DOC 56 **1158/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

12 november 2025

VOORSTEL VAN RESOLUTIE

ter bescherming van onze welvaartsstaat tegen hybride oorlogsvoering

(ingediend door de heer Axel Weydts en mevrouw Annick Lambrecht)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

12 novembre 2025

PROPOSITION DE RÉSOLUTION

visant à protéger notre État-providence contre la guerre hybride

(déposée par M. Axel Weydts et Mme Annick Lambrecht)

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*
Open Vld	:	*Open Vlaamse liberalen en democraten*
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)*

TOELICHTING

DAMES EN HEREN,

Dit voorstel van resolutie vraagt de regering om een geïntegreerde strategie uit te werken die onze welvaartsstaat beschermt tegen hybride oorlogsvoering door de weerbaarheid van de samenleving, de economie, de kritische infrastructuur en de democratische instellingen te versterken.

De wereld bevindt zich in een tijdperk waarin onze welvaartsstaat wordt ondermijnd door externe dreigingen. Oorlog wordt vandaag niet langer enkel met wapens gevoerd: de grenzen tussen oorlog en vrede vervagen in een voortdurende grijze zone waarin staten, bedrijven en andere actoren hun invloed uitoefenen via cyberaanvallen, desinformatie, economische chantage en sabotage. Deze hybride oorlogsvoering is uitgegroeid tot het kenmerk bij uitstek van de geopolitieke rivaliteit in de 21e eeuw. Niet enkel onze veiligheid, maar ook de fundamenten van onze welvaart en ons maatschappelijk vertrouwen worden geraakt.

In plaats van tanks of soldaten aan de grens zien we digitale virussen, misleidende informatiecampagnes en cyberaanvallen op onze ziekenhuizen, bedrijven, sociale media, infrastructuur en bevoorradingsketens. Het doel is duidelijk: onze samenleving verzwakken van binnenuit, polariseren en het vertrouwen in onze instellingen ondermijnen. De gevolgen daarvan raken rechtstreeks aan wat we samen hebben opgebouwd: ons samenlevingsmodel, onze economie en koopkracht, en het onderlinge vertrouwen dat de basis vormt van onze welvaartsstaat. Er is een nieuwe realiteit van permanente druk.

België in de frontlinie van de hybride dreiging

Door onze open economie, onze sterke digitalisering en onze internationale rol is België bijzonder kwetsbaar voor deze nieuwe vorm van agressie. Als gastland van de NAVO en de Europese Unie, als financiële en logistieke draaischijf, en als natie die inzet op kennis en innovatie, bevindt ons land zich in de frontlinie van de hybride dreigingen. De voorbije jaren hebben herhaaldelijke cyberaanvallen, desinformatiecampagnes en sabotagepogingen doorheen Europa aangetoond dat deze risico's niet louter theoretisch zijn, maar een reële bedreiging vormen voor onze veiligheid en ons sociaaleconomisch weefsel.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS

La présente proposition de résolution demande au gouvernement d'élaborer une stratégie intégrée visant à protéger notre État-providence contre la guerre hybride en renforçant la résilience de la société, l'économie, les infrastructures critiques et les institutions démocratiques.

Dans le climat mondial actuel, notre État-providence est ébranlé par des menaces extérieures. Aujourd'hui, la guerre ne se fait plus seulement avec des armes: la frontière entre guerre et paix s'estompe dans une zone grise permanente où les États, les entreprises et autres acteurs exercent leur influence par le biais de cyberattaques, de désinformation, de chantage économique et de sabotage. Cette guerre hybride est devenue la caractéristique par excellence de la rivalité géopolitique au XXIe siècle. Elle touche non seulement notre sécurité, mais aussi les fondements de notre prospérité et de notre confiance sociale.

Au lieu des chars ou des soldats à la frontière, nous voyons des virus numériques, des campagnes d'information trompeuses et des cyberattaques contre nos hôpitaux, nos entreprises, nos réseaux sociaux, nos infrastructures et nos chaînes d'approvisionnement. L'objectif est clair: affaiblir notre société de l'intérieur, la polariser et saper la confiance dans nos institutions. Les effets de cette guerre hybride affectent de plein fouet ce que nous avons construit ensemble: notre modèle de société, notre économie et notre pouvoir d'achat, ainsi que la confiance mutuelle qui constitue le fondement de notre État-providence. Nous sommes confrontés à une nouvelle réalité caractérisée par une pression permanente.

La Belgique en première ligne face à la menace hybride

Vu son économie ouverte, sa numérisation avancée et son rôle international, la Belgique est particulièrement vulnérable à cette nouvelle forme d'agression. En tant que pays hôte de l'OTAN et de l'Union européenne, plaque tournante financière et logistique et nation misant sur la connaissance et l'innovation, notre pays est en première ligne face aux menaces hybrides. Ces dernières années, la multiplication des cyberattaques, des campagnes de désinformation et des tentatives de sabotage à travers l'Europe a montré que ces risques n'étaient pas purement théoriques, mais constituaient une réelle menace pour notre sécurité et notre tissu socioéconomique.

Terwijl Rusland tegen Oekraïne een conventionele oorlog voert, woedt er parallel een onzichtbare oorlog van spionage, sabotage en manipulatie die rechtstreeks de welvaart en de veiligheid van de Europese landen raakt. De aanwezigheid van verdachte schepen en de zogenaamde schaduwvloot in de Noordzee, nabij windmolenparken en datakabels, toont aan hoe reëel de dreiging is voor onze maritieme en energie-infrastructuur en onderstreept de urgentie om onze economie te beschermen.

Naar een nieuwe veiligheidslogica

Om onze welvaartsstaat te beschermen, volstaat de klassieke veiligheidsarchitectuur niet langer. De hybride dreigingen overschrijden domeinen en vereisen een geïntegreerde aanpak waarin defensie, economie, energie, digitale veiligheid en maatschappelijke veerkracht samenkomen. We moeten evolueren naar een "*whole-of-society"*-model waarin burgers, bedrijven en overheden samenwerken om onze weerbaarheid te verhogen en partners worden in weerbaarheid, om collectief verantwoordelijk onze samenleving te beschermen.

Landen als Finland en Estland tonen hoe betrokken burgers, transparante communicatie en mediawijsheid bijdragen aan een veerkrachtige samenleving. België kan en moet uit deze en andere voorbeelden leren om een eigen model van "beschermde welvaart" te ontwikkelen, waarin veiligheid, solidariteit en democratie elkaar versterken.

Weerbaarheid als maatschappelijke investering

Weerbaarheid overstijgt het militaire domein en is een maatschappelijke en strategische investering. Ze gaat over de capaciteit van een samenleving om ontwrichting te voorkomen, schokken op te vangen en zich snel te herstellen, ongeacht de aard van de dreiging: militair, economisch, digitaal of maatschappelijk. Dit voorstel van resolutie bouwt voort op het brede begrip van nationale veiligheid en stelt een geïntegreerde strategie voor die de Belgische weerbaarheid versterkt op onderling verbonden domeinen:

1. cyberdefensie: van een loutere bescherming naar een geloofwaardige afschrikking, met een versterking van het Centrum voor Cybersecurity België (hierna: CCB) en de Cybermacht van Defensie;

Alors que la Russie mène une guerre conventionnelle contre l'Ukraine, une guerre invisible d'espionnage, de sabotage et de manipulation sévit en parallèle, affectant directement la prospérité et la sécurité des pays européens. La présence de navires suspects et de la "flotte fantôme" en mer du Nord, à proximité des parcs éoliens et des câbles de données, montre combien la menace qui pèse sur nos infrastructures maritimes et énergétiques est réelle et souligne l'urgence qu'il y a à protéger notre économie.

Vers une nouvelle logique de sécurité

L'architecture de sécurité classique ne suffit plus à protéger notre État-providence. Les menaces hybrides transcendent les différents domaines et exigent une approche intégrée combinant défense, économie, énergie, sécurité numérique et résilience sociétale. Nous devons évoluer vers un modèle pansociétal "*whole-of-society*", au sein duquel les citoyens, les entreprises et les pouvoirs publics travaillent ensemble pour renforcer notre résilience et puissent devenir des partenaires en matière de résilience, afin de protéger notre société de manière collectivement responsable.

En observant des pays comme la Finlande ou l'Estonie, on peut voir comment des citoyens engagés, une communication transparente et un bon discernement à l'égard des médias peuvent contribuer à construire une société résiliente. La Belgique peut et doit s'inspirer de ces exemples et d'autres pour bâtir son propre modèle de "prospérité protégée", dans lequel la sécurité, la solidarité et la démocratie se renforcent mutuellement.

La résilience en tant qu'investissement sociétal

La résilience dépasse le domaine militaire et constitue un investissement sociétal et stratégique. Elle concerne la capacité d'une société à prévenir la dislocation, à absorber les chocs et à se rétablir rapidement, que ce soit face à une menace militaire, économique, numérique ou sociétale. La présente proposition de résolution s'appuie sur le concept de sécurité nationale au sens large et propose une stratégie intégrée susceptible de renforcer la résilience de la Belgique dans plusieurs domaines interdépendants:

1. la cyberdéfense: passer d'une simple protection à une dissuasion crédible, incluant le renforcement du Centre pour la Cybersécurité Belgique (ci-après le CCB) et de la Force Cyber de la Défense;

2. bescherming tegen drones: de ontwikkeling van een nationaal detectienetwerk en een coördinatieplatform voor counter-UAS[1];

3. schrap infrastructuur: een verplichte stresstest, redundantie in ontwerp en bescherming van kritieke infrastructuur, ruimte- en maritieme activa;

4. maritieme veiligheid: een versterkte samenwerking met Nederland en de NAVO voor de surveillance en de bescherming van de Noordzee;

5. maatschappelijke weerbaarheid: de uitbouw van partnerschappen naar Fins model, de versterking van de civiele bescherming en burgerparticipatie;

6. bescherming van de democratie: de bestrijding van desinformatie, transparantie in de partijfinanciering, veilige verkiezingen en een sterke mediawijsheid;

7. economische weerbaarheid: een verminderde afhankelijkheid van autoritaire regimes, een screening van strategische investeringen en een stimulering van technologische autonomie.

Sinds 2021 worden hybride aanvallen expliciet erkend als potentiële grond voor het inroepen van artikel 5 van het NAVO-verdrag. De Belgische *National Risk Assessment* 2023-2026 identificeert de "hybride actor" als één van de meest waarschijnlijke en impactvolle dreigingen voor de komende jaren. Daarom is dit voorstel van resolutie een oproep tot strategische herbewapening. Niet met wapens alleen, maar met kennis, coördinatie, en maatschappelijke betrokkenheid. Door te investeren in de weerbaarheid beschermen we niet enkel onze infrastructuur, maar ook de fundamenten van onze democratische rechtsstaat, onze welvaart en ons vertrouwen in elkaar.

Zoals gewezen NAVO-secretaris-generaal Jens Stoltenberg het samenvatte: "*Resilience is our first line of defence*". Dit voorstel geeft daar een Belgisch, geïntegreerd en toekomstgericht antwoord op. Alleen zo beschermen we onze welvaartsstaat.

Axel Weydts (Vooruit)
Annick Lambrecht (Vooruit)

[1] Counter-UAS (C-UAS) verwijst naar technologieën en strategieën die zijn ontworpen om ongeoorloofde of vijandige drones te detecteren, te volgen en te neutraliseren.

2. la protection contre les drones: le déploiement d'un réseau de détection national et d'une plate-forme de coordination pour les dispositifs *Counter-UAS (Counter-Unmanned Aerial Systems)*[1];

3. les infrastructures: stress test obligatoire, redondance en projet et protection des infrastructures critiques, des actifs spatiaux et maritimes;

4. la sécurité maritime: une coopération renforcée avec les Pays-Bas et l'OTAN en vue de la surveillance et de la protection de la mer du Nord;

5. la résilience sociétale: la mise en place de partenariats sur le modèle finlandais, le renforcement de la protection civile et de la participation citoyenne;

6. la protection de la démocratie: la lutte contre la désinformation, la transparence dans le financement des partis politiques, la sécurité des élections et une solide éducation aux médias;

7. la résilience économique: réduction de la dépendance à l'égard des régimes autoritaires, screening des investissements stratégiques et stimulation de l'autonomie stratégique.

Depuis 2021, les attaques hybrides sont explicitement reconnues comme motif potentiel d'invocation de l'article 5 du traité de l'OTAN. L'évaluation nationale des risques pour la Belgique 2023-2026 identifie "l'acteur hybride" comme l'une des menaces les plus probables et les plus impactantes pour les années à venir. C'est pourquoi la présente proposition de résolution lance un appel à un réarmement stratégique, non seulement au moyen d'armes, mais aussi par le biais de la connaissance, de la coordination et de l'engagement sociétal. En investissant dans la résilience, nous protégeons non seulement nos infrastructures, mais aussi les fondements de notre état de droit démocratique, de notre prospérité et de notre confiance mutuelle.

Ainsi que l'ancien secrétaire général de l'OTAN, Jens Stoltenberg, le résumait, "la résilience est notre première ligne de défense" (traduction). La présente proposition donne à cet appel une réponse belge intégrée et orientée vers l'avenir. C'est là la seule manière de protéger notre État-providence.

[1] *Counter-UAS* (C-UAS) renvoie aux technologies et stratégies conçues pour détecter, suivre et neutraliser les drones illicites ou ennemis.

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 oorlogsvoering een combinatie vormt 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 oorlogsvoering 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 (FIMI2) 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 cyberaanvallen en/of datadiefstal op communicatienetwerken, financiële systemen, energienetwerken en industriële controlesystemen een directe bedreiging vormen voor de nationale veiligheid;

G. 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;

[2] 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 la guerre hybride combine 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 la guerre hybride, et en particulier la désinformation, vise 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 (FIMI2) 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 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;

G. 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;

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

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

I. 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;

J. overwegende dat zich concrete voorbeelden voordoen van hybride agressie in de Noord- en Oostzee met Ruslands zogenaamde "schaduwvloot" van anonieme olietankers en vrachtschepen die onder wisselende vlaggen varen om sancties te ontwijken en aantoonbaar rond vitale havens en energie-installaties opereren en mogelijk spioneren en saboteren;

K. overwegende dat onbemande luchtvaartuigen (UAS[3]/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;

L. 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;

M. 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;

[3] UAS zijn *Unmanned Aircraft Systems*.

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

I. 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;

J. considérant qu'il existe des exemples concrets d'agression hybride en mer du Nord et en mer Baltique avec la "flotte fantôme" russe composée de pétroliers et de cargos anonymes qui changent plusieurs fois de pavillon afin d'éluder les sanctions, opèrent manifestement à proximité de ports et d'installations énergétiques vitaux et se livrent potentiellement à des activités d'espionnage et de sabotage;

K. considérant que des aéronefs sans équipage à bord (UAS[3]/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;

L. 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;

M. 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;

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

N. gezien de groeiende strategische afhankelijkheid van satellieten voor cruciale maatschappelijke functies zoals communicatie, navigatie (Galileo), financiële transacties en aardobservatie (Copernicus), en de belangrijke rol die België speelt als vijfde grootste bijdrager aan de Europese Ruimtevaartorganisatie (ESA);

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

P. 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;

Q. 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;

R. 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;

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

T. overwegende dat de Nationale Veiligheidsstrategie (NVS) van 2021 een geïntegreerd beleid vooropstelt dat inzet op een versterkte weerbaarheid van ons land op alle niveaus waarbij zes vitale belangen worden vooropgesteld om te beschermen (de democratische rechtsstaat, de territoriale integriteit, de fysieke veiligheid, de economische veiligheid, de ecologische veiligheid en de sociale en politieke stabiliteit);

U. gelet op het regeerakkoord van 31 januari 2025, waarin hybride dreigingen als prioriteit worden

N. vu la dépendance stratégique croissante à l'égard des satellites pour des fonctions sociales cruciales telles que les communications, la navigation (Galileo), les transactions financières et l'observation de la Terre (Copernicus), ainsi que le rôle majeur joué par la Belgique en tant que cinquième plus grand contributeur de l'Agence spatiale européenne (ESA);

O. 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 de l'OTAN, rendent notre pays particulièrement vulnérable en tant que cible privilégiée et nation de première ligne pour les opérations hybrides hostiles;

P. 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;

Q. 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;

R. 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;

S. 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;

T. considérant que la Stratégie nationale de sécurité (SNS) de 2021 préconise une politique intégrée qui mise sur une résilience accrue de notre pays à tous les niveaux, axée sur la protection de six intérêts vitaux (l'état de droit démocratique, l'intégrité territoriale, la sécurité physique, la sécurité économique, la sécurité écologique et la stabilité sociale et politique);

U. vu l'accord de gouvernement du 31 janvier 2025, qui considère les menaces hybrides comme une priorité

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

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

W. 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;

X. 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 nationaal niveau vereisen;

Y. 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;

Z. overwegende dat een effectieve respons op hybride dreigingen een paradigmaverschuiving vereist van een 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. een vernieuwde nationale cyberstrategie op te stellen en te implementeren, die niet enkel reactief en defensief is, maar gebaseerd is op een geloofwaardige afschrikking, waarbij enerzijds de systemen zo robuust worden gemaakt dat een aanval zinloos wordt ("*deterrence by denial*") en anderzijds een capaciteit wordt ontwikkeld om een aanval te attribueren en een proportionele kost op te leggen aan de agressor ("*deterrence by punishment*");

1.2. de capaciteiten van het Centrum voor Cybersecurity België (CCB) verder uit te bouwen en te verankeren als

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

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

W. 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;

X. 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 au niveau national;

Y. 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;

Z. considérant qu'une réponse efficace aux menaces hybrides nécessite un changement de paradigme, 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. d'élaborer et de mettre en œuvre une nouvelle stratégie nationale en matière de cybersécurité, qui ne soit pas uniquement réactive et défensive, mais qui repose aussi sur une dissuasion crédible, ce qui implique, d'une part, d'accroître la robustesse des systèmes de manière à rendre vaine toute attaque (dissuasion par déni) et, d'autre part, de développer une capacité pour attribuer une attaque et infliger un préjudice proportionnel à l'agresseur (dissuasion par la punition);

1.2. de développer plus avant les capacités du Centre pour la cybersécurité Belgique (CCB) et d'ériger celui-ci

de centrale autoriteit voor de nationale cyberdefensie, met een verhoging van de middelen voor proactieve initiatieven zoals het *"Spear Warning"*-programma en het *"Belgian Anti-Phishing Shield*" (BAPS);

1.3. de militaire cybercapaciteiten van de Cybermacht 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;

1.4. een logische hergroepering en/of fusie van de veiligheidsdepartementen en de coördinatiemechanismen inzake cyberveiligheid te onderzoeken;

1.5. de volledige en snelle omzetting van de Europese NIS2-richtlijn te verzekeren, door de volledige implementatie en uitvoering van de wet van 26 april 2024[4] en het koninklijk besluit van 9 juni 2024[5] en het afdwingen van de verplichting om robuuste, proportionele cybersecuritymaatregelen te nemen door alle essentiële en belangrijke entiteiten in België;

1.6. het CCB als nationaal *Computer Security Incident Response Team* (CSIRT) de nodige middelen te geven om de verplichte incidentmeldingen volgens de NIS2-richtlijn effectief te verwerken en de betrokken entiteiten te ondersteunen;

1.7. in navolging van het initiatief "*Hack the Government 2024*" een federaal programma voor "ethische hackers" op te zetten en te financieren, in samenwerking met de academische instellingen en de private sector, om talent te identificeren en op te leiden om de defensieve capaciteiten van de overheid en de vitale sectoren continu te testen en te versterken;

2. inzake UAV's[6] in het lage luchtruim:

en tant qu'autorité centrale pour la cyberdéfense nationale, en augmentant ses moyens pour des initiatives proactives comme le programme "*Spear Warning*" et le système "*Belgian Anti-Phishing Shield*" (BAPS);

1.3. de développer plus avant les cybercapacités militaires de la Force Cyber 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;

1.4. d'étudier la possibilité de procéder au regroupement et/ou une fusion logique des départements de sécurité et des mécanismes de coordination en matière de cybersécurité;

1.5. de procéder à 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[4] et de l'arrêté royal du 9 juin 2024[5] et en obligeant l'ensemble des entités importantes et essentielles en Belgique à prendre des mesures de cybersécurité efficaces et proportionnées;

1.6. d'allouer au CCB, en tant que Centre national de réponse aux incidents de sécurité informatique (CSIRT), les moyens nécessaires pour qu'il puisse traiter effectivement les signalements obligatoires d'incidents conformément à la directive NIS2 et soutenir les entités concernées;

1.7. de mettre en place et de financer, dans le prolongement de l'initiative "*Hack the Government 2024*", un programme fédéral pour "hackers éthiques", en collaboration avec les institutions académiques et le secteur privé, en vue d'identifier et de former les personnes ayant les aptitudes requises pour pouvoir tester et renforcer en continu les capacités défensives des autorités et des secteurs vitaux;

2. en ce qui concerne les aéronefs sans pilote[6] (*Unmanned Aerial Vehicles,* UAV) dans l'espace aérien bas:

4 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.

5 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.

6 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.

4 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.

5 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.

6 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.

2.1. een nationaal detectie- en waarschuwingsnetwerk op te richten voor de vroegtijdige opsporing van onbemande en niet-aangemelde luchtvaartuigen;

2.2. 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;

2.3. 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[7];

2.4. een *single point of contact* of coördinatieplatform aan te stellen tussen alle bevoegde overheidsdiensten met één nationaal contactpunt voor C-UAS-incidentmelding en respons;

2.5. aangepaste noodprocedures voor de luchthavens en de private luchtvaart te ontwikkelen en tegen het licht te houden om de veiligheid van het vliegverkeer te waarborgen bij drone-incursies;

2.6. te investeren in technische forensische middelen en analytische teams voor de inlichtingendiensten om betrouwbare attributie en bewijsvoering richting internationale partners en sanctieprocedures mogelijk te maken;

2.7. de samenwerking tussen de publiek-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;

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

2.9. 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, het juridische kader en de budgettaire uitgaven in verband met hybride drone-dreigingen;

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

2.1. de créer un réseau national de détection et d'alerte pour la détection précoce d'aéronefs sans pilote et non déclarés;

2.2. 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 ;

2.3. 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[7];

2.4. d'instaurer un point de contact unique ou une plateforme de coordination entre tous les services publics compétents, en prévoyant un point de contact national unique pour le signalement des incidents C-UAS et la réponse à ceux-ci;

2.5. de développer des procédures d'urgence adaptées pour les aéroports et l'aviation privée et de les analyser afin de garantir la sécurité du trafic aérien en cas d'incursions de drones;

2.6. d'investir dans des moyens techniques d'investigation et des équipes d'analyse pour les services de renseignement afin de pouvoir disposer d'une procédure d'attribution de responsabilité et d'administration de la preuve qui soit fiable aux yeux des partenaires internationaux et de procédures de sanction;

2.7. de stimuler la collaboration entre le secteur public et le secteur privé et le monde académique afin de pouvoir 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;

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

2.9. 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, le cadre juridique et les dépenses budgétaires liées aux menaces hybrides de drones;

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

3. inzake de infrastructuur:

3.1. de uitbaters van kritieke infrastructuur, vastgelegd volgens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren[8], te verplichten om periodieke en realistische stresstests uit te voeren die specifiek gericht zijn op hybride scenario's om de reële weerbaarheid van de organisatie en haar crisisrespons te evalueren;

3.2. te onderzoeken in hoeverre redundantie en "*resilience by design*", rekening houdend met de CERN-richtlijn, 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;

3.3. 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;

3.4. de veiligheidsnormen en -protocollen voor het nationale spoorwegnet aan te vullen, in nauw overleg met de infrastructuurbeheerder Infrabel, waarbij naast de huidige focus op operationele veiligheid, kabeldiefstal en spoorlopen nood- en beveiligingsprocedures noodzakelijk zijn inzake de dreiging van een gecoördineerde sabotage bij cruciale knooppunten en seinhuizen;

3.5. 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;

3.6. met de EU- en de NAVO-partners in gesprek te gaan om na te gaan of België als hoofdzetel van de EU- en NAVO-instellingen de last van anti-hybride oorlogsvoering alleen kan dragen of mogelijk ondersteunende middelen van partners nodig heeft, met name inzake anti-spionage;

[8] Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, bekendgemaakt in het *Belgisch Staatsblad* van 15 juli 2011.

3. en ce qui concerne les infrastructures:

3.1. d'imposer aux exploitants d'infrastructures telles que définies dans la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques[8], l'obligation de réaliser des tests de résistance périodiques et réalistes, spécifiquement axés sur des scénarios hybrides, afin de pouvoir évaluer la résilience réelle de l'organisation et sa capacité de réaction en cas de crise;

3.2. d'examiner dans quelle mesure la redondance et la résilience par conception ("*resilience by design*"), compte tenu de la directive du CERN, 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;

3.3. 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;

3.4. de compléter les normes et protocoles de sécurité pour le réseau ferroviaire national, en étroite concertation avec le gestionnaire d'infrastructure Infrabel, en mettant l'accent, outre sur la sécurité opérationnelle, les risques de vols de câbles et d'intrusions sur les voies, comme c'est déjà le cas actuellement, sur les procédures d'urgence et de sécurisation à mettre en place pour contrer toute menace de sabotage coordonné aux points nodaux et postes de signalisation cruciaux;

3.5. 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);

3.6. d'engager le dialogue avec les partenaires de l'UE et de l'OTAN afin de déterminer si la Belgique, en tant que siège des institutions de l'UE et de l'OTAN, peut supporter seule la charge que représente la guerre anti-hybride ou si elle a besoin de l'aide de ses partenaires, notamment en matière de contre-espionnage;

[8] Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, publiée au *Moniteur belge* du 15 juillet 2011.

3.7. de belangrijke rol van België binnen de Europese Ruimtevaartorganisatie (ESA), met name met het ESA Redu Centre, op financieel en wetenschappelijk vlak te blijven verderzetten;

3.8. een integrale nationale strategie voor de beveiliging van ruimte-activa (*"space security"*) te ontwikkelen, met een kader voor de fysieke en cybernetische bescherming van Belgische en 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;

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 ter gemeenschappelijke beveiliging van de Noordzee;

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

4.4. in nauwe samenwerking met de NAVO, de marine van verhoogde en permanente surveillancemogelijkheden te voorzien, met inbegrip van de gecoördineerde inzet van bemande en onbemande systemen (lucht-, oppervlakte- en onderwaterdrones), sensoren op de vaste installaties en geavanceerde satellietmonitoring, teneinde de verdachte activiteiten op zee of nabij maritieme infrastructuren in realtime te detecteren en te monitoren;

4.5. een nationaal plan voor de bescherming van onderzeese infrastructuur ("*seabed security"*) op te stellen en te implementeren, dat voorziet in een publiek-privaat partnerschap met de uitbaters van deze infrastructuur, gefocust op preventie, detectie en herstel;

4.6. een snelle herstelcapaciteit te ontwikkelen voor na een onderzees incident van sabotage of een ongeval waarbij cruciale kabels of leidingen werden beschadigd;

3.7. de faire en sorte que la Belgique puisse continuer à assumer le rôle important qui est le sien au sein de l'Agence spatiale européenne (ESA), grâce notamment au Centre Redu de l'ESA et ce, sur le plan tant financier que scientifique;

3.8. de développer une stratégie nationale globale pour la sécurisation d'actifs spatiaux ("*space security*"), en prévoyant un cadre pour la protection physique et cybernétique 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;

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 en vue d'une sécurisation commune de la mer du Nord;

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

4.4. de doter la marine, en étroite collaboration avec l'OTAN, de capacités de surveillance renforcées et permanentes, incluant le déploiement coordonné de systèmes avec et sans équipage (drones sous-marins, aériens et terrestres), de capteurs sur les installations fixes et d'une surveillance satellitaire avancée, afin de permettre la détection et la surveillance en temps réel des activités suspectes en mer ou à proximité d'infrastructures maritimes;

4.5. d'élaborer et de mettre en œuvre un plan national pour la protection des infrastructures sous-marines (sécurité des fonds marins, "*seabed security"*) prévoyant un partenariat public-privé avec les exploitants de ces infrastructures, axé sur la prévention, la détection et la réparation;

4.6. de développer 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 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;

4.8. 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. een structureel en permanent partnerschap te creëren 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. 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 private sector, de media, de academische wereld en het maatschappelijk middenveld periodiek worden samengebracht om een gemeenschappelijke cultuur van weerbaarheid te bevorderen;

5.3. een versnelling hoger te schakelen in het organiseren en het promoten van vrijwilligerskorpsen en vrijwillige maatschappelijke engagementen, met name een maatschappelijke dienst voor een inzet bij Defensie, de hulpdiensten (brandweer, civiele bescherming), de zorgsector of sociale projecten;

5.4. de capaciteiten van de Civiele Bescherming en het Nationaal Crisiscentrum te moderniseren en te versterken om beter voorbereid te zijn op grootschalige, langdurige en complexe crisissen die het gevolg kunnen zijn van hybride aanvallen, met name langdurige, wijdverspreide stroomuitval, de grootschalige disruptie van communicatienetwerken of een crisis in de voedsel- of drinkwatervoorziening;

4.7. 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);

4.8. 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. d'instaurer un partenariat structurel et permanent 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 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 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;

5.3. d'accélérer l'organisation et la promotion des corps de volontaires et des engagements volontaires au service de la société, parmi lesquels un service citoyen au sein de la Défense, des services de secours (services d'incendie, protection civile), du secteur des soins ou de projets sociaux;

5.4. de moderniser et renforcer les capacités de la Protection civile et du Centre de crise national afin qu'ils soient mieux préparés à faire face à des crises de grande envergure, de longue durée et complexes qui pourraient résulter d'attaques hybrides, notamment des coupures d'électricité à grande échelle et de longue durée, des perturbations à grande échelle des réseaux de communication ou une crise de l'approvisionnement en nourriture et en eau potable;

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;

5.6. bij de gemeenschapsregeringen aan te dringen EHBO-cursussen een vaste en periodieke plek in het curriculum van het secundair onderwijs te geven en een samenwerking met de Medische Dienst van Defensie te onderzoeken;

6. inzake desinformatie en democratie:

6.1. een volledige uitvoering te geven aan het opzetten van een interdepartementaal mechanisme voor het opsporen, het monitoren, het analyseren en het rapporteren van desinformatie- en informatie-operaties, zoals voorzien in de Nationale Veiligheidsstrategie van 2021;

6.2. een strategie en procedures te ontwikkelen voor de publieke attributie van desinformatiecampagnes aan statelijke actoren, sinds het publiekelijk benoemen van verantwoordelijkheden een krachtig instrument is om de ontkenbaarheid van hybride acties te doorbreken en de politieke en reputatiekost voor de agressor te verhogen;

6.3. bij de gemeenschapsregeringen aan te dringen om een versnelling hoger te schakelen in het uitrollen en het aanpassen van de lespakketten mediawijsheid en digitaal burgerschap aan de nieuwe uitdagingen, met als doel de cognitieve weerbaarheid van de bevolking tegen manipulatie, desinformatie en polariserende narratieven structureel te verhogen;

6.4. de crisiscommunicatiecapaciteiten van de overheid tegen het licht te houden en indien nodig te versterken, sinds het essentieel is om snel transparant, consistent en accuraat te communiceren in tijden van crisis;

6.5. samen met de deelstaten de onafhankelijkheid en de pluriformiteit van het Belgische medialandschap te ondersteunen als een cruciale buffer tegen buitenlandse beïnvloeding waar nodig;

6.6. de transparantie van onlineplatformen te verhogen via een strikte en proactieve handhaving van de *Digital Services Act* (DSA), met bijzondere aandacht voor de

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;

5.6. d'insister auprès des gouvernements des Communautés afin qu'ils intègrent dans le programme de l'enseignement secondaire des cours de secourisme donnés à intervalles réguliers, et qu'ils examinent la possibilité d'une collaboration avec le Service médical de la Défense;

6. en ce qui concerne la désinformation et la démocratie:

6.1. de mener à bien la mise en place d'un mécanisme interdépartemental pour la détection, la surveillance, l'analyse et le rapportage d'opérations de désinformation et d'information, comme le prévoit la Stratégie de sécurité nationale de 2021;

6.2. de développer une stratégie et des procédures permettant d'imputer publiquement des campagnes de désinformation à des acteurs étatiques, sachant que la dénonciation publique des responsables est un moyen efficace d'empêcher l'agresseur de nier les actions hybrides et de lui faire assumer les conséquences politiques de ses actions et leurs retombées sur sa réputation;

6.3. d'insister auprès des gouvernements des Communautés pour qu'ils accélèrent la mise en œuvre des modules d'éducation aux médias et à la citoyenneté numérique et leur adaptation aux nouveaux défis, afin de renforcer structurellement la résilience cognitive de la population face à la manipulation, à la désinformation et aux discours polarisants;

6.4. d'évaluer les capacités de communication de crise des autorités publiques et, si nécessaire, de les renforcer, sachant qu'il est essentiel en temps de crise d'assurer une communication rapide, transparente, cohérente et précise;

6.5. en concertation avec les entités fédérées, de soutenir, partout où cela est nécessaire, l'indépendance et la diversité du paysage médiatique belge, lequel constitue un rempart fondamental contre les influences étrangères;

6.6. d'accroître la transparence des plateformes en ligne en veillant, de manière stricte et proactive, au respect de la législation européenne sur les services

verplichtingen van zeer grote onlineplatformen om de risico's van desinformatie te mitigeren;

6.7. in lijn met de aanbevelingen uit het GRECO-rapport van 7 mei 2024, de wet van 4 juli 1989 betreffende de financiering van politieke partijen te herzien om elke vorm van directe of indirecte financiering door buitenlandse staten, of door entiteiten die onder hun controle staan, ondubbelzinnig te verbieden;

6.8. te onderzoeken of de controlemogelijkheden en de middelen van de parlementaire controlecommissie voor de verkiezingsuitgaven en de boekhouding van de politieke partijen kunnen worden versterkt om een effectieve handhaving te verzekeren;

6.9. de cyberbeveiliging van de volledige verkiezingsinfrastructuur, van de systemen voor de registratie van kiezers en de digitale communicatie van de partijen tot de software voor de telling van de stemmen, te onderwerpen aan een onafhankelijke en diepgaande audit door het Centrum voor Cybersecurity (CCB), en zo veel mogelijk uitvoering te geven aan de daaropvolgende aanbevelingen;

6.10. de Belgische parlementsleden, de experts en de Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking actief aan te moedigen om deel te nemen aan verkiezingswaarnemingsmissies in landen van de Europese Politieke Gemeenschap en aan de NAVO Oost- en Zuidflank, en Belgische *soft power* in te zetten om de democratie in het ons nabije buitenland te ondersteunen;

6.11. een beleid voor informatieveiligheid te ontwikkelen en te implementeren voor alle overheidsdiensten en aanverwante instellingen, met een duidelijk evenwicht tussen de openbaarheid van bestuur enerzijds en de bescherming van gevoelige informatie anderzijds, om te voorkomen dat de openbaar beschikbare data door hybride actoren kunnen worden misbruikt;

7. inzake economische weerbaarheid:

7.1. de energie-weerbaarheid van België te versterken door het energieaanbod verder te diversifiëren, de strategische infrastructuur te beveiligen en langetermijncontracten af te sluiten met betrouwbare partners, met het oog op het verminderen van de afhankelijkheid van autoritaire regimes en het beschermen tegen energiechantage;

numériques (*Digital Services Act*), et en étant particulièrement attentif aux obligations des très grandes plateformes en ligne, et ce afin d'atténuer les risques de désinformation;

6.7. conformément aux recommandations formulées dans le rapport du Groupe d'États contre la corruption (GRECO) du 7 mai 2024, de réviser la loi du 4 juillet 1989 relative au financement des partis politiques afin d'interdire catégoriquement toute forme de financement direct ou indirect par des États étrangers ou par des entités qu'ils contrôlent;

6.8. d'étudier la possibilité de renforcer les capacités de contrôle et les moyens de la Commission parlementaire de contrôle des dépenses électorales et de la comptabilité des partis politiques afin d'assurer le respect effectif de la législation;

6.9. de soumettre à un audit indépendant et approfondi, réalisé par le Centre pour la Cybersécurité Belgique (CCB), la cybersécurité de l'ensemble de l'infrastructure électorale, depuis les systèmes d'enregistrement des électeurs et la communication numérique des partis jusqu'aux logiciels de comptage des voix, et de mettre autant que possible en œuvre les recommandations qui en résulteront;

6.10. d'encourager les parlementaires belges, les experts et les agents du Service public fédéral Affaires étrangères, Commerce extérieur et Coopération au développement à participer à des missions d'observation électorale dans des pays de la Communauté politique européenne et sur les flancs oriental et méridional de l'OTAN, et d'user du *soft power* de la Belgique pour soutenir la démocratie dans les pays voisins;

6.11. d'élaborer et de mettre en œuvre une politique de sécurité de l'information pour tous les services publics et institutions connexes, en établissant un équilibre clair entre la transparence administrative, d'une part, et la protection des informations sensibles, d'autre part, afin d'empêcher que les données accessibles au public ne soient utilisées à mauvais escient par des acteurs hybrides;

7. en ce qui concerne la résilience économique:

7.1. de renforcer la résilience énergétique de la Belgique en diversifiant davantage l'offre énergétique, en sécurisant les infrastructures stratégiques et en concluant des contrats à long terme avec des partenaires fiables, en vue de réduire la dépendance à l'égard de régimes autoritaires et de se protéger contre le chantage énergétique;

7.2. te onderzoeken hoe de financiële sector beter kan worden geïntegreerd in het nationale weerbaarheidsbeleid, met aandacht voor cyberdreigingen, sanctie-ontwijking, witwaspraktijken en buitenlandse inmenging in financiële instellingen;

7.3. 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;

7.4. binnen het kader van het *European Chips Act*[9], in samenwerking met de deelstaten actief deel te nemen aan de Europese initiatieven ter bevordering van de technologische soevereiniteit, onder meer door de onderzoeks- en productiecapaciteit voor halfgeleiders in België te versterken en door de samenwerking met gelijkgezinde landen te stimuleren;

7.5. 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;

7.6. het mandaat, de middelen en de effectiviteit van de Interfederale Screeningscommissie (ISC) voor buitenlandse directe investeringen (*Foreign Direct Investment*, FDI) grondig te evalueren en waar nodig te versterken;

7.7. de interfederale taskforce economische veiligheid, opgericht naar aanleiding van de *European Economic Security Strategy* (EESS)[10], structureel te verankeren als een permanent coördinatieplatform tussen de federale en de gewestelijke overheden, in nauw overleg met de private sector, om de risico's op economische dwang, sabotage of verstoring tijdig te detecteren en te mitigeren;

7.8. in aansluiting bij de *European Economic Security Strategy* (EESS) en de aanbevelingen van de Europese

[9] Verordening (eu) 2023/1781 van het Europees Parlement en de Raad van 13 september 2023 tot vaststelling van een kader voor maatregelen ter versterking van het Europese halfgeleiderecosysteem en tot wijziging van Verordening (EU) 2021/694 (chipsverordening), bekendgemaakt in het *Publicatieblad van de Europese Unie* van 18 september 2023.

[10] Gezamenlijke mededeling aan het Europees Parlement, de Europese Raad en de raad betreffende een "strategie voor economische veiligheid van de EU", gedaan te brussel op 20 juni 2023.

7.2. d'examiner comment mieux intégrer le secteur financier dans la politique nationale de résilience, en accordant une attention particulière aux cybermenaces, au contournement des sanctions, aux pratiques de blanchiment et à l'ingérence étrangère dans les institutions financières;

7.3. 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;

7.4. de participer activement, dans le cadre de la législation européenne sur les semi-conducteurs (*European Chips Act*[9]) et en concertation avec les entités fédérées, aux initiatives européennes de promotion de la souveraineté technologique, notamment en renforçant la capacité de recherche et de production de semi-conducteurs en Belgique et en stimulant la coopération avec les pays partageant une même vision;

7.5. 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;

7.6. d'évaluer en profondeur le mandat, les moyens et l'efficacité du Comité de filtrage interfédéral (CFI) pour les investissements directs étrangers (IDE), et de les renforcer si nécessaire;

7.7. d'ancrer structurellement la *task force* interfédérale pour la sécurité économique, créée dans le cadre de la stratégie européenne en matière de sécurité économique (EESS)[10], en tant que plate-forme de coordination permanente entre l'autorité fédérale et les autorités régionales, en étroite concertation avec le secteur privé, afin de détecter à temps et d'atténuer les risques de coercition économique, de sabotage ou de perturbation;

7.8. conformément à la stratégie européenne en matière de sécurité économique et aux recommandations de la

[9] Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (règlement sur les puces), publié au *Journal officiel de l'Union européenne* du 18 septembre 2023.

[10] Communication conjointe au Parlement européen, au Conseil européen et au Conseil relative à la "Stratégie européenne en matière de sécurité économique", faite à Bruxelles le 20 juin 2023.

Commissie van juni 2023, een Belgische strategie voor de economische veiligheid te ontwikkelen die de weerbaarheid van de kritieke sectoren en technologieën (zoals kwantumtechnologie, halfgeleiders, AI, biotechnologie, ruimtevaart en defensie-industrie) bevordert, en die voorziet in een afwegingskader tussen de open handel en de nationale veiligheid;

7.9. een "*resilience test*" te introduceren voor de strategische sectoren en de ondernemingen met een nationale veiligheidsrelevantie, die periodiek de robuustheid van hun bedrijfscontinuïteit, cybersecurity en afhankelijkheden beoordeelt, vergelijkbaar met de stresstests in de financiële sector;

7.10. het *EU Anti-Coercion Instrument* (ACI)[11] actief te benutten om de economische weerbaarheid van België en de EU tegen dwangmaatregelen door derde landen te versterken;

7.11. in overleg met de deelstaten, te voorzien in ondersteuningsmechanismen voor kmo's die actief zijn in de kritieke waardeketens, zodat zij toegang krijgen tot financiering, cyberbescherming en exportdiversificatie-instrumenten om hun weerbaarheid tegen buitenlandse druk of overnames te vergroten;

7.12. in samenwerking met de academische wereld en denktanks, te onderzoeken of naar analogie met het Egmontinstituut voor de Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelings-samenwerking, de Federale Overheidsdienst Economie, K.M.O., Middenstand en Energie een Belgisch centrum voor economische veiligheid en weerstand kan oprichten, dat onderzoek, opleiding en advies aanbiedt over de economische veiligheid, de hybride dreigingen en de strategische autonomie;

7.13. 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

Commission européenne de juin 2023, de déployer une stratégie belge en matière de sécurité économique visant à favoriser la résilience des secteurs et technologies critiques (tels que la technologie quantique, les semi-conducteurs, l'IA, la biotechnologie, l'industrie spatiale et l'industrie de défense), et prévoyant un cadre d'arbitrage entre le commerce ouvert et la sécurité nationale;

7.9. d'instaurer, pour les secteurs stratégiques et les entreprises présentant un intérêt pour la sécurité nationale, un "test de résilience" qui évalue périodiquement la robustesse de leur continuité d'exploitation, leur cybersécurité et leurs dépendances, à l'instar de ce qui se fait dans le secteur financier avec les tests de résistance;

7.10. de mettre activement à profit l'Instrument anti-coercition de l'UE (IAC)[11] pour renforcer la résilience économique de la Belgique et de l'UE contre les mesures de coercition prises par des pays tiers;

7.11. de prévoir, en concertation avec les entités fédérées, des mécanismes de soutien aux PME actives dans les chaînes de valeur critiques, de sorte qu'elles aient accès au financement, à la cyberprotection et à des instruments de diversification des exportations leur permettant d'accroître leur résilience face aux pressions ou rachats étrangers;

7.12. d'examiner, en collaboration avec le monde académique et les groupes de réflexion universitaires, si, par analogie avec l'Institut Egmont créé dans le cadre du Service public fédéral Affaires étrangères, Commerce extérieur et Coopération au développement, le Service public fédéral Économie, PME, Classes moyennes et Énergie pourrait créer un centre belge pour la sécurité et la résilience économiques, qui proposerait des services de recherche, de formation et de conseil en matière de sécurité économique, de menaces hybrides et d'autonomie stratégique;

7.13. 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

[11] Verordening (EU) 2023/2675 van het Europees Parlement en de Raad van 22 november 2023 betreffende de bescherming van de Unie en haar lidstaten tegen economische dwang door derde landen, bekendgemaakt in het *Publicatieblad van de Europese Unie* van 10 juli 2024, L 90.409.

[11] Règlement (UE) 2023/2675 du Parlement européen et du Conseil du 22 novembre 2023 relatif à la protection de l'Union et de ses États membres contre la coercition économique exercée par des pays tiers, publié au *Journal officiel de l'Union européenne* du 10 juillet 2024, L 90.409.

weerbaarheid als strategische pijler in de gezamenlijke veiligheidsplannen met de bondgenoten.

21 oktober 2025

Axel Weydts (Vooruit)
Annick Lambrecht (Vooruit)

économique en tant que pilier stratégique dans les plans de sécurité communs avec les alliés.

21 octobre 2025

Centrale drukkerij - Imprimerie centrale