterstand in die dossiers. Aangezien wij hebben beslist om het OCAD structureel te versterken, zal de achterstand worden weggewerkt. Intussen zijn de selecties van de nieuwe medewerkers, die ook een achterstand hadden opgelopen, ook afgerond. Het OCAD stelt alles in het werk om de dossiers zo snel mogelijk af te werken.

In het geval van een concrete dreiging ten opzichte van een kritieke infrastructuur kan het OCAD altijd een punctuele dreigingsanalyse opstellen, uiteraard met het bijbehorende dreigingsniveau, wat vervolgens het Crisiscentrum moet toelaten om de gepaste veiligheidsmaatregelen uit te vaardigen.

Het OCAD werd inderdaad verzocht om een analyse van de interstatelijke dreiging in het kader van de oorlog op te maken, die verder gaat dan enkel de kritieke infrastructuren. Andere mogelijke targets buiten de kritieke infrastructuren worden daarin meegenomen, zoals gevoelige sectoren, nationale en internationale sleutelfiguren en instellingen. Momenteel wordt bekeken of het noodzakelijk is om het OCAD expliciet een bijkomende opdracht te geven inzake de interstatelijke dreiging. Daarover worden vandaag gesprekken gevoerd met binnenlandse en buitenlandse partnerdiensten.

Het OCAD zal desgevallend een voorstel daarvoor doen aan het CCIV, vervolgens aan het SCIV en ten slotte aan de Nationale Veiligheidsraad, die daarover zal beslissen.

Mijnheer Vandenput, er zijn twee mechanismen voor de interdepartementale samenwerking op de Noordzee. Ten eerste is er het Maritiem Informatiekruispunt, dat is samengesteld uit Fedpol, DG Scheepvaart, de douane en de marine, die de zee permanent monitoren en zo onze ogen en oren op zee zijn. De patrouilles van de scheepvaartpolitie en de marine zullen worden uitgestuurd indien dat nodig is. Het tweede mechanisme is de risicobeoordeling in het kader van het vernieuwde Scheepvaartwetboek, dat begin dit jaar in werking is getreden onder leiding van de minister van Noordzee. Het Maritiem Informatiekruispunt zal samen met de actoren en de exploitanten een veiligheidsbeoordeling van mogelijke dreigingen en zwakke plekken opmaken en verbeterpunten oplijsten. De Nationale Autoriteit voor Maritieme Beveiliging (NAMB) moet het plan vervolgens goedkeuren. Men voorziet om de vijf jaar in een actualisatie van dat plan, evenals een evaluatie. Voor de havens werden de ISPS-niveaus aangepast door de NAMB. De

havens zijn verplicht om de daaraan verbonden bijkomende veiligheidsmaatregelen uit te voeren.

De stresstest is vervat in het beveiligingsplan van de exploitant van de kritieke infrastructuren. Per sector en subsector wordt de inspectiedienst belast met het controleren van die plannen en wat de exploitant met die maatregelen heeft gedaan, zodat men kan vaststellen of er aan die maatregelen wordt voldaan. Dat zou men kunnen omschrijven als stresstest.

Mijnheer Verduyckt, ik ben al ingegaan op de identificatie en de beveiliging van de kritieke infrastructuur. Laat het duidelijk zijn, alle sectoren zijn even belangrijk en worden gelijkwaardig geacht, getuige alle activiteiten van het crisiscentrum.

Wat de uiteindelijke beveiliging betreft, kunnen we spreken van een gedeelde verantwoordelijkheid voor de infrastructuur. De exploitant is verantwoordelijk voor het melden van incidenten aan het Crisiscentrum, de politie en de sectorale overheden voor de opvolging ervan. De sectorale autoriteit is dan weer verantwoordelijk voor de inspectie. Het OCAD is ook betrokken, want het maakt de punctuele en strategische dreigingsanalyses op, terwijl het Crisiscentrum natuurlijk een overkoepelende en coördinerende rol heeft, los van de afkondiging van de federale fase of incidenten met kritieke infrastructuur, door zijn ondersteuning bij de opmaak van een nationaal voedselveiligheidsplan.

Wat het energie-eiland betreft, als dat effectief wordt gerealiseerd moeten we nagaan of we dat als kritieke infrastructuur aanduiden. Dat zal gebeuren op basis van een analyse van de sectorale overheid. Indien dat het geval is, zullen de reguliere mechanismen in werking treden en zullen de analyses, beveiligingsplannen, controles en meldingen van incidenten moeten plaatsvinden. Indien het eiland niet als kritieke infrastructuur wordt aangeduid, gebeurt de beveiliging structureel via de NAMB. Het is dus niet zo dat het eiland dan niet wordt beveiligd of de situatie niet wordt gecontroleerd.

De vragen van de heer Francken waren vooral voor mijn collega. De vraag van mevrouw Ingels over de nationale weerbaarheidsstrategie en de multiriskanalyse heb ik in het begin proberen te beantwoorden.

01.14 **Ludivine Dedonder**, ministre: Monsieur le président, chers collègues, si j'ai rappelé, en guise d'introduction, que la Défense n'avait pas de responsabilités explicites en matière de protection des infrastructures critiques en général, elle dispose, conformément au plan STAR approuvé par le gouvernement, d'un certain nombre de capacités qui, lorsque ses ressources le permettent, peuvent venir en appui ou contribuer aux missions des services civils concernés, quand ils en font la demande.

Zoals gezegd is het dankzij deze duale capaciteit, gewaarborgd door de militaire programmawet 2023-2030, dat Defensie op het nationale grondgebied dus niet alleen structurele veiligheidstaken kan uitvoeren, maar specifieker ook ondersteuning van civiele diensten kan garanderen door missies om kritieke infrastructuur te beschermen.

De taken van de Dienst voor Opruiming en Vernietiging van Ontploffingstuigen (DOVO) maken deel uit van die structurele veiligheidstaken op het nationale grondgebied. Het gaat dan onder meer om het neutraliseren, ontmantelen en evacueren van achtergebleven, niet-ontplofte munitie en explosieven. Het kan ook gaan om interventies in een context gericht op onze kritieke infrastructuur.

De son côté, la capacité CBRN spécialisée de la Défense est une capacité niche qui contribue à la lutte contre la prolifération des armes de destruction massive mais aussi au Plan d'urgence national en cas d'incident majeur sur notre territoire. Elle participe à la prévention, à la protection et à la récupération face aux dangers provenant d'armes ou engins contenant des substances toxiques. Elle est également engagée dans la lutte contre le terrorisme et joue un grand rôle dans la résilience sur le terrain national.

Au travers de protocoles d'accords interdépartementaux, 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'autorité fédérale de contrôle du nucléaire, l'AFCN.

La Défense met, par ailleurs, à contribution des hélicoptères A109 équipés de spectromètres gamma de l'AFCN, afin d'effectuer des contrôles radiologiques de zones sensibles.

De plus, un accord de coopération existe entre la composante terre et les pompiers du service incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale, à des fins d'échange d'expertise en CBRN.

Enfin, le développement de notre capacité CBRN scientifique s'établit en coordination avec la police scientifique fédérale.

De defensielaboratoria spelen een sleutelrol bij de eenduidige identificatie van CBRN-agentia, meer bepaald onder het mandaat van de Organisatie voor het Verbod op Chemische Wapens (OPCW). Daarnaast is het Federaal Oriëntatielaboratorium (FOL) het landelijke meldpunt voor de behandeling van pakjes met een vermoedelijk CBRN-risico. De gespecialiseerde CBRN-capaciteit van Defensie speelt de facto een belangrijke rol op het nationale grondgebied en biedt een waaier aan capaciteiten, ervaring en voorbereiding op CBRN-kwesties, die zijn gelijke niet kent bij onze civiele partners.

En matière de cybersécurité, j'ai évoqué en introduction les cyberattaques importantes qui ont récemment visé notre pays et certaines de nos infrastructures. Ces cyberattaques, que nous avons pu contrer, sont la preuve que notre choix d'investir dans la cybersécurité était effectivement le bon et que des investissements supplémentaires en la matière étaient bien sûr nécessaires. Il s'agit d'une de mes priorités depuis mon entrée en fonction, et cette priorité façonnera d'ailleurs le reste de la législature.

In 2022 werd de focus gelegd op het versterken van de operationale cybercapaciteiten bij de ADIV en de opstart van wat op termijn de cybercomponent van Defensie moet worden, namelijk de cybercommand.

De grootste bedreiging van vandaag is *cybernetics*. Meer dan ooit moeten wij ons daartegen wapenen. Het is duidelijk dat cybercapaciteit de capaciteit van de toekomst is voor onze industriële basis.

Comme je l'ai indiqué dans le cadre de ma note de politique générale de 2023, le développement des capacités cybernétiques de la Défense se prolongera cette année. Il en va du bon fonctionnement de notre organisation mais aussi, par extension, du bon fonctionnement de notre État et de la société dans son ensemble.

L'ambition est de pratiquement doubler le personnel actuellement en place dans ce domaine. Pour des raisons évidentes de sécurité, nous ne communiquons pas publiquement les moyens dédiés à cette capacité spécifique. Nous travaillons avec de nombreux partenaires publics et privés, avec l'objectif d'arriver à un équilibre de deux tiers de civils et un tiers de militaires pour cette composante.

Je suis bien évidemment consciente du défi en matière de ressources humaines dans ce domaine, comme pour le reste de la Défense. C'est un point d'attention majeur. Nous travaillons également avec nos entreprises dans ce cadre. Nous avons également la possibilité d'engager sous la réserve militaire, c'est-à-dire d'avoir des personnes qui travaillent à temps partiel dans des entreprises de cybersécurité et à la Défense. Nous avons aussi la possibilité de former en continu et surtout d'offrir l'accès à des informations classifiées, à des informations relatives aux opérations et aux déploiements à l'étranger, ce qui attire aussi de nombreuses personnes.

En collaboration étroite avec d'autres acteurs clé de la lutte contre la cybercriminalité et la criminalité nationale tels que le Centre de crise national, le Centre pour la cybersécurité Belgique, la police fédérale, le SFP Affaires étrangères, le nouveau Cybercommand de la Défense participe lui aussi à la protection des infrastructures critiques, comme le prévoient la stratégie nationale de sécurité ainsi que tâches qui lui sont assignées dans la stratégie cybersécurité Belgique 2.0 ou encore son rôle dans le plan national d'urgence cybernétique.

Parallèlement à la poursuite du renforcement des capacités du Cybercommand et conformément aux mesures nationales à prendre dans le cadre de la directive européenne sur la résilience des entités critique, nous analyserons comment ces mesures peuvent apporter une contribution supplémentaire à la cybersécurité des infrastructures critiques belges.

Il y avait également une question concernant les capacités offensives. Il y a eu récemment une adaptation législative pour permettre à la Défense de réagir en cas d'attaque, donc de contre-attaquer. C'est le cas si la Défense est attaquée mais aussi si un autre département ou une infrastructure critique d'intérêt national sont attaqués. Nous avons désormais cette possibilité.

Naast de eigen kritieke infrastructuur herbergt België ook de belangrijkste instellingen van de Europese Unie en de NAVO, evenals vele andere internationale organisaties die bescherming verdienen. Om onze positie

als gastland te bestendigen en de veilige werking van deze infrastructuur en instellingen te vrijwaren, heeft België meer in het algemeen zijn capaciteiten op het gebied van antiterrorisme, spionage, subversie en georganiseerde misdaad versterkt, met name via het STAR-plan. In dit kader verzamelt de ADIV de nodige gegevens, die hij doorgeeft aan het OCAD, dat vervolgens dreigingsevaluaties maakt, onder meer met betrekking tot de beveiliging van kritieke infrastructuur.

Avec la Belgian Pipeline Organisation (BPO), la Défense assure également l'exploitation et le maintien en l'état de la partie belgo-luxembourgeoise du système de pipelines d'Europe centrale. Ce système logistique constitue l'épine dorsale de l'approvisionnement en vrac de carburants avion des bases aériennes en France, en Belgique, en Allemagne, aux Pays-Bas et au Luxembourg.

La capacité totale de ce dispositif robuste dépasse les besoins militaires. La capacité excédentaire est alors mise à disposition de clients civils, de manière à continuer à assurer un entraînement optimal du personnel, ainsi qu'une rotation suffisante des produits nécessaires au maintien de sa qualité.

Cet usage civil contribue également au financement du système et, donc, à la réduction des coûts pour les pays membres. D'importants aéroports civils tels que Schiphol, Bruxelles et Francfort sont notamment raccordés au réseau.

Naast het evidente militaire belang mag ook het economische belang van deze eenheid voor België niet worden onderschat. Vliegtuigbrandstof voor Brussels Airport en Luxembourg Airport wordt exclusief geleverd door de BPO. Dat geldt ook voor een zeer groot deel van de bevoorrading van Bierset.

Door haar centrale ligging in het netwerk fungeert de BPO als spil in dit netwerk door de toegangspunten van de Amsterdam-Rotterdam-Antwerpenzone te verbinden met de verschillende klanten in binnen- en buitenland. Van het binnen de BPO getransporteerde volume vervolgt de helft zijn weg naar zusterorganisaties in de buurlanden. De combinatie van militaire en civiele behoeften vereist een zeer intensief gebruik van het systeem, dat permanent operationeel is.

La résilience de toute cette infrastructure face aux menaces dans toutes leurs dimensions est concrètement définie par l'OTAN. Sa protection s'effectue selon différents niveaux de responsabilité en lien notamment avec des services de sécurité externes. En cas d'incident majeur, une chaîne de notifications est prévue à l'attention de la Défense.

À côté des moyens nationaux propres à la Défense et au SGRS, nous nous appuyons sur les moyens de nos partenaires et Alliés, que ce soit au niveau européen ou au niveau de l'OTAN, pour l'échange d'informations de différentes sources, notamment satellitaires.

Cette approche s'inscrit dans notre stratégie de résilience pour la protection des infrastructures critiques développée depuis l'année passée avec la *critical equipment resilience*. La surveillance satellite fait donc partie de la stratégie belge avec des investissements prévus dans ses capacités avec le Plan STAR.

La Défense joue également un rôle dans la *Quick Reaction Alert* pour la mission de police aérienne dans le cadre de l'OTAN, y compris sur le territoire national et pour nos infrastructures critiques ou pour le déploiement national dans le cadre de la lutte contre le terrorisme.

Des experts de la Défense interviennent en outre au sein du *National Airspace Security Center.* Dans ce carrefour interfédéral de l'information pour les questions aéronautiques, physiquement implanté au sein du *Control and Reporting Center* de Beauvechain, s'opère une étroite coopération entre le personnel mis à disposition entre autres de la Défense, de la Direction générale Transport aérien du SPF Mobilité, de la police fédérale et des douanes afin d'assurer une réponse conjointe en cas d'incident aussi rapidement et efficacement que possible.

Le NASC est un Centre interfédéral de connaissances de la situation qui collecte, analyse et traite les informations sur les incidents aéronautiques ou les éléments liés à l'aviation et les retransmet à toutes les autorités et services concernés pour une exploitation ultérieure.

Dans ce cadre, selon leur niveau de compétence, c'est le SPF Économie et l'Institut belge des services postaux et des télécommunications qui sont chargés de déterminer précisément et dans son ensemble à quoi se rapporte cette infrastructure.

Nonobstant cette liste des infrastructures critiques identifiées par le Centre de crise national, il est à noter que les opérateurs et la marine accordent évidemment toute l'attention et la sécurité nécessaires à l'ensemble des infrastructures présentes en mer.

Cela est d'autant plus important dans le contexte de la guerre en Ukraine avec, notamment, une série de risques de sabotage d'infrastructures énergétiques, de pipelines ou encore de réseaux de communication, dont des câbles sous-marins.

Pour prendre l'exemple de ces câbles sous-marins, il est clair qu'ils constituent des enjeux géostratégiques pouvant potentiellement bouleverser la conjoncture mondiale tant en matière de télécommunications et d'approvisionnement énergétique qu'en matière économique. Concrètement, nous nous devons de nous prévaloir contre tout risque d'interruption ou d'interception de ceux-ci par un ennemi.

Les menaces sont multiples à cet égard. Elles peuvent provenir tant d'organisations terroristes et criminelles que d'instances dirigées par des États hostiles. Les risques dépendent forcément toujours du niveau technologique de l'auteur du sabotage et de l'accessibilité de l'infrastructure visée.

Op nationaal niveau is de exploitant verantwoordelijk voor de bewakings- en de beschermingsmaatregelen voor de infrastructuur. De federale politie voert die 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.

Defensie overlegt regelmatig met de offshore-industrie, bijvoorbeeld via de werkgroep Windmolenparken, en onderhoudt contacten met partners als Elia, Otary en Parkwind over de veiligheid en de organisatie van gezamenlijke oefeningen in en rond windmolenparken, maar ook over het delen van middelen, zoals de bewakingscamera's rond die windmolenparken.

La marine joue un rôle de soutien important dans la sécurité générale des eaux belges. Cela ne comprend d'ailleurs pas que la surveillance et la sécurisation des infrastructures critiques en mer, mais aussi le contrôle de la pêche, la lutte contre les trafics de drogue, d'êtres humains, d'armes, la préservation de l'environnement et l'appui lors de catastrophes et incidents tels que la pollution par les hydrocarbures.

À cet effet, du personnel de la douane, de la police maritime et du SPF Mobilité a été intégré au sein de la capacité de commandement de la marine pour les opérations dans les eaux nationales. Ensemble, ils forment le Carrefour d'Information Maritime (CIM). Les quatre autorités ont chacune leurs propres missions et disposent de bases de données avec des informations sur toute la région côtière belge.

In het Maritiem Informatiekruispunt bundelen ze hun krachten om 24/7 informatie te verzamelen, te analyseren en te delen. Om de bewaking en de beveiliging van de Belgische wateren en de daar aanwezige maritieme aanvoerlijnen en offshore-infrastructuur te optimaliseren, lopen er momenteel besprekingen over een samenwerking, bijvoorbeeld in het kader van het toekomstige energie-eiland, onder meer met Elia. Gezien de centrale ligging is die infrastructuur uitermate geschikt voor de installatie van sensoren, communicatiesystemen en aanlegplaatsen voor drones, om zo de mogelijkheden voor de inzet van mariene capaciteiten en beeldcompilatie in het MIK te verbeteren.

La coopération interdépartementale dans le MIK peut également intéresser les services de sécurité, le Centre de crise national et le NASC en cas d'opération d'urgence et de secours.

Aux niveaux européen et transatlantique, des réunions périodiques sont organisées entre tous les partenaires qui suivent de près les transits des navires d'intérêt susceptibles de constituer une menace. Les navires issus de pays non-membres de l'OTAN sont surveillés par le Commandement maritime allié de l'organisation.

Tant qu'aucune infraction flagrante n'est détectée, un État ne peut pas procéder à l'arraisonnement d'un navire. Mais en cas de doute, l'exploitant et/ou la marine peuvent être amenés à effectuer une étude *a posteriori* des fonds marins et des infrastructures critiques qui y seraient éventuellement présentes.

Wat de internationale wateren betreft, herinner ik u er bovendien aan dat België in 2015 het Verdrag tot bestrijding van wederrechtelijke gedragingen gericht tegen de veiligheid van de zeevaart en het protocol bij

dit verdrag heeft geratificeerd. Dit verdrag bepaalt onder meer dat alle ondertekenende landen maatregelen kunnen nemen tegen vaartuigen die misdrijven plegen, zoals het saboteren van onderwaterinfrastructuur in internationale wateren.

Il est à noter que les vulnérabilités des infrastructures critiques sont, par définition, bien plus grandes en haute mer, où la liberté de navigation prévaut, et où la surveillance est rendue plus compliquée de par les fonds marins, et la nécessité de moyens technologiques renforcés et avancés pour étendre la zone de surveillance. En dehors d'une zone économique exclusive, il est par conséquent très difficile de pouvoir attribuer une attaque ou un sabotage à un acteur hostile.

L'initiative prise par l'Italie est connue. Au demeurant, le Centre d'excellence de l'OTAN – avec lequel la Défense belge collabore – s'y trouve.

Par ailleurs, vous savez qu'au travers du plan STAR, nous disposons désormais d'une stratégie de développement technologique, qui est le fil conducteur de ma politique consistant à renforcer les partenariats avec les centres de recherche et les acteurs privés au travers de l'adoption de la DIRS (Defence, Industry and Research Strategy). Nous avons désormais non seulement la stratégie, mais aussi les moyens, lesquels s'élèvent désormais à 1,8 milliard d'euros, en vue d'investir dans la recherche et le développement auprès de nos entreprises. Notre souhait est, bien entendu, de travailler avec elles de manière générale.

Verschillende initiatieven voor de ontwikkeling van nieuwe technologie lopen momenteel via DIANA en het European Defence Agency.

Je terminerai en revenant sur d'autres aspects qui peuvent être mis en oeuvre par la Défense dans le cadre de l'aide à la nation et à la société en général. Sur la base de l'ensemble du matériel disponible au niveau des bataillons de génie et de logistique, qui se complètent l'un l'autre, les fonctionnalités sécurisation et manutention non qualifiée peuvent être fournies en appui d'autres services via la Compagnie de protection territoriale, lancée le 1er janvier 2022. Cette compagnie est 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.

De ontwikkeling van de nationale logistieke hub, waarin het STAR-plan voorziet, past in dit kader. Die hub zal duidelijk bijdragen aan het verbeteren van de militaire mobiliteit, ook op nationaal niveau, en daarmee aan de veerkracht van het land. Dit knooppunt zal fungeren als expertisecentrum inzake voorbereiding en projectie van uitrusting.

01.15 **Steven Creyelman** (VB): Ik wil beide ministers danken voor hun zeer exhaustief antwoord. In de commissie voor Volksgezondheid, waar ik ook deel van uitmaak, loopt het beantwoorden van vragen soms nog net iets anders. Mijn dank voor alle antwoorden. Mevrouw Verlinden heeft bijvoorbeeld voor de vragen die zij niet kon beantwoorden, gezegd waarom dat niet kon en was zo vriendelijk om door te verwijzen naar de bevoegde minister. U bent vandaag beiden een voorbeeld voor bepaalde andere ministers; ik zal me zacht uitdrukken en geen namen noemen.

Ik wil mij ook verontschuldigen bij mevrouw Dedonder omdat ik een stuk van het antwoord niet kon beluisteren, maar ik zal dat zeker online nog doen. Ik vermoed dat u ook hebt geantwoord op alle vragen die ik heb gesteld. Dank u wel.

01.16 **Philippe Pivin** (MR): Monsieur le président, je me joins aux remerciements qui viennent d'être exprimés. J'ai reçu un certain nombre de réponses à la multitude de questions que j'avais déposées. Pour le reste, madame Verlinden, j'ai beaucoup entendu que vous renvoyiez aux compétences du premier ministre, de vos collègues de la Justice et des Douanes, qui m'ont déjà répondu quant à certains éléments. Vous avez aussi renvoyé aux autorités sectorielles.

Je ne pense pas avoir été présent au moment où il a été décidé de fixer l'ordre du jour de cette séance de commission, et que l'initiative provient d'un collègue de la N-VA. Je regrette que l'on ait limité le champ de discussion pour ces matières aux commissions de l'Intérieur et de la Défense, à partir du moment où d'autres collègues du gouvernement sont manifestement concernés par la problématique, qui reprend toutes les infrastructures critiques – l'informatique, la santé, les prisons, etc.

D'autre part, madame la ministre, le renvoi aux opérateurs privés, que je comprends fort bien, et à la responsabilité de ceux-ci, n'exonère évidemment pas le gouvernement de sa propre responsabilité. Si les opérateurs privés ont la charge d'élaborer des plans, le gouvernement a la charge et la responsabilité de s'assurer que les plans sont bien élaborés et répondent aux défis et aux menaces.

Les choses sont-elles bien mises en place pour s'assurer que les plans que l'on charge des opérateurs privés d'élaborer sont effectivement mis en œuvre et correspondent aux attentes? Des analyses sont-elles effectuées pour le vérifier? Des conclusions ont-elles été tirées à la suite de ces analyses?

Peter Buysrogge, voorzitter: Mijnheer Pivin, aangezien u even over de regeling van de werkzaamheden hebt gesproken, wil ik nog het volgende meegeven.

Wij organiseren hier een eerste debat over de kritieke infrastructuur. Het klopt dat niet alle vragen worden beantwoord, omdat niet alle bevoegde ministers aanwezig zijn. Het staat u evenwel vrij om bijkomende initiatieven te nemen en de bevoegde ministers nader te ondervragen over de kwestie of om andere initiatieven te nemen in functie van het voeren van een nog volledig debat. Het werk is hier vandaag zeker niet afgerond.

Zijn er nog leden die willen spreken?

01.17 **Theo Francken** (N-VA): Mijnheer de voorzitter, ik verontschuldig mij voor het ijsberen, maar 22 jaar Wetstraatzitten heeft gevolgen voor mijn onderrug. Ik moet van de dokter voldoende wandelen. Om mijn tienduizend stappen te halen op een dag die helemaal gevuld is met zittende vergaderingen, zit er niets anders op dan tijdens de vergadering te proberen ijsberen aan de achterkant van de zaal. Ik hoop dat het u niet heeft gestoord.

Peter Buysrogge, voorzitter: Mijnheer Francken, zolang het maar letterlijk en niet figuurlijk is, is dat geen probleem.

01.18 **Theo Francken** (N-VA): Mijnheer de voorzitter, mevrouw de minister van Binnenlandse Zaken en mevrouw de minister van Defensie, alle gekheid op een stokje, jullie antwoord was duidelijk. Er komt een resolutie aan waarmee wij het verdere debat in het Parlement zullen voeren.

Mevrouw de minister Dedonder, het klopt dat er heel wat initiatieven lopen en dat ook met de Europese fondsen een aantal goede zaken lopen. België doet daaraan mee. Wij zullen dat zeker opvolgen.

Die deelname is ook nodig om geruststellende signalen te geven aan de publieke opinie, om aan te duiden dat wij echt met de zaak bezig zijn en *on top of things* zijn. Ik moet immers toegeven dat het opblazen van Nord Stream 1 tot ernstige consternatie heeft geleid, ook bij mij. Ik volg toch al jaren de defensiepolitiek in Europa en ook ik was verbaasd dat het zo ver kon gaan qua sabotage en aanslagen op grote gas- en andere infrastructuur.

Wij moeten daarover evenwel niet naïef zijn. Dat zijn echt wel doelwitten. Er lopen echter heel wat initiatieven. België is ermee bezig. U bent er zich van bewust. Defensie is er ook mee bezig. Wij zullen het dus zeker opvolgen.

Mijnheer de voorzitter, wij zullen een resolutie indienen op basis waarvan wij in de commissie voor Landsverdediging over een en ander zeker nog van gedachten zullen kunnen wisselen.

Het incident is gesloten.
L'incident est clos.

De openbare commissievergadering wordt gesloten om 16.12 uur.
La réunion publique de commission est levée à 16 h 12.