DOC 56 **1158/007**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

5 november 2026

RESOLUTIE

ter bescherming van onze welvaartsstaat tegen hybride acties

Tekst aangenomen
door de plenaire vergadering

Zie:

Doc 56 **1158/ (2025/2026)**:
001: Voorstel van resolutie van de heer Weydts en mevrouw Lambrecht.
002 en 003: Amendementen.
004: Verslag.
005: Tekst aangenomen door de commissie.
006: Amendement.

Zie ook:
Integraal verslag:
5 november 2026.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

5 novembre 2026

RÉSOLUTION

visant à protéger notre État-providence contre les actions hybrides

Texte adopté
par la séance plénière

Voir:

Doc 56 **1158/ (2025/2026)**:
001: Proposition de résolution de M. Weydts et Mme Lambrecht.
002 et 003: Amendements.
004: Rapport.
005: Texte adopté par la commission.
006: Amendement.

Voir aussi:
Compte rendu intégral:
5 novembre 2026.

04806

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

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. overwegende dat de technologie en de mate van asymmetrie binnen conflicten fundamenteel is veranderd en zich steeds vaker manifesteert in een schemergebied tussen oorlog en vrede, waar statelijke en niet-statelijke actoren gecoördineerd gebruikmaken van militaire, politieke, economische, informationele, juridische en cybernetische middelen om strategische doelen te bereiken door het onder druk te zetten van ons samenlevingsmodel;

B. overwegende dat hybride acties een combinatie vormen van militaire acties, cyberaanvallen, economische druk, desinformatie, politieke beïnvloeding, sabotage en andere asymmetrische middelen;

C. overwegende dat hybride conflicten de drempels van openlijke gewapende conflicten niet overschrijden maar de traditionele grenzen vervagen en een toestand van permanente, laag-intensieve confrontatie creëren;

D. overwegende dat hybride actie en met name desinformatie gericht is op het ondermijnen van de democratische besluitvormingsprocessen, het zaaien van maatschappelijke tweedracht en het verzwakken van het vertrouwen in de overheid, de media, de wetenschap en de rechtsstaat, waarbij informatiemanipulatie en inmenging (FIMI1) wordt aangewend als een primair instrument om het gedrag van de bevolking te beïnvloeden, de samenleving te polariseren, paniek te zaaien en interne conflicten te voeden;

E. overwegende dat het voorkomen en het weerstaan van hybride dreigingen interventies op verschillende domeinen vereist;

F. overwegende dat de voorbereiding van de burgers, de economische actoren, het middenveld, de overheidsinstanties en de politici op het omgaan met hybride acties zowel de eerste verdedigingslinie tegen de aanvallen vormt als een essentieel onderdeel van de veerkracht;

G. overwegende dat cyberaanvallen en/of datadiefstal op communicatienetwerken, financiële systemen, energienetwerken en industriële controlesystemen een directe bedreiging vormen voor de nationale veiligheid;

[1] FIMI: *Foreign Information Manipulation and Interference.*

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. considérant que la la technologie et le degré d'asymétrie dans les conflits a fondamentalement changé et que ceux-ci se manifestent de plus en plus souvent dans une zone grise entre guerre et paix, où des acteurs étatiques et non étatiques utilisent de manière coordonnée des moyens militaires, politiques, économiques, informationnels, juridiques et cybernétiques pour atteindre des objectifs stratégiques en mettant notre modèle de société sous pression;

B. considérant que les actions hybrides combinent actions militaires, cyberattaques, pressions économiques, désinformation, influence politique, sabotage et d'autres moyens asymétriques;

C. considérant que les conflits hybrides ne dépassent pas les seuils des conflits armés ouverts, mais estompent les frontières traditionnelles et créent une situation de confrontation permanente et de faible intensité;

D. considérant que les actions hybrides, et en particulier la désinformation, visent à saper les processus décisionnels démocratiques, à semer la division dans la société et à affaiblir la confiance dans les pouvoirs publics, les médias, la science et l'état de droit en utilisant la manipulation de l'information et l'ingérence (FIMI1) comme instrument fondamental pour influencer le comportement de la population, polariser la société, semer la panique et alimenter les conflits internes;

E. considérant que la prévention des menaces hybrides et la résistance à celles-ci requièrent des interventions dans différents domaines;

F. considérant que la préparation des citoyens, des acteurs économiques, de la société civile, des administrations et du personnel politique à faire face aux actions hybrides constitue à la fois la première ligne de défense contre les attaques et un élément essentiel de la résilience;

G. considérant que les cyberattaques et/ou le vol de données sur les réseaux de communication, dans les systèmes financiers, sur les réseaux énergétiques et dans les systèmes de contrôle industriels constituent une menace directe pour la sécurité nationale;

[1] FIMI: *Foreign Information Manipulation and Interference.*

H. overwegende dat die afschrikking doeltreffender wordt door de daden aan hun plegers toe te schrijven en door de mogelijkheid te hebben tegenmaatregelen te nemen, waaronder collectieve maatregelen, zoals sancties op het niveau van de NAVO en de Europese Unie, via de tenuitvoerlegging van de relevante solidariteitsclausules van de verdragen;

I. overwegende dat volgens het World Economic Forum de menselijke factor verantwoordelijk is voor ongeveer 90 % tot 95 % van de tekortkomingen op het gebied van cyberveiligheid;

J. overwegende dat de Belgische open economie en internationale afhankelijkheden (energie, technologie, bevoorrading) een risico betekenen op economische druk en verstoring van toevoerketens en daarbij gewaakt moet worden over de strategische sectoren en de buitenlandse investeringen;

K. overwegende dat de bescherming van de fysieke en digitale integriteit, de bescherming tegen sabotage en de beveiliging van de kritieke infrastructuur en de infrastructuur van federaal, regionaal en lokaal belang zoals bijvoorbeeld de kerncentrales, de energiecentrales, de transportnetwerken, de water- en communicatiesystemen, de voedseldistributiecentra alsook de pijpleidingen en de datakabels, een cruciaal onderdeel vormen van de hybride veiligheid;

L. overwegende dat de maritieme infrastructuur – in het bijzonder de Belgische Exclusieve Economische Zone (EEZ) in de Noordzee, de havens, de pijpleidingen en de kabels voor internet en energiebevoorrading – kwetsbaar is voor activiteiten van buitenlandse maritieme eenheden en schaduwvloten, en cruciaal is voor onze veiligheid en welvaart;

M. overwegende dat zich concrete voorbeelden voordoen van hybride acties in de Noord- en Oostzee, de Middellandse Zee en onze Belgische havens en binnenwateren met anonieme olietankers en (vracht) schepen die onder wisselende vlaggen varen; enerzijds om sancties te ontwijken, als deel van een zogenaamde “schaduwvloot”, en anderzijds om rond vitale havens en energie-installaties te opereren voor spionage en sabotage, als deel van een zogenaamde “spookvloot”;

N. gelet op de groeiende offshore-infrastructuur en het aangekondigde investeringspakket van 1000 miljard euro op de derde Noordzeetop in Hamburg van 26 januari 2026, dat het aanvalsoppervlak voor hybride actoren vergroot;

H. considérant que cette dissuasion est rendue plus efficace en imputant les actes à leurs auteurs et en ayant la possibilité d’adopter des contre-mesures, y compris collectives, telles que des sanctions au niveau de l’OTAN et de l’Union européenne, par la mise en œuvre des clauses de solidarité pertinentes des traités;

I. considérant que, selon le Forum Économique Mondial, le facteur humain représente environ 90 % à 95 % des failles de cybersécurité;

J. considérant que l’économie ouverte de la Belgique et ses dépendances internationales (énergie, technologie, approvisionnement) exposent notre pays à un risque de pressions économiques et de perturbation des chaînes d’approvisionnement et qu’il convient, à cet égard, d’être attentif aux secteurs stratégiques et aux investissements étrangers;

K. considérant que la protection de l’intégrité physique et numérique, la protection contre le sabotage et la sécurisation des infrastructures critiques et des infrastructures d’intérêt fédéral, régional et local telles que les centrales nucléaires, les centrales énergétiques, les réseaux de transport, les systèmes d’approvisionnement en eau et de communication, les centres de distribution de produits alimentaires, ainsi que les pipelines et les câbles de données, constituent un élément clé de la sécurité hybride;

L. considérant que les infrastructures maritimes – en particulier la zone économique exclusive (ZEE) belge en mer du Nord, les ports, les pipelines et les câbles internet et d’approvisionnement en énergie – sont vulnérables aux activités d’entités maritimes et flottes fantômes étrangères, et qu’elles sont d’une importance cruciale pour notre sécurité et notre prospérité;

M. considérant qu’il existe des exemples concrets d’actions hybrides en mer du Nord, en mer Baltique et en mer Méditerranée, ainsi que dans les ports et eaux intérieures belges, impliquant des pétroliers et des cargos anonymes qui changent à plusieurs reprises de pavillon; d’une part, afin d’éluder les sanctions dans le cadre des activités d’une “flotte de l’ombre” et, d’autre part, afin de mener, à proximité de ports et d’installations énergétiques vitaux, des activités d’espionnage et de sabotage, dans le cadre des activités d’une “flotte fantôme”;

N. vu le développement des infrastructures offshore et le paquet d’investissement de 1000 milliards d’euros annoncé lors du troisième Sommet de la mer du Nord organisé à Hambourg le 26 janvier 2026, qui élargit la surface d’attaque des acteurs hybrides;

O. overwegende dat onbemande luchtvaartuigen (UAS[2]/drones) in hybride omstandigheden routinematig worden ingezet voor inlichtingenvergaring, gerichte sabotage, het verstoren van bevoorradingsketens en civiele luchtvaartoperaties, alsmede voor informatie- en psychologische operaties; dat dergelijke inzet veelal via proxy-actoren of vanaf commerciële vaartuigen plaatsvindt om de toekenning en de escalatie te bemoeilijken; en dat deze middelen daardoor een directe bedreiging vormen voor de kritieke infrastructuur, de continuïteit van vitale diensten en het publiek vertrouwen;

P. overwegende dat burgers, lokale besturen en civiele diensten de eerste lijn vormen bij elke crisis waardoor de maatschappelijke weerbaarheid, de transparante communicatie, de burgerparticipatie en de mediawijsheid essentieel zijn om destabiliserende buitenlandse invloeden tegen te gaan;

Q. overwegende dat vrije en eerlijke verkiezingen een doelwit zijn waarbij buitenlandse actoren heimelijk politieke partijen financieren, campagnes voeren van misleiding en het vertrouwen in de verkiezingsresultaten aantasten;

R. overwegende dat de gehele bevolking het slachtoffer kan worden van desinformatiecampagnes, dat bepaalde groepen, zoals jongeren, bijzonder kwetsbaar zijn, alsook dat sociale media heel belangrijke kanalen zijn voor desinformatiecampagnes;

S. gelet op de *Digital Services Act*, die onder meer verplichtingen oplegt aan de grote platforms op het gebied van de bestrijding van desinformatie;

T. overwegende dat bepaalde derde landen, teneinde de democratische processen op ongepaste wijze te beïnvloeden, hooggeplaatste personen trachten te rekruteren – soms met succes – of trachten gebruik te maken van diaspora's, universiteiten of zogenaamd culturele evenementen;

U. overwegende dat de vestiging van de hoofdzetel van de Europese Unie, evenals de aanwezigheid van andere internationale instellingen en financiële knooppunten, en België als specifiek *NATO Host Nation*, ons land bijzonder kwetsbaar maken als primair doelwit en frontlijnnatie voor vijandige hybride operaties;

[2] UAS zijn *Unmanned Aircraft Systems*.

O. considérant que des aéronefs sans équipage à bord (UAS[2]/drones) sont utilisés dans le cadre d'opérations de routine en conditions hybrides à des fins de collecte de renseignements, de sabotage ciblé, de perturbation des chaînes d'approvisionnement et des opérations aériennes civiles, ainsi que pour des opérations d'information et des opérations psychologiques; que ces opérations se déroulent le plus souvent avec le concours d'acteurs intermédiaires ou à partir de navires commerciaux afin de compliquer toute imputation de responsabilité et toute escalade; et que ces moyens constituent donc une menace directe pour les infrastructures critiques, la continuité des services vitaux et la confiance du public;

P. considérant que les citoyens, les pouvoirs locaux et les services civils sont en première ligne en cas de crise, si bien que la résilience sociétale, la communication transparente, la participation citoyenne et l'éducation aux médias sont essentielles lorsqu'il s'agit de contrer les influences étrangères déstabilisatrices;

Q. considérant que les élections libres et équitables sont une cible privilégiée pour des acteurs étrangers qui financent secrètement des partis politiques, mènent des campagnes de désinformation et sapent la confiance dans les résultats électoraux;

R. considérant que l'ensemble de la population est susceptible d'être soumise à des opérations de désinformation; que certains groupes comme les jeunes sont particulièrement vulnérables, que les réseaux sociaux sont des vecteurs très importants des opérations de désinformation;

S. vu le *Digital Services Act*, qui impose notamment des obligations aux grandes plateformes en matière de lutte contre la désinformation;

T. considérant que certains États tiers cherchent, afin d'influencer indûment les processus démocratiques, à recruter, parfois avec succès, des personnalités haut placées, ou à utiliser des diasporas, des universités ou des manifestations soi-disant culturelles;

U. considérant que l'implantation du siège de l'Union européenne et la présence d'autres institutions et centres financiers internationaux, ainsi que le statut de la Belgique en tant que nation hôte spécifique de l'OTAN, rendent notre pays particulièrement vulnérable en tant que cible privilégiée et nation de première ligne pour les opérations hybrides hostiles;

[2] UAS: *Unmanned Aircraft Systems* (systèmes d'aéronef sans équipage à bord)

V. gelet op de NAVO-top van juli 2023 te Vilnius, met de nadruk op cyberweerbaarheid en de verdediging tegen hybride dreigingen, en de NAVO-top in Den Haag van juni 2025, waar de versterking van de civiele en militaire weerbaarheid, de bescherming van kritieke infrastructuur en de verhoogde investeringen in defensie en cybercapaciteiten centraal stonden;

W. overwegende dat de NAVO de hybride aanvallen erkent als een mogelijke grond voor het inroepen van artikel 5 van het NAVO-verdrag, wat de ernst van deze dreiging onderstreept, en de NAVO-lidstaten, inclusief België, conform artikel 3 daarom verplicht zijn hun nationale weerbaarheid ten aanzien van de hybride dreiging aanzienlijk te versterken;

X. gezien de verschillende Europese wetgevende initiatieven en strategieën op het gebied van cyberbeveiliging en -defensie, evenals de nationale en regionale omzetting daarvan, die gericht zijn op het versterken van de veerkracht tegen hybride dreigingen;

Y. gezien de essentiële rol van het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) bij het bereiken van een gemeenschappelijk hoog niveau van cyberbeveiliging in de hele Europese Unie;

Z. overwegende dat de *Belgian National Risk Assessment* (BNRA) 2023-2026 van het Nationaal Crisiscentrum (NCCN) de dreiging van een "hybride actor" expliciet identificeert als een significant risico voor België;

AA. overwegende dat de jaarverslagen van de Algemene Dienst Inlichting en Veiligheid (ADIV) en de Veiligheid van de Staat (VSSE) consistent waarschuwen voor een intensifiëring van spionage, inmenging en sabotageactiviteiten op het Belgisch grondgebied;

BB. overwegende dat de Nationale Veiligheidsstrategie (NVS) van 2026 vijf vitale belangen vooropstelt die bepalend zijn voor de interne cohesie van ons land en het voortbestaan van onze maatschappij (rechtstaat, democratie, weerbaarheid en nationale waarden; fysieke veiligheid, territoriale integriteit; leefomgeving; economische welvaart; internationale orde; functionering van de EU);

CC. gelet op het regeerakkoord van 31 januari 2025, waarin hybride dreigingen als prioriteit worden aangemerkt, en waarin onder meer in volgende maatregelen wordt voorzien: de oprichting van een territoriale verdedigingslinie; een vrijwillige militaire dienst voor jongeren; een bijdrage van Defensie aan een weerbaarheidsplan; een strategie tegen buitenlandse inmenging met een

V. vu le sommet de l'OTAN de juillet 2023 à Vilnius, centré sur la cyber-résilience et la défense contre les menaces hybrides, et le sommet de l'OTAN de juin 2025 à La Haye, axé sur le renforcement de la résilience civile et militaire, la protection des infrastructures critiques et la hausse des investissements dans la défense et les cybercapacités;

W. considérant que l'OTAN reconnaît les attaques hybrides comme un motif possible d'invocation de l'article 5 du traité de l'OTAN, ce qui montre la gravité de cette menace, et que les États membres de l'OTAN, dont la Belgique, ont donc l'obligation, conformément à l'article 3, d'accroître sensiblement leur résilience nationale face à la menace hybride;

X. vu les différentes initiatives législatives et stratégies européennes en matière de cybersécurité et de cyberdéfense, ainsi que leur transposition aux niveaux national et régional, qui visent à renforcer la résilience face aux menaces hybrides;

Y. considérant le rôle essentiel de l'Agence de l'Union européenne pour la cybersécurité (ENISA) pour atteindre un niveau commun élevé de cybersécurité dans l'ensemble de l'Union européenne;

Z. considérant que l'évaluation nationale des risques pour la Belgique (BNRA) 2023-2026 du Centre de crise national (NCCN) identifie explicitement la menace d'un "acteur hybride" comme un risque significatif pour la Belgique;

AA. considérant que les rapports annuels du Service général du renseignement et de la sécurité (SGRS) et de la Sûreté de l'État (VSSE) lancent à bon droit une mise en garde contre une intensification des activités d'espionnage, d'ingérence et de sabotage sur le territoire belge;

BB. considérant que la Stratégie nationale de sécurité (SNS) de 2026 identifie cinq intérêts vitaux déterminants pour la cohésion interne de notre pays et la subsistance de notre société (l'état de droit, la démocratie, la résilience et les valeurs nationales; la sécurité physique, l'intégrité territoriale, le milieu de vie; la prospérité économique; l'ordre international; l'efficacité de l'UE);

CC. vu l'accord de gouvernement du 31 janvier 2025, qui considère les menaces hybrides comme une priorité et prévoit, entre autres, les mesures suivantes: la création d'une ligne de défense territoriale; un service militaire volontaire pour les jeunes; une contribution de la Défense à un plan de résilience; une stratégie de lutte contre l'ingérence étrangère, axée sur la protection des

focus op bescherming van de kritieke infrastructuur; investeringen in het cybercommando; en voldoende middelen voor de Algemene Dienst Inlichtingen en Veiligheid;

DD. gelet op de door de Europese Commissie recente voorgestelde Europese interne veiligheidsstrategie, genaamd *Protect EU*;

EE. gelet op het feit dat België de eerste Europese *"safe harbor"* voor ethische hackers is, die ethische hackers juridisch beschermt tegen vervolging mits strenge voorwaarden;

FF. overwegende dat de Europese Commissie een reeks instrumenten heeft ontwikkeld, zoals de *Hybrid Toolbox*, de *Digital Services Act*, de NIS2- en CER-richtlijnen en een mechanisme voor de screening van buitenlandse investeringen, die een kader vormen voor een gecoördineerde Europese aanpak, maar een actieve implementatie op federaal en regionaal niveau vereisen;

GG. gelet op het interdepartementale Platform Hybride Dreigingen (onder mandaat van het CCIV), dat de expertise van alle federale veiligheids- en inlichtingendiensten bundelt en de nationale aanpak van hybride dreigingen coördineert;

HH. gelet op het lidmaatschap van België sinds 2021 van het *Hybrid Centre of Excellence (Hybrid CoE)* in Helsinki, dat een belangrijke pijler vormt van de Belgische beleidsontwikkeling op het vlak van hybride dreigingen binnen een gezamenlijke Europese en trans-Atlantische aanpak;

II. gelet op de EU- en NAVO-ondersteuningsmechanismen waarop België een beroep kan doen, namelijk *EU Hybrid Rapid Response Teams (HRRT)* en *NATO Counter Hybrid Support Teams (CHST)*;

JJ. overwegende dat de aanvaarding van buitenlandse steun voor de ondermijning van de essentiële nationale belangen krachtens artikel 546 van het Strafwetboek een strafbaar feit is waarop een straf van niveau 3 staat;

KK. gelet op de *North Sea Summit* in Oostende in 2023 die tot de oprichting van het Noord-Zeeveiligheidspact (NorthSeal) leidde, met als deelnemende landen België, Nederland, Duitsland, Noorwegen, het Verenigd Koninkrijk en Denemarken;

LL. overwegende dat een effectieve respons op hybride dreigingen een paradigmaverschuiving vereist van een

infrastructures critiques; des investissements dans le cyber commandement; et des moyens suffisants pour le Service général du renseignement et de la sécurité;

DD. vu la stratégie européenne de sécurité intérieure proposée récemment par la Commission européenne, dénommée "*Protect EU*";

EE. vu le fait que la Belgique est le premier "refuge" européen pour les hackers éthiques, en ce qu'elle protège juridiquement ceux-ci contre les poursuites sous certaines conditions strictes;

FF. considérant que la Commission européenne a développé une série d'instruments, comme la boîte à outils hybride (*Hybrid Toolbox*), la législation sur les services numériques (*Digital Services Act*), les directives NIS2 et CER et un mécanisme de surveillance des investissements étrangers, qui constituent un cadre pour une approche européenne coordonnée mais qui requièrent une mise en œuvre active aux niveaux fédéral et régional;

GG. vu la plateforme interdépartementale Menaces hybrides (créée au sein du Comité de coordination pour le Renseignement et la Sécurité), qui rassemble l'expertise de tous les services fédéraux de sécurité et de renseignement et coordonne l'approche nationale face aux menaces hybrides;

HH. vu l'adhésion de la Belgique, depuis 2021, au Centre d'excellence hybride (CdE) d'Helsinki, qui constitue un pilier important de l'élaboration de la politique belge en matière de menaces hybrides dans le cadre d'une approche européenne et transatlantique commune;

II. vu les mécanismes de soutien de l'UE et de l'OTAN auxquels la Belgique peut faire appel, à savoir les équipes d'intervention rapide de l'UE en cas de menaces hybrides (HRRT) et les *Counter Hybrid Support Teams (CHST)* de l'OTAN;

JJ. considérant que l'article 546 du Code pénal a introduit l'acceptation d'une aide étrangère pour saper les intérêts nationaux essentiels comme infraction susceptible de peine de niveau 3;

KK. vu le sommet de la mer du Nord à Ostende en 2023 qui a abouti à la création du Pacte de sécurité pour la mer du Nord (NorthSeal), auquel la Belgique, les Pays-Bas, l'Allemagne, la Norvège, le Royaume-Uni et le Danemark sont parties;

LL. considérant qu'une réponse efficace aux menaces hybrides nécessite un changement de paradigme,

reactieve, sectorale benadering naar een proactieve, geïntegreerde strategie, oftewel een "*whole-of-government*"- en "*whole-of-society*"-benadering;

VERZOEKT DE FEDERALE REGERING:

1. inzake cyberdefensie:

1.1. de rol van de minister van Binnenlandse Zaken en Veiligheid inzake cyberveiligheid te versterken via een duidelijke en logische hergroepering van de veiligheidsbevoegdheden, waarbij het Centrum voor Cybersecurity België (CCB) wordt samengevoegd met andere relevante veiligheidsdepartementen, met uitzondering van het departement Justitie;

1.2. de militaire cybercapaciteiten van de Cyber Force en het Cyber Command van Defensie verder te ontwikkelen, in lijn met de Nationale Veiligheidsstrategie, met als kerntaak de defensienetwerken en de wapensystemen te beveiligen, en met een bijzondere focus op de interoperabiliteit en de informatiedeling binnen de NAVO en de EU;

1.3. de volledige en snelle omzetting van de Europese NIS2-richtlijn aan te houden, door de volledige implementatie en uitvoering van de wet van 26 april 2024[3] en het koninklijk besluit van 9 juni 2024[4] en het afdwingen van de verplichting om robuuste, proportionele cybersecuritymaatregelen te nemen door alle essentiële en belangrijke entiteiten in België;

1.4. een cultuur van cyberbeveiliging binnen de overheidsdiensten en bij de bevolking in het algemeen te ontwikkelen door middel van opleidingen, de verspreiding van goede praktijken en elke andere maatregel waarmee de aandacht kan worden gevestigd op die uitdaging;

1.5. te onderzoeken hoe binnen Defensie een programma voor ethische hackers kan worden opgezet om talent te identificeren en op te leiden en om de defensieve capaciteiten van de overheid en de vitale sectoren continu te testen en te versterken;

1.6. de rol van ENISA te versterken, zodat die organisatie uitgroeit tot een volwaardig agentschap dat de

[3] Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, bekendgemaakt in het *Belgisch Staatsblad* van 17 mei 2024.

[4] Koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, bekendgemaakt in het *Belgisch Staatsblad* van 24 juni 2024.

impliquant le passage d'une approche sectorielle réactive à une stratégie intégrée proactive, c'est-à-dire une approche pangouvernementale et pansociétale;

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. en ce qui concerne la cyberdéfense:

1.1. de renforcer le rôle du ministre de la Sécurité et de l'Intérieur dans le domaine de la cybersécurité grâce à un regroupement clair et cohérent des compétences en matière de sécurité, en réunissant le Centre pour la cybersécurité Belgique (CCB) et d'autres départements compétents en matière de sécurité, à l'exception du département de la Justice;

1.2. de développer plus avant les cybercapacités militaires de la Cyber Force et du Cyber Command de la Défense, conformément à la Stratégie nationale de sécurité, en lui donnant pour tâche principale de sécuriser les réseaux de défense et les systèmes d'armes, une attention particulière devant être accordée à cet égard à l'interopérabilité et au partage d'informations au sein de l'OTAN et de l'UE;

1.3. de poursuivre la transposition rapide et intégrale de la directive européenne NIS2 en veillant à la mise en œuvre et à l'exécution intégrales de la loi du 26 avril 2024[3] et de l'arrêté royal du 9 juin 2024[4] et en obligeant l'ensemble des entités importantes et essentielles en Belgique à prendre des mesures de cybersécurité efficaces et proportionnées;

1.4. de développer la culture de la cybersécurité au sein des administrations et de la population générale par des formations, la diffusion de bonnes pratiques et toute autre mesure permettant d'attirer l'attention sur cet enjeu;

1.5. d'examiner de quelle manière un programme destiné aux hackers éthiques pourrait être mis en place au sein de la Défense en vue d'identifier et de former les personnes ayant les aptitudes requises et afin de tester et de renforcer en continu les capacités défensives des autorités et des secteurs vitaux;

1.6. de consolider le rôle de l'ENISA, qui doit devenir une véritable agence coordonnant la réponse aux

[3] Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, publiée au *Moniteur belge* du 17 mai 2024.

[4] Arrêté royal du 9 juin 204 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, publié au *Moniteur belge* du 24 juin 2024.

respons op dreigingen en cyberaanvallen coördineert en dat over de middelen beschikt om de lidstaten rechtstreeks te ondersteunen, in het bijzonder bij gecoördineerde aanvallen tegen meerdere lidstaten;

1.7. de strategische keuze te maken voor digitale soevereiniteit en hierbij prioritair in te zetten op het gebruik van open standaarden, open source oplossingen en transparante governance-mechanismen om de kwaliteit, controleerbaarheid en weerbaarheid van onze digitale systemen te garanderen;

1.8. maatschappelijke initiatieven die industrie, academische wereld en overheid samenbrengen om de cyberweerbaarheid van het digitale ecosysteem te versterken, in navolging van succesvolle voorbeelden in buurlanden, structureel te ondersteunen;

2. inzake UAV's[5] in het lage luchtruim:

2.1. de minister van Mobiliteit te gelasten op Europees niveau te ijveren voor een verplicht Europees registratiesysteem voor alle drones, waarbij in real-time onderscheid wordt gemaakt tussen gekende (civiele) drones en ongeregistreerde, potentieel verdachte toestellen;

2.2. de rapportage en de informatie-uitwisseling van drone-incidenten prioritair te versterken en uit te diepen, door met name een sterke samenwerking tussen alle bevoegde overheidsdiensten, waaronder Defensie, Binnenlandse Zaken, SkeyDrone, VSSE, OCAD, NCCN, politiediensten en burgerluchtvaart- en havenautoriteiten[6];

2.3. het *National Air Security Center* te bevestigen als enige coördinatieplatform tussen alle bevoegde overheidsdiensten en als nationaal contactpunt voor C-UAS-incidentmelding;

2.4. waar mogelijk bij te dragen aan de versterking van forensische en analytische capaciteiten binnen de inlichtingenketen, teneinde, mits de nodige synergie en middelen dit toelaten, betrouwbare attributie en bewijsvoering richting internationale partners en sanctieprocedures te ondersteunen;

5 UAV's, (*unmanned aerial vehicle*), zijn vliegtuigen zonder menselijke piloot aan boord, die worden gebruikt voor verschillende toepassingen, variërend van militaire operaties tot recreatieve activiteiten.

6 SkeyDrone is een joint venture tussen de Belgische luchtverkeersleidingsdienst skeyes en Brussels Airport Company.

menaces et cyberattaques, et doit avoir les moyens de soutenir directement les États membres, spécialement lors d'attaques coordonnées contre plusieurs États membres;

1.7. d'opérer un choix stratégique en faveur de la souveraineté numérique et, dans ce cadre, de privilégier l'utilisation de normes ouvertes, de solutions open source et de mécanismes de gouvernance transparents afin de garantir la qualité, l'auditabilité et la résilience de nos systèmes numériques;

1.8. de soutenir de manière structurelle les initiatives sociétales réunissant l'industrie, le monde académique et les pouvoirs publics afin de renforcer la cyber-résilience de l'écosystème numérique, en s'inspirant des expériences concluantes menées dans les pays voisins;

2. en ce qui concerne les aéronefs sans pilote[5] (*Unmanned Aerial Vehicles,* UAV) dans l'espace aérien bas:

2.1. de charger le ministre de la Mobilité d'œuvrer au niveau européen en faveur d'un système d'enregistrement européen obligatoire pour tous les drones, permettant de distinguer en temps réel les drones connus (civils) des appareils non enregistrés et potentiellement suspects ;

2.2. de renforcer et de développer en priorité la procédure de signalement et d'échange d'informations concernant les incidents impliquant des drones, notamment par une collaboration active entre tous les services publics compétents, notamment la Défense, l'Intérieur, SkeyDrone, VSSE, OCAD, NCCN, les services de police et les autorités de l'aviation civile et portuaires[6];

2.3. de réaffirmer que le Centre national de sécurité aérienne (*National Air Security Center*) est l'unique plateforme de coordination entre tous les services publics compétents et le point de contact national pour la notification des incidents C-UAS;

2.4. de contribuer, dans la mesure du possible, au renforcement des capacités d'investigation et d'analyse au sein de la chaîne du renseignement de manière à renforcer, si les synergies et les moyens disponibles le permettent, une procédure d'attribution de responsabilité et d'administration de la preuve qui soit fiable aux yeux des partenaires internationaux ainsi que des procédures de sanction;

5 Les UAV (*unmanned aerial vehicle*) sont des aéronefs sans pilote humain à bord, qui sont utilisés pour diverses applications, allant des opérations militaires aux activités de loisirs.

6 SkeyDrone est une coentreprise entre skeyes, l'entreprise belge chargée du contrôle du trafic aérien, et Brussels Airport Company.

2.5. de samenwerking tussen Defensie, de private sector en de academische wereld te stimuleren om tot uitmuntende counter-UAS-technologie te komen en de kans te grijpen België een plaats te laten innemen als hoogtechnologisch pionier binnen Europa en de wereld;

2.6. met de NAVO- en de EU-partners in overleg te gaan om gezamenlijk tot een counter-UAS-beleid te komen;

2.7. regelmatig in de schoot van de bevoegde commissies van de Kamer van volksvertegenwoordigers te rapporteren over de drone-incidenten en de counter-UAS-operaties, inclusief de responsmaatregelen en het juridische kader;

3. inzake de infrastructuur:

3.1. te onderzoeken in hoeverre redundantie en "*resilience by design*", rekening houdend met de CER-wet, CER-richtlijn, NIS2-richtlijn en DORA-wetgeving, verder verplicht kunnen worden bij de ontwikkeling en de modernisering van kritieke infrastructuren, zoals dubbele dataverbindingen, noodvoedingen, back-upbesturingen en noodcommunicatiesystemen, om de continuïteit van de vitale diensten te verzekeren bij fysieke of cyberaanvallen en teneinde te voorkomen dat entiteiten zich richten op louter administratieve naleving;

3.2. te onderzoeken in hoeverre een nationaal opleidings- en/of certificeringsprogramma voor veiligheidsofficieren van kritieke entiteiten kan worden opgezet, in samenwerking met Defensie en het CCB, om een uniforme minimumexpertise in crisismanagement, cyberveiligheid en hybride dreigingsherkenning te garanderen;

3.3. in nauwe samenwerking met de infrastructuurbeheerder Infrabel, te onderzoeken hoe de militaire mobiliteit en de beveiliging van cruciale spoorweginfrastructuur en knooppunten die essentieel zijn voor strategische troepenverplaatsingen en logistieke defensie-operaties, kunnen worden verbeterd;

3.4. een nauwere samenwerking met de Europese partners binnen de *Critical Entities Resilience Directive* (CER) te verzekeren, met name om grensoverschrijdende dreigingen (energie-, transport- en datanetwerken) gezamenlijk te monitoren, te testen en te beschermen, zoals voor de beveiliging van de Westerschelde, als toegangspoort naar de Belgische zeehavens;

2.5. de stimuler la collaboration entre la Défense, le secteur privé et le monde académique dans l'optique de créer une technologie C-UAS de pointe et de donner l'occasion à la Belgique de jouer un rôle de pionnier en matière de haute technologie en Europe et dans le monde;

2.6. de se concerter avec les partenaires de l'OTAN et de l'UE afin d'élaborer conjointement une politique *Counter-UAS*;

2.7. de faire rapport régulièrement à la commission compétente de la Chambre des représentants sur les incidents impliquant des drones et les opérations *Counter-UAS*, y compris les mesures de réponse et le cadre juridique;

3. en ce qui concerne les infrastructures:

3.1. d'examiner dans quelle mesure la redondance et la résilience par conception ("*resilience by design*"), compte tenu de la loi CER, la directive CER, la directive NIS2 et la réglementation DORA, peuvent être rendues obligatoires dans le cadre du développement et de la modernisation des infrastructures critiques, comme les doubles connexions de données, les alimentations de secours, les procédures de *back-up* et les systèmes de communication d'urgence, afin de garantir la continuité des services vitaux en cas d'attaques physiques ou de cyberattaques et de manière à éviter que les entités se concentrent sur une conformité purement administrative;

3.2. de voir dans quelle mesure il est possible de mettre en place un programme national de formation et/ou de certification d'officiers de sécurité d'entités critiques en collaboration avec la Défense et le CCB, afin de garantir une expertise minimum uniforme en matière de gestion de crise, de cybersécurité et de reconnaissance des menaces hybrides;

3.3. d'examiner, en étroite concertation avec le gestionnaire d'infrastructure Infrabel, comment améliorer la mobilité militaire ainsi que la sécurité de infrastructures ferroviaires et des points nodaux qui sont cruciaux et essentiels aux déplacements stratégiques de troupes et aux opérations logistiques de la Défense;

3.4. de garantir une collaboration plus étroite avec les partenaires européens dans le cadre de la Directive sur la résilience des entités critiques (CER), notamment en vue de permettre une surveillance, un contrôle et une protection collectifs en matière de menaces transfrontalières (réseaux énergétiques, de transport et de données), par exemple à des fins de sécurisation de l'Escaut occidental, qui est la voie d'accès aux ports maritimes belges;

3.5. waar mogelijk de synergieën die bestaan tussen Defensie en het ESA Redu Centre te benutten;

3.6. binnen Defensie te onderzoeken welke rol zij kunnen spelen in ruimtebeveiliging, en hierbij oog te hebben voor de bescherming van de Belgische en de Europese satellieten en hun grondinfrastructuur;

4. inzake maritieme veiligheid en de Noordzee:

4.1. de Belgisch-Nederlandse Samenwerking tussen de marines, BENESAM, verder uit te diepen en een pad richting volledige integratie te onderzoeken, met name voor de krachtige bestrijding van de maritieme hybride dreiging en ook de civiele maritieme autoriteiten hierin te betrekken;

4.2. de engagementen van de *Ostend Declaration 2023* en en van het Noordzee-Veiligheidspact dat België met vijf buurlanden heeft afgesloten, zo goed mogelijk uit te voeren en uit diepen via informatiedeling, gezamenlijke oefeningen en afstemming van nationale procedures ter gemeenschappelijke beveiliging van de Noordzee;

4.3. aan te dringen op een vierde Noordzeetop, in navolging van die in Esbjerg, Oostende en Hamburg, waar defensie een minstens even belangrijke plaats moet innemen als energie, aangezien de thema's intrinsiek samenhangen;

4.4. de maritieme surveillancemogelijkheden in NAVO-verband waar mogelijk verder te versterken via een geïntegreerd *Maritime Awareness*-beeld en tevens te beogen dat deze infrastructuur complementair bijdraagt aan de klassieke maritieme veiligheid;

4.5. de federale minister bevoegd voor de Noordzee te gelasten om in samenwerking met de ministers bevoegd voor energie en telecommunicatie een nationaal plan voor de bescherming van onderzeese infrastructuur op te stellen;

4.6. de federale minister bevoegd voor de Noordzee te gelasten om in samenwerking met de ministers bevoegd voor energie en telecommunicatie een snelle herstelcapaciteit te ontwikkelen voor na een onderzees incident van sabotage of een ongeval waarbij cruciale kabels of leidingen werden beschadigd;

4.7. daarbij flankerende maatregelen te nemen waarbij herstelbestendigheid en beschermingsnormen standaard

3.5. de mettre à profit, dans la mesure du possible, les synergies qui existent entre la Défense et le Centre ESA de Redu;

3.6. d'examiner, au sein de la Défense, le rôle que celle-ci peut jouer en matière de sécurité spatiale, notamment en ce qui concerne la protection des satellites belges et européens et de leurs infrastructures au sol;

4. en ce qui concerne la sécurité maritime et la mer du Nord:

4.1. d'approfondir plus avant la coopération maritime belgo-néerlandaise BeNeSam et d'examiner la piste d'une intégration complète, notamment pour permettre une lutte efficace contre la menace hybride maritime, et d'y impliquer également les autorités civiles maritimes;

4.2. de concrétiser le mieux possible les engagements pris dans le cadre de la Déclaration d'Ostende 2023 et du Pacte de sécurité de la mer du Nord conclu entre la Belgique et cinq pays voisins, et de les approfondir, par le partage d'informations, des exercices conjoints et l'harmonisation des procédures nationales, en vue d'une sécurisation commune de la mer du Nord;

4.3. de demander instamment l'organisation d'un quatrième Sommet de la mer du Nord, faisant suite à ceux d'Esbjerg, d'Ostende et de Hambourg, où le thème de la défense occuperait une place au moins aussi importante que l'énergie, ces thèmes étant intrinsèquement liés;

4.4. de continuer à renforcer, dans la mesure du possible, les capacités de surveillance maritime dans le cadre de l'OTAN au travers d'une vision intégrée de la surveillance maritime et de veiller également à ce que cette infrastructure apporte une contribution complémentaire à la sécurité maritime classique;

4.5. de charger le ministre fédéral qui a la mer du Nord dans ses attributions d'élaborer, en collaboration avec les ministres qui ont l'Énergie et les Télécommunications dans leurs attributions, un plan national pour la protection des infrastructures sous-marine;

4.6. de charger le ministre fédéral qui a la mer du Nord dans ses attributions de développer, en collaboration avec les ministres qui ont l'Énergie et les Télécommunications dans leurs attributions, des capacités de réparation rapide après un incident sous-marin de sabotage ou un accident ayant endommagé des câbles ou des conduites essentiels;

4.7. de prendre à cet effet des mesures d'accompagnement qui intégreront systématiquement, dès la phase

vanaf de ontwerpfase van nieuwe infrastructuur worden meegenomen en een risicoanalyse verplicht dient te worden opgelegd bij werken in de nabijheid van onderzeese infrastructuur ter voorkoming van accidentele beschadiging;

4.8. daarbij de focus op de maritieme veiligheid niet te beperken tot de Noordzee, maar ook uit te breiden naar de Belgische havens en binnenlandse waterwegen, en in dat kader de bestaande samenwerkingsplatformen te versterken door de Lokale Comités voor Maritieme Beveiliging maximaal in te zetten op lokale informatie-uitwisseling en het overlegplatform van de Nationale Autoriteit voor Maritieme Beveiliging ten volle in te schakelen voor de aanpak van hybride dreigingen die het lokale niveau overstijgen;

4.9. de juridische mogelijkheden te onderzoeken om, binnen de grenzen van het internationaal recht, zoals UNCLOS, een robuuster inspectie- en handhavingsregime te ontwikkelen voor schepen die een duidelijk en acuut risico vormen voor de maritieme veiligheid, zelfs wanneer zij zich in de Exclusieve Economische Zone (EEZ) bevinden;

4.10. zich diplomatiek en in de toekomst te verzetten tegen een heropstart van de onderzeese Russische gasleiding *Nord Stream* of gelijkaardige projecten door België of haar Europese partners onder het huidige Russische regime;

5. inzake maatschappelijke weerbaarheid en crisisbeheer:

5.1. te streven naar een gedragen partnerschap tussen Defensie, de overheden (de federale regering, de deelstaten en de lokale besturen), de private sector (in het bijzonder de uitbaters van de vitale diensten) en het maatschappelijk middenveld, naar het voorbeeld van het "*Comprehensive Security*"-model van NAVO-partner Finland, waarin nationale weerbaarheid wordt gezien als een collectieve opdracht;

5.2. dit partnerschap spoedig te concretiseren door in de eerste plaats het Belgisch Nationaal Weerbaarheidsplan en het Belgisch Nationaal Enablement-plan te voltooien, als twee complementaire onderdelen van het Belgisch Nationaal Verdedigingsplan "SHIELD";

5.3. te onderzoeken hoe de Hoge Studies Veiligheid en Defensie toegankelijker te maken voor een breed publiek, zoals binnen de eigen federale ambtenarij, en de oprichting van een hoogwaardige "nationale veiligheidscursus" te onderzoeken, naar het voorbeeld van de Nationale Defensie Cursus (MPK) van NAVO-partner Finland, waarbij leidinggevenden uit de publieke en

de conception de nouvelles infrastructures, une capacité de réparation et des normes de protection, et rendront obligatoire la réalisation d'une analyse des risques lors de travaux effectués à proximité d'infrastructures sous-marines afin de prévenir tout dommage accidentel;

4.8. de ne pas limiter à cet égard l'attention portée à la sécurité maritime à la mer du Nord, mais de l'étendre également aux ports et aux voies navigables intérieures belges, et de renforcer, dans ce contexte, les plates-formes de coopération existantes en mobilisant au maximum les Comités locaux pour la Sûreté maritime, pour échanger des informations au niveau local, ainsi que la plateforme de concertation de l'Autorité nationale pour la sûreté maritime, pour faire face aux menaces hybrides qui dépassent le niveau local;

4.9. d'examiner, dans les limites du droit maritime international comme UNCLOS, les possibilités juridiques pour pouvoir mettre en place un système plus solide d'inspection et de maintien pour les navires présentant un risque aigu et évident pour la sécurité maritime, même lorsque ceux-ci se trouvent dans la zone économique exclusive (ZEE);

4.10. de s'opposer diplomatiquement, dans le futur, à une remise en service du gazoduc sous-marin russe *Nord Stream* ou de projets analogues par la Belgique ou ses partenaires européens, tant que le régime russe actuel reste en place;

5. en ce qui concerne la résilience sociale et la gestion de crise:

5.1. de s'efforcer d'instaurer un partenariat soutenu entre la Défense, les autorités (gouvernement fédéral, entités fédérées et pouvoirs locaux), le secteur privé (en particulier les exploitants des services vitaux) et la société civile, inspiré du modèle de "*Comprehensive Security*" (sécurité globale) de la Finlande, partenaire de l'OTAN, dans lequel la résilience nationale est considérée comme une mission collective;

5.2. de concrétiser rapidement ce partenariat en finalisant en premier lieu le Plan national de résilience et le Plan national d'enablement belges, deux composantes complémentaires du Plan national de défense belge "SHIELD";

5.3. d'examiner comment rendre les Hautes Études de sécurité et de défense plus accessibles à un large public, comme au sein de la fonction publique fédérale elle-même, et d'envisager la création d'un "cours de sécurité nationale" de qualité, calqué sur les formations et entraînements à la défense donnés par la MPK en Finlande, pays partenaire de l'OTAN, qui réunissent

de private sector, de media, de academische wereld en het maatschappelijk middenveld periodiek worden samengebracht om een gemeenschappelijke cultuur van weerbaarheid te bevorderen;

5.5. informatiecampagnes te blijven organiseren om de zelfredzaamheid van de bevolking te verhogen, met concrete en praktische informatie over hoe zij zich kunnen voorbereiden op noodsituaties, het verwerven van de basiskennis inzake EHBO en het kennen van de juiste informatiekanalen van de overheid in geval van een crisis;

6. inzake economische weerbaarheid:

6.1. de strategische industriepolitiek verder uit te bouwen, gericht op de ontwikkeling van industriële ecosystemen in domeinen die van vitaal belang zijn voor de nationale veiligheid en de defensie, waaronder de productie van defensiematerieel, cybertechnologie, energie-infrastructuur en kritieke componenten;

6.2. de samenwerking tussen de inlichtingen- en veiligheidsdiensten (VSSE, ADIV, CCB) en de economische regulatoren te versterken, om de informatie-uitwisseling over economische spionage, technologische diefstal en supply chain-inmenging te vergemakkelijken en geïntegreerde responsmechanismen uit te bouwen;

6.3. in de context van de NAVO en de EU actief te pleiten voor de erkenning van de economische veiligheid als een volwaardig onderdeel van de collectieve defensie, en voor de opname van de economische weerbaarheid als strategische pijler in de gezamenlijke veiligheidsplannen met de bondgenoten.

Brussel, 5 november 2026.

De voorzitter van de Kamer van volksvertegenwoordigers,

Peter De Roover

De griffier van de Kamer van volksvertegenwoordigers,

Nicole Marquet

périodiquement des dirigeants du secteur public, du secteur privé, des médias, du monde universitaire et de la société civile afin de promouvoir une culture commune de la résilience;

5.5. de continuer à organiser des campagnes d'information visant à accroître l'autonomie de la population, et notamment de lui donner des informations concrètes et pratiques sur la manière de se préparer aux situations d'urgence, d'acquérir les connaissances de base en secourisme et de connaître les bons canaux d'information des autorités publiques en cas de crise;

6. en ce qui concerne la résilience économique:

6.1. de poursuivre le déploiement d'une politique industrielle stratégique axée sur le développement d'écosystèmes industriels dans des domaines vitaux pour la sécurité nationale et la défense, comme la production de matériel de défense, la cybertechnologie, les infrastructures énergétiques et les composants critiques;

6.2. de renforcer la coopération entre les services de renseignement et de sécurité (VSSE, SGRS, CCB) et les régulateurs économiques afin de faciliter l'échange d'informations sur l'espionnage économique, le vol de technologie et l'ingérence dans la chaîne d'approvisionnement, et de mettre en place des mécanismes de réponse intégrés;

6.3. dans le cadre de l'OTAN et de l'UE, de plaider activement en faveur de la reconnaissance de la sécurité économique comme élément à part entière de la défense collective et en faveur de l'intégration de la résilience économique en tant que pilier stratégique dans les plans de sécurité communs avec les alliés.

Bruxelles, le 5 novembre 2026.

Le président de la Chambre des représentants,

La greffière de la Chambre des représentants,

Centrale drukkerij - Imprimerie centrale