ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
27 mai 2026
Séance de 11 heures

Compte rendu n° 71

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de M. Jean-Michel Jacques, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures.

M. le président Jean-Michel Jacques. Mes chers collègues, nous accueillons à présent Mme Agnès Romatet-Espagne, directrice des affaires internationales, stratégiques et technologiques au secrétariat général de la défense et de la sécurité nationale (SGDSN).

Madame la directrice, votre direction est chargée de dossiers internationaux au sein du SGDSN. Elle assure un suivi des principales crises ou conflits dans le monde et coordonne la réflexion interministérielle sur les évolutions stratégiques en cours. La revue nationale stratégique (RNS) 2025 anticipe à l'horizon 2030 un conflit de haute intensité en Europe, qui s'accompagnerait d'actions hybrides massives. Nos compétiteurs et adversaires mènent déjà de telles actions, non seulement dans les espaces traditionnels comme le cyber, mais également dans le champ informationnel en métropole, dans nos outre-mer, en Afrique, et même sur des territoires moins habituels, comme l'Arctique et le Grand Nord.

Ces attaques diverses interviennent également dans les espaces exo-atmosphériques ou les fonds marins. De nouveaux modes d'action aussi sont utilisés, comme des survols de drones, des sabotages ou des actes de provocation. Nous attendons de vous, madame la directrice, que vous nous dressiez aujourd'hui un panorama de la menace et d'où elle prend ses sources. Nous pensons naturellement à la Russie, mais elle n'est pas la seule puissance à recourir à ce genre de méthode agressive, sous le seuil de la guerre conventionnelle. À ce titre, nous serions également très intéressés si vous pouviez nous dresser un panorama des différents acteurs qui mènent ce genre d'attaques hybrides.

Mme Agnès Romatet-Espagne, directrice des affaires internationales, stratégiques et technologiques au Secrétariat général de la défense et de la sécurité nationale. Je voudrais, si vous me le permettez, profiter de cette audition pour prendre un peu de recul, cerner ce concept de menaces hybrides et en dresser un panorama. Il s'agit également pour moi de revenir sur les actions conduites par le SGDSN et la France dans ce domaine, à la fois sur le plan national, dans un cadre européen, et peut-être également dans un cadre otanien.

Il convient de revenir avec précision sur ce que recouvrent les stratégies hybrides, en rappelant d'emblée que leur définition est rigoureuse et que chacun des termes employés est délibérément choisi. Pour la France, les stratégies hybrides correspondent au recours, par un acteur étranger, à une combinaison intégrée et volontairement ambiguë de modes d'action militaires et non militaires, directs et indirects, légaux ou illégaux, difficilement attribuables. Jouant avec les seuils estimés de ripostes et de conflits armés, cette combinaison est conçue pour contraindre et affaiblir la France et ses partenaires.

Cette ambiguïté constitue un ressort central, puisqu'elle permet à l'attaquant d'agir en dessous du seuil de conflictualité ouvert, en jouant avec les limites de riposte qui pourraient entraîner un affrontement. Dans cette logique, l'un des éléments les plus critiques tient à la difficulté d'attribuer les actions. Elle permet aux acteurs d'avancer masqués.

Afin de structurer notre analyse, treize champs de l'hybridité ont été identifiés sur le territoire national, une catégorisation reprise du document de référence de l'Union européenne, établi avec le Centre d'excellence d'Helsinki (CoE) en 2021, « *The landscape of Hybrid Threats: A conceptual model* ». Ces treize champs sont les suivants : le cyber,

l'informationnel, l'arsenalisation du droit ou *lawfare*, le champ politique, les entraves à nos opérations militaires, le spatial, les infrastructures dites d'importance vitale, le champ économique, le champ culturel, le champ sociétal, le champ diplomatique, le champ du renseignement et le champ des services publics.

Parmi ces domaines, certains apparaissent comme davantage prioritaires, en raison de la fréquence des attaques et de leur détectabilité, notamment le cyber, la manipulation de l'information, le *lawfare*, l'économie et les entraves aux opérations militaires. De notre côté, nous rajoutons le champ spatial, qui s'impose désormais comme un domaine d'avenir à risque élevé pour le futur.

Le recours à ces stratégies poursuit des objectifs multiples. Il s'agit d'abord de fragiliser durablement un État ou la cohésion et les valeurs de sa société par la perturbation, la sidération, la paralysie, l'intimidation, la déstabilisation ou la remise en cause de la légitimité de ses institutions. Ensuite, ces stratégies sont employées pour imposer une volonté contraire aux intérêts de la cible, c'est-à-dire de l'État visé, ou l'influencer dans la durée sans qu'elle en ait pleinement conscience.

Elles permettent également de placer la cible devant le fait accompli, tout en entravant sa capacité de réponse, notamment dans des scénarios combinant conflit conventionnel et pressions hybrides simultanées, comme celui retenu dans le cadre de la RNS. Elles cherchent aussi à augmenter progressivement le seuil de réponse en produisant des actions dont les effets sont très légèrement au-dessus de ce qui est considéré comme inacceptable, mais n'entraîne pour autant pas de réponse de la part de la victime, en recherchant un effet de cliquet. Enfin, elles visent à saper la cohésion entre Alliés et partenaires et à entraver ainsi les capacités de réponses collectives ou coordonnées. Depuis 2022, la France a fait l'objet de stratégies hybrides de plus en plus désinhibées, qui ont pour objet de porter préjudice à notre image et de polariser l'opinion publique. Les outre-mer ont été particulièrement visés, comme vous l'avez très justement rappelé, monsieur le président. Dans le domaine des cyberattaques, les principales menaces proviennent d'acteurs réputés liés à la Chine et à la Russie ; ou à des acteurs criminels affiliés à des compétiteurs stratégiques, avec une confusion de plus en plus prononcée entre la criminalité organisée et les moyens de cyberattaque. Ces actions prennent la forme d'espionnage, de vols de données, de cyberattaques par rançongiciels ou des attaques par déni d'accès.

L'utilisation de l'économie comme une arme stratégique est de plus en plus assumée depuis 2022. Les espaces communs, comme les espaces aériens, la très haute altitude, l'espace exo et extraatmosphérique, les fonds marins ou les espaces maritimes font l'objet d'une compétition renouvelée et de stratégies hybrides qui se déploient tous azimuts. La très haute altitude est un domaine peu régulé, qui est nouvellement exploité par des compétiteurs. Je pense par exemple au survol délibéré d'au moins un ballon stratosphérique chinois au-dessus des États-Unis en 2023. S'agissant des grands fonds marins, les menaces visent tout particulièrement les infrastructures dédiées à l'énergie et aux télécommunications.

Moscou mène à ce titre des actions hostiles et subversives en Europe : sabotages, assassinats ciblés, tentatives visant des hauts responsables politiques, manœuvres visant notre base industrielle et technologique de défense (BITD), couplées à des manœuvres d'intimidation nucléaire et à une agressivité conventionnelle. La Russie a également multiplié les actions hostiles vis-à-vis de la France en deçà du conflit direct. À ce sujet, Anne-Sophie

Dhiver, directrice adjoint de Viginum, est déjà venue évoquer devant vous les manœuvres informationnelles.

Je ne reviendrai pas non plus sur les sabotages, espionnages, détentions arbitraires de ressortissants, survols du territoire de certains alliés, velléités d'ingérence dans les processus électoraux, manifestations hostiles contre les forces françaises et alliées, actions sur le territoire national pour déstabiliser nos sociétés. À l'échelle européenne, un pic a été observé en 2024, notamment dans le contexte des Jeux olympiques, suivi d'une possible phase de réorganisation des forces russes visant à accroître l'efficacité des actions menées. Le recours aux *proxys*, qui ne sont d'ailleurs jamais russes, est systématique dans ces attaques. Les trois pays les plus ciblés à l'échelle européenne sont la France, l'Allemagne et la Pologne, en raison de notre soutien à l'Ukraine et de l'influence que nous pouvons exercer au sein de l'Union européenne.

Les ingérences chinoises sur notre territoire national se concentrent dans deux domaines en particulier : le contrôle de la diaspora chinoise en France et la prédation du patrimoine scientifique et technologique de la nation, sujet qui a d'ailleurs fait l'objet de propositions dans l'actualisation de la loi de programmation militaire, que vous avez été conduits à examiner il y a quelques jours.

Le troisième acteur que nous identifions comme l'un des plus critiques est l'Iran, qui fait peser une menace sur le territoire national, notamment en ayant recours à des *proxys* issus du milieu de la criminalité organisée pour mener des actions. Par ce biais, la République islamique d'Iran cherche d'abord à cibler sur le territoire national des cibles juives ou en lien avec Israël. Sous réserve des résultats de l'enquête en cours, et selon les premiers éléments qui ont déjà été rendus publics par le ministre de l'intérieur notamment, l'attentat qui a été déjoué contre le siège parisien de la Bank of America fin du mois de mars pourrait avoir été mené par des proxys commandités par le pouvoir iranien.

Face à ces menaces, comment agissons-nous ? La revue nationale stratégique propose deux objectifs stratégiques en particulier. Le premier vise l'objectif d'une France unie et résiliente. L'acculturation de nos citoyens, et en particulier de nos jeunes, aux enjeux de défense et de sécurité nationale, en particulier aux manœuvres hybrides dans les champs informationnels, constitue une priorité. En effet, si nous ne savons pas ce contre quoi nous devons nous battre, et si nos concitoyens n'en ont pas conscience, comment le faire efficacement ?

Un objectif stratégique est spécifiquement dédié à l'hybridité dans la revue nationale stratégique, l'objectif stratégique n° 9, qui prévoit une capacité à agir dans les champs hybrides. Il faut que d'ici 2030, la France soit parvenue à contraindre ses adversaires, et tout particulièrement la Russie, et à les décourager dans la mise en œuvre de leur stratégie hybride.

Face à ces constats, des moyens supplémentaires doivent être donnés à la communauté du renseignement, à la lutte cyber. De plus, le dispositif interministériel de lutte contre les ingérences numériques étrangères doit être renforcé. Nous travaillons activement sur le développement d'outils de lutte contre le *lawfare*, notamment dans le domaine économique, ce qui implique nécessairement un relais européen.

Il nous faut aussi disposer d'une organisation nationale robuste. Au niveau interministériel, depuis 2019, ma direction en constitue le point de contact. Nous devons, à ce titre, à la fois travailler sur la doctrine, mais aussi sur le champ européen. À l'avenir, l'un des enjeux résidera également dans la capacité à mesurer et à anticiper l'évolution de ces menaces.

Leur caractère diffus, progressif et souvent invisible rend difficile l'identification des changements d'échelle. L'image d'une montée en température progressive, imperceptible au départ, illustre bien cette difficulté. C'est pourquoi des travaux sont en cours pour mieux structurer les outils d'analyse, agréger les signaux faibles et relier les informations issues de différents champs, afin de disposer d'une lecture consolidée de la situation.

Nous réfléchissons donc à la manière de mieux mesurer et avoir une vision consolidée de ce que nous sommes en train de vivre et de ce que nous pourrions vivre. Nos travaux d'anticipation, également conduits par ma direction, doivent nous permettre de mieux faire face à ces situations. Chaque acteur qui maîtrise techniquement son sujet est responsable selon ses prérogatives ; par exemple Viginum pour les menaces visant les manipulations d'informations, ou l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour le cyber. Pour notre part, le secrétaire général préside un comité de liaison sécurité économique, et un groupe de travail est dédié à l'arsenalisation juridique. Chacun est responsable dans son champ, mais il s'agit également de faire travailler ces différents acteurs ensemble, pour pouvoir disposer d'une vision commune.

En conclusion, je souhaite revenir sur le volet européen. Ce sujet est pris en compte à Bruxelles, dans le cadre du groupe de travail « Renforcement de la résilience et lutte contre les menaces hybrides » (ERCHT). Je rappelle à ce sujet que dès la Boussole stratégique de 2022, le Conseil de l'Union européenne avait placé les menaces hybrides au cœur des menaces de l'environnement stratégique.

Dans ce cadre, une boîte à outils hybrides a été constituée. Opérationnelle depuis 2022, elle est activée principalement par les États membres, mais également par des États partenaires. En cas de campagne hybride, les équipes de réaction rapide sont maintenant constituables. Elles ont d'ailleurs été actionnées à deux reprises, en Moldavie en 2025 et récemment en Arménie.

À ce titre, une boîte à outils est spécifiquement dédiée à la lutte contre les manipulations de l'information d'origine étrangère (*Foreign Information Manipulation and Interference* ou FIMI) à Bruxelles. En outre, un régime de sanctions spécifiquement dédié aux acteurs de déstabilisation russe a été mis en place. Des sanctions ont été prises à travers cinq paquets, contre soixante-neuf individus et dix-neuf entités listés au titre de l'hybridité. Enfin, une réflexion a été entamée par Bruxelles sur un régime horizontal de sanctions qui ne viserait pas spécifiquement un pays. Il faudrait également évoquer les actions conduites dans le cadre de l'Otan ; peut-être aurons-nous l'occasion d'y revenir lors de vos questions.

M. le président Jean-Michel Jacques. Je cède la parole aux orateurs de groupe

M. José González (RN). La lecture de la feuille de route 2026-2027 du SGDSN confirme à quel point la menace cyber est devenue un enjeu stratégique majeur pour la continuité de l'État et la protection de notre souveraineté nationale. Les cyberattaques récentes et massives visant nos administrations, nos opérateurs critiques ou nos infrastructures

numériques montrent que nos adversaires contournent aujourd'hui les formes classiques de confrontations militaires pour nous fragiliser dans la durée. Malheureusement, la réponse apportée par l'État a pu paraître, pour beaucoup, sous-dimensionnée.

Il faut aussi relever que la dimension transnationale des cyberattaques rend les coopérations internationales incontournables, qu'il s'agisse du partage de renseignements techniques, de l'identification des menaces, de la protection des infrastructures critiques ou encore de la réponse coordonnée à des attaques d'ampleur.

Je souhaiterais donc vous interroger sur trois points précis. D'abord, très directement, j'aimerais savoir comment la SGDSN évalue aujourd'hui le niveau de coopération opérationnelle entre la France et ses partenaires en matière de cybersécurité et de lutte contre les menaces hybrides. Les mécanismes de partage d'informations et d'alertes vous paraissent-ils suffisamment réactifs face à l'accélération et la massification des attaques ?

Ensuite, dans un contexte de compétition internationale, comment équilibrez-vous l'approfondissement nécessaire des coopérations cyber avec la préservation de notre autonomie stratégique et de notre souveraineté numérique ? Quelle dépendance technologique et quel mécanisme de mutualisation peuvent, à terme, créer des vulnérabilités pour la France ?

Enfin, puisqu'il faut considérer l'évolution rapide des technologies de rupture, pouvez-vous nous éclairer un peu plus sur les coopérations mises en place ou envisagées dans ces domaines structurants ?

Mme Agnès Romatet-Espagne. Je ne peux parler à la place de Vincent Strubel de la qualité des coopérations qu'il peut conduire avec des partenaires, dont je sais qu'ils sont de plus en plus nombreux à le solliciter. D'après ce que j'en vois, ces coopérations sont à la fois désirées par l'Anssi, évidemment dans la limite de ses moyens humains disponibles, mais qu'elles sont également productives.

Il est d'ailleurs possible d'identifier les pays avec lesquels ces coopérations se développent. Je pense notamment à certains pays qui ne viennent pas toujours spontanément à l'esprit, comme Singapour, avec lequel la coopération dans le domaine cyber est particulièrement solide, mais également à plusieurs partenaires européens ainsi qu'au Canada, qui manifeste une forte demande dans ce domaine. Ces coopérations présentent un caractère mutuellement bénéfique.

La question de la sécurité numérique est liée à celle de la souveraineté numérique et de la sécurité nationale. Cette problématique s'inscrit dans une dynamique naturellement européenne, compte tenu des fragilités liées à la nature des équipements et à l'hébergement des données, selon qu'elles reposent ou non sur des infrastructures cloud souveraines. Ces sujets sont désormais mieux pris en compte, y compris à Bruxelles, où une réflexion est engagée sur les dépendances à l'égard de certains fournisseurs, qui pourraient créer des fragilités.

Cela étant, il ne saurait être question d'un sevrage immédiat ou global, qui serait à la fois irréaliste et techniquement impraticable. Une telle transformation ne peut s'inscrire que dans le temps long, et requiert des moyens budgétaires et techniques, ainsi qu'une planification de longue haleine.

En matière de coopération, nous ne pouvons pas adopter une approche exhaustive. Nos capacités ne le permettent pas, et nous privilégions des partenariats ciblés avec des États partageant des systèmes et des préoccupations similaires. C'est dans cet esprit que nous entretenons des coopérations étroites avec les Britanniques. Nous nous efforçons également d'établir une telle coopération avec l'Allemagne, dont la prise de conscience sur les enjeux hybrides est plus récente, mais s'accélère. Nous collaborons également avec des partenaires comme l'Australie, le Canada ou Singapour.

Ces coopérations s'inscrivent souvent dans des dispositifs institutionnels comparables aux nôtres, qui facilitent naturellement le dialogue. Elles répondent à une demande croissante de nos interlocuteurs, mais également à notre propre besoin de confrontation des analyses, de partage d'informations sur les menaces et, le cas échéant, de dialogue en amont sur la communication publique relative à ces enjeux.

Mme Corinne Vignon (EPR). Je souhaite vous interroger à propos du dispositif de protection du potentiel scientifique et technique piloté par le SGDSN. Cet indispensable dispositif interministériel visant à contrôler l'accès aux savoir-faire et infrastructures les plus sensibles des laboratoires de recherche et des sites industriels stratégiques de notre pays a été rénové en intégrant de nouvelles menaces comme certains usages de l'IA, du calcul quantique, des biotechnologies de synthèse ou encore des technologies spatiales.

Le rapport sénatorial du 29 septembre 2021 sur les influences étatiques extra-européennes dans le monde universitaire et académique français avait estimé à cinquante-deux le nombre d'établissements de l'enseignement supérieur et de la recherche qui adhèrent au dispositif, avec 563 zones à régime restrictif (ZRR) couvrant plus de 150 unités de recherche.

Le rapport avait dressé trois constats. Premièrement, le seuil de vigilance est trop haut et ne s'applique qu'à des risques élevés, comme les intérêts économiques, militaires, la prolifération et le terrorisme. Deuxièmement, il n'est pas adapté aux nouvelles stratégies d'influence et reste largement sous les radars des institutions académiques et judiciaires. Enfin, il souffre d'un manque global de moyens, de coordination, de sensibilisation de la communauté académique à l'émergence des nouvelles menaces.

Deux risques concernaient particulièrement le dispositif interministériel : l'intrusion, c'est-à-dire l'entrée non autorisée dans les zones à régime restrictif ; et la captation, c'est-à-dire le vol ou le détournement des documents ou de matériel au sein d'une ZRR. Ces risques portent directement atteinte à notre souveraineté. Madame la directrice, quel est le niveau de protection effective des ZRR ? A-t-il été relevé ?

Mme Agnès Romatet-Espagne. Les zones à régime restrictif, au nombre d'environ 1 500 aujourd'hui sur le territoire national, ont pour objet de matérialiser, au sein d'entités publiques comme privées, une restriction d'accès. Concrètement, cela signifie que toute personne souhaitant y entrer doit faire l'objet d'une vérification préalable, afin de garantir la protection d'informations ou de savoir-faire sensibles.

Les modes de captation d'informations sont parfois extrêmement simples. L'accueil d'un stagiaire, la participation à une délégation étrangère ou encore des coopérations internationales apparemment anodins peuvent s'avérer très dangereux.

La hausse du nombre de ZRR s'accompagne d'une prise de conscience accrue, très fortement encouragée par le ministère de l'enseignement supérieur et de la recherche, de la réalité de la menace, dans un environnement qui a pu parfois faire preuve de naïveté. La direction générale de la sécurité intérieure (DGSI) y contribue également de manière décisive.

Il importe toutefois de concilier cette exigence de protection avec le maintien des principes fondamentaux de la recherche, en particulier la liberté académique et la nécessaire ouverture internationale. L'enjeu consiste donc à garder les yeux grands ouverts sur les éléments qui sont partagés et les risques qui peuvent en découler.

Ils incluent, en premier lieu, les atteintes à la sécurité économique, l'un des risques couverts par le dispositif de protection du potentiel scientifique et technique de la nation (PPST). Ils concernent également la prolifération d'armes de destruction massive, le risque de contribuer au renforcement des capacités militaires d'un adversaire, ainsi que la menace terroriste.

Enfin, une évolution récente des risques mérite d'être soulignée, à savoir le phénomène de débauchage. Il s'agit pour des acteurs étrangers de recruter des experts de haut niveau, souvent en fin de carrière, disposant d'une expertise pointue et de réseaux étendus, afin de capter des connaissances stratégiques. Face à ce risque, des dispositions nouvelles ont été introduites, permettant de soumettre à autorisation les projets de départ à l'étranger de ces profils sensibles. L'objectif n'est pas d'entraver les mobilités, mais de garantir que ces départs ne s'accompagnent pas d'un transfert de savoirs ou d'informations susceptibles de porter atteinte à notre souveraineté. Il me vient par exemple à l'esprit, l'exemple de la furtivité dans le domaine des sous-marins.

La disposition soumise à votre Assemblée nous permettra simplement de vérifier que ceux qui pourraient – très légitimement – vouloir poursuivre une carrière à l'étranger demandent l'autorisation. Il s'agit simplement de vérifier qu'ils ne partent pas avec des informations ou des connaissances qui seraient de nature à porter atteinte à notre sécurité et à notre souveraineté.

M. Arnaud Saint-Martin (LFI-NFP). Je souhaite également vous interroger sur les zones à régime restrictif dans les universités et les laboratoires de recherche, dont le périmètre a été étendu par un cavalier législatif assez laborieux lors de l'actualisation de la loi de programmation militaire (LPM).

Mon groupe et moi-même avons exprimé notre inquiétude et notre soutien aux communautés scientifiques concernées autant que consternées, qui ne cessent de nous alerter depuis que cette disposition a été votée. De plus en plus nombreuses et proliférantes, ces ZRR transforment des établissements publics à caractère scientifique et technologique comme l'Institut national de recherche en sciences et technologies du numérique (Inria) en bunkers, et bientôt d'autres, par contagion. Les ZRR sont devenues par glissement progressif et sans véritable débat démocratique un instrument de contrôle de la recherche technico-scientifique placé sous la surveillance du SGDSN, qui s'imposerait presque comme directeur de laboratoire.

Les chercheurs peuvent ainsi être empêchés d'accéder à leurs établissements sans motivation écrite et sans justification, silence valant refus, ouvrant la voie à des dérives. Je pense notamment à cette chercheuse recrutée en postdoctorat à Bordeaux, qui a été écartée

d’une ZRR sans explication, la seule cause plausible étant son engagement militant au mouvement Soulèvements de la Terre, organisation légale et légitime.

Ces dérives inquiètent, d’autant plus que la répression à l’égard de l’engagement dans l’enseignement supérieur s’intensifie. Depuis 2024, le dispositif s’étend même aux sciences humaines et sociales, ces disciplines reconnaissant les principes de la *disputatio* et l’exercice autonome de la pensée critique, sont désormais exposées à l’appréciation hétéronome du renseignement intérieur.

Or on rappellera qu’un arsenal juridique existe déjà pour prévenir la France de la divulgation d’informations. Dès lors, pourquoi l’adjonction d’un tel surcontrôle ? Comment sera-t-il techniquement mis en œuvre ? Pourquoi concernera-t-il seulement les chercheurs hors Union européenne (UE) ? Disposez-vous d’éléments d’évaluation transmissibles aux parlementaires, qui justifieraient une telle évolution du dispositif initié en 2011 ? Si tel n’est pas le cas, vous engagez-vous à le faire dans un délai raisonnable ?

Enfin, le média *Disclose* a révélé que l’entreprise Sermat continuait à vendre en 2025 des composants pour faire fonctionner les drones Male israéliens, les composants n’entrant pas dans le champ des biens classés à double usage. Y a-t-il eu une réévaluation des procédures de classement des biens à double usage, à la suite de cette affaire ? Comment le SGDSN a-t-il adapté ce dispositif placé sous son autorité ?

Mme Agnès Romatet-Espagne. Vous me donnez l’occasion de revenir sur un dispositif qui a été conçu avec un souci d’équilibre particulièrement marqué. Tout d’abord, je tiens à vous rassurer : ce n’est évidemment pas le SGDSN, avec ses moyens limités, qui est chargé d’instruire l’ensemble des demandes relatives aux accès aux zones à régime restrictif. Le dispositif repose sur une procédure structurée éprouvée, et qui prévoit des voies de recours.

En réalité, les personnes concernées par les dispositions introduites dans la loi de programmation militaire ne représentent qu’un nombre très restreint de chercheurs. Il s’agit uniquement de profils travaillant sur des technologies particulièrement critiques et disposant d’un niveau d’expertise, d’expérience et de réseaux les rendant particulièrement attractifs pour des acteurs étrangers. Pour ces profils, une obligation est instaurée ; elle consiste à solliciter une autorisation préalable en cas de collaboration ou de départ à l’étranger. Cette demande est adressée à leur ministère de tutelle, et une procédure d’appel est prévue en cas de désaccord avec la décision initiale.

Il ne me semble pas choquant que l’on puisse, dans certaines circonstances, refuser l’accès à des laboratoires détenant des informations critiques pour notre sécurité nationale à des scientifiques de certaines nationalités, dont nous savons qu’ils travaillent dans des domaines qui peuvent porter atteinte à notre dissuasion. Je m’abstiendrai de citer certaines nationalités, mais vous seriez surpris de constater que le faible nombre de refus aujourd’hui opposés (2 %) recouvre, comme par hasard, ces nationalités.

Vous pourriez vous interroger sur la pertinence d’un tel système pour un nombre aussi restreint de cas. La réponse tient précisément à son caractère dissuasif. Il convient également de préciser que ce dispositif ne concerne pas l’ensemble des chercheurs, et qu’il n’a pas vocation à entraver la coopération scientifique internationale. En revanche, il cible des

profils très spécifiques, notamment des chercheurs expérimentés, disposant de compétences pointues et de réseaux étendus, dont le départ pourrait entraîner une perte significative.

Enfin, je souhaite aborder brièvement le cas Sermat concernant certaines exportations sensibles. Lorsque des informations préoccupantes nous sont parvenues, des mesures conservatoires ont été immédiatement prises, notamment la suspension des licences concernées. Dans l'attente des conclusions de l'enquête de la direction générale des douanes et droits indirects (DGDDI), toutes les garanties ont été mises en place pour empêcher Sermat d'exporter du matériel, comme vous le savez déjà.

M. Jean-Louis Thiériot (DR). Je souhaiterais obtenir votre analyse sur la nature de l'hybridité telle que nous la connaissons aujourd'hui. Selon vous, s'agit-il surtout d'une différence de nature ou simplement d'une différence de degrés ? Nous faisons face à une forme d'« *indirect approach* » chère à Liddell Hart qui s'inscrit dans l'histoire du renseignement. En effet, la PPST constitue un enjeu de longue date, comme l'illustre l'affaire Farewell notamment. La guerre informationnelle s'est illustrée récemment par le cas de Jean Clémentin, plume du *Canard Enchaîné*, recruté par le StB, service de renseignement tchécoslovaque. Ces réalités existaient déjà, il y a fort longtemps. En résumé, considérez-vous que l'hybridité, notamment à cause du cyber, prend une nouvelle dimension ?

Ensuite, nous avons déjà évoqué des tentatives d'ingérence et des guerres informationnelles des grands acteurs. Que repérez-vous dans nos outre-mer ? Je pense notamment au groupe d'initiative de Bakou, dont on connaît les capacités déstabilisantes.

Enfin, vous avez cité les « treize champs » de l'hybridité. Pouvez-vous me rappeler dans quel document ces champs sont évoqués ? S'agit-il de la RNS ?

Mme Agnès Romatet-Espagne. Ces treize champs ont été définis par le centre d'excellence européen établi pour la lutte contre les menaces hybrides, établi à Helsinki depuis 2017 et la Commission européenne[1]. Les Finlandais, particulièrement exposés à la menace russe et ayant pris très tôt la mesure de l'expression de cette agressivité dans le champ de l'hybridité, ont développé ce centre européen, qui constitue aujourd'hui une référence, et travaille notamment avec l'Otan. Ce centre d'excellence a été l'un des premiers à structurer l'analyse des stratégies hybrides, notamment en définissant les treize champs que nous utilisons aujourd'hui. Cette production est publique et accessible sur son site internet.

Je reviens maintenant à votre première question, que je trouve particulièrement stimulante, à laquelle je vais répondre en réfléchissant à voix haute devant vous. Vous soulignez à juste titre que la numérisation de nos sociétés permet d'amplifier des attaques notamment dans le domaine cyber ou dans la manipulation de l'information. À cela s'ajoute un facteur déterminant : la mondialisation et nos interdépendances, en particulier économiques, créent des vulnérabilités nouvelles. Par exemple, une action initiée dans un domaine spécifique, tel que l'arsenalisation du droit, engendre des effets bien plus importants qu'on n'aurait pu imaginer il y a plusieurs décennies. Nos sociétés ont effectivement rehaussé la capacité de nuisance de ces modes d'action très classiques.

La question qui se pose alors est de savoir si nous faisons face à davantage d'actions hybrides ou à leur intensification. Pour ma part, je ne crains pas tant la

---

[1] ***The landscape of Hybrid Threats: A conceptual model***, *2021*

multiplication d'actions de faible intensité, même si leur accumulation peut représenter un coût significatif en termes de temps, d'énergie et de perturbations pour l'État. En revanche, je redoute davantage la capacité de certains acteurs à identifier finement nos vulnérabilités et à concentrer leurs efforts sur un point critique, en ciblant une efficacité maximale. Une action précise, puissante, déclenchée au bon moment et au bon endroit, est susceptible de produire un « effet domino ». Nous avons en tête certains scénarios récents, notamment en Pologne, où des systèmes critiques ont été proches de subir des interruptions majeures, des *black-out* sur les réseaux électriques.

Dans le même esprit, nous avons nous-mêmes conduit des exercices de simulation portant sur des scénarios de rupture, par exemple des *black-out* dans le domaine spatial, avant les Jeux olympiques. Nous avons l'intention de renouveler ces exercices.

M. le capitaine de vaisseau Yann Briand, sous-directeur des affaires internationales, stratégiques et technologiques, SGDSN. Pour compléter ce point, je souhaiterais apporter un éclairage d'ordre plus analytique, en m'appuyant notamment sur des travaux académiques de Dimitri Minic, chercheur à l'Institut français des relations internationales (IFRI). Dans sa thèse, publiée, consacrée à la dissuasion russe, il met en évidence une conception sensiblement différente de celle que nous connaissons en France. Cette dissuasion russe est marquée par un *continuum*, qui commence par le dépôt de têtes de cochons devant une mosquée et se finit par les missiles balistiques. Or la Russie semble gravir régulièrement ces échelons pour cibler nos démocraties qui soutiennent l'Ukraine. C'est une stratégie de long terme, extrêmement dangereuse, très pensée, qui a probablement été échafaudée il y a vingt ans.

De fait, le niveau de violence et le nombre d'attaques continueront jusqu'au seuil du conflit armé. En outre, l'estimation de ce seuil n'est probablement pas la même à Bruxelles, à Paris et à Moscou. Ceci rend la situation actuelle extrêmement périlleuse, dans la mesure où nous nous en rapprochons dangereusement.

Mme Agnès Romatet-Espagne. S'agissant des outre-mer, pour le dire crûment, nos compétiteurs, la Russie en particulier, procèdent à une exploitation extrêmement opportuniste de courants politiques locaux, certains favorables à une plus grande d'autonomie, d'autres instrumentalisant des thématiques socio-économiques récurrentes. La Nouvelle-Calédonie a été l'objet de ces actions. De plus, dans la sous-région mélanésienne, certaines stratégies visent également la Nouvelle-Calédonie, pour des raisons de nature économique.

Comme je l'ai déjà mentionné, les failles, les fragilités, les points névralgiques peuvent devenir les cibles idéales pour nos concurrents, qui savent très bien attiser les braises.

M. le président Jean-Michel Jacques. Aujourd'hui, il est question de Russie, mais lorsque Daesh était réellement plus puissant, il pratiquait les mêmes méthodes contre notre Nation.

Mme Catherine Hervieu (EcoS). Le contexte international est marqué par l'intensification des stratégies de guerre hybride : cyberattaques, influence informationnelle, pressions économiques, opérations clandestines. Les acteurs cherchent à affaiblir nos démocraties sans franchir le seuil d'un conflit armé ouvert.

Notre groupe considère que la guerre hybride n’est plus une menace périphérique, mais un mode durable et structurant des rapports de puissances contemporains. Ces menaces ont toujours existé, mais elles atteignent un nouveau seuil. Nous pensons évidemment aux pays baltes et plus particulièrement à l’Estonie, autour de Narva.

Cela illustre la manière dont des campagnes informationnelles peuvent exploiter des vulnérabilités sociétales et identitaires afin de fragiliser la cohésion nationale. Ces stratégies existent également dans notre pays à travers des influences politiques, économiques, financières ou médiatiques, qui cherchent à instrumentaliser les émotions et les inquiétudes de nos compatriotes, au détriment des intérêts de la France. Tout s’est accéléré depuis 2022, comme vous l’avez indiqué, à partir des données factuelles. Ce changement se poursuit-il de manière encore plus prononcée ?

Ensuite, les attaques cyber et ingérences nombreuses sont certes plus médiatisées, mais elles ont une plus grande influence sur les populations, alors que l’éducation aux médias demeure très faible en France. Nous considérons que le manque de moyens alloués aux services compétents est gravissime et qu’il est urgent d’agir.

La France et l’Union européenne disposent-elles aujourd’hui de doctrines, de capacités de résilience et de mécanismes de coordination suffisamment adaptés pour répondre durablement à ces stratégies de déstabilisation, sans porter atteinte aux principes démocratiques et à l’État de droit ? Enfin, quelles coopérations européennes et internationales vous paraissent-elles prioritaires pour renforcer la résilience démocratique, technologique et informationnelle de notre pays face à ces nouvelles formes de confrontations stratégiques ?

Mme Agnès Romatet-Espagne. Madame la députée, toute la difficulté réside, en réalité, dans notre capacité à mesurer la menace, tant à l’échelle nationale qu’à l’échelle européenne. En premier lieu, l’attribution formelle des actions hybrides demeure particulièrement complexe. Nous faisons, à cet égard, preuve d’une grande prudence dans nos prises de parole publiques. D’autres États européens, tels que la Pologne, la Finlande ou encore les pays baltes, adoptent une approche plus audacieuse, s’appuyant sur des faisceaux d’indices pour estimer qu’une attaque est attribuable à tel ou tel compétiteur. Pour notre part, nous sommes plus prudents prudence repose sur une exigence de rigueur. Néanmoins, il nous faudra probablement faire évoluer notre doctrine.

Le niveau d’inquiétude de nos partenaires européens ne cesse de croître. Les États que vous avez cités, notamment les pays baltes, mais aussi l’Allemagne et la Pologne, font état d’une tension de plus en plus forte. Cette évolution traduit à la fois une meilleure compréhension des stratégies hybrides et une prise de conscience accrue de leur nocivité.

Elle s’explique également par la visibilité croissante de certaines actions, qui ont marqué l’opinion publique. Les survols de drones, en particulier, ont joué un rôle d’accélérateur dans cette prise de conscience, en révélant concrètement la nature des menaces et en suscitant une inquiétude à laquelle les responsables politiques ont dû répondre. De fait, la menace est aujourd’hui de plus en plus prégnante.

Vous posez enfin une question fondamentale, celle de notre capacité, en tant que sociétés démocratiques, à faire face à ces défis. Il faut rappeler que toutes nos actions s’inscrivent dans un cadre juridique strict, ce qui constitue à la fois une force et une contrainte. Nous ne lançons pas des attaques cyber, ni des survols de drones autour du

territoire russe, nous ne manipulons pas nous-mêmes des informations. Nous ne recourons ni à des actions offensives clandestines, ni à des manipulations d'information.

Cela ne signifie pas pour autant que nous sommes démunis. Nous disposons d'outils que nous pouvons renforcer et mieux mobiliser. Il s'agit notamment de capacités de détection, d'attribution et de signalement. L'exemple des actions menées sur la flotte fantôme en offre une illustration.

M. le président Jean-Michel Jacques. Pour mémoire, les treize menaces hybrides que vous avez mentionnées sont les suivantes : la désinformation et manipulation informationnelle, les cyberattaques sur les structures, l'influence politique clandestine, le champ du politique, l'ingérence électorale, l'instrumentalisation de l'énergie, le sabotage des infrastructures critiques, les pressions diplomatiques, l'instrumentalisation du droit, l'espionnage et les opérations clandestines, l'utilisation des groupes proxys, l'instrumentalisation des migrations et enfin, les menaces et démonstrations de force militaires.

Mme Agnès Romatet-Espagne. Vous avez relevé l'influence de nature politique. Or la loi n° 2024-850 du 25 juillet 2024 que le Parlement a voté nous fournit justement des moyens, dans le cadre de l'État de droit et nous permet de mieux prévenir les ingérences étrangères, à travers des mesures de transparence, grâce à la création du registre des activités d'influences étrangères.

Mme Sabine Thillaye (Dem). Madame la directrice, vous avez évoqué la nécessité d'une prise de conscience et avez posé la question suivante : sommes-nous assez conscients ? De fait, les directives européennes NIS 2 et REC et le règlement sur la résilience opérationnelle numérique du secteur financier (Dora), n'ont toujours pas été transposés dans le cadre français, bien qu'une échéance au deuxième semestre 2024 était attendue. Leur transposition est désormais annoncée pour le mois de juillet 2026, ce qui ne témoigne pas d'une extrême diligence, à l'heure où nous sommes confrontés à des menaces aussi actuelles que précises, notamment sur nos infrastructures critiques.

Quel changement envisagez-vous concernant la guerre hybride ? Qu'anticipez-vous à l'horizon 2030, compte tenu notamment de l'évolution de l'intelligence artificielle ? Aussi, comment faire en sorte que les prescriptions de la RNS parviennent également jusqu'à nos concitoyens, sur le terrain ?

Mme Agnès Romatet-Espagne. Sommes-nous suffisamment conscients ? Je soulignais les nécessaires efforts de pédagogie. Pour sa part, Viginum porte la création d'une académie de lutte contre les manipulations de l'information. La sensibilisation doit intervenir dès le plus jeune âge. Mme Hervieu mentionnait précédemment l'enjeu de l'éducation aux médias. Il s'agit effectivement d'une évidence, mais Viginum y œuvre, en travaillant avec l'éducation nationale.

Mme Catherine Hervieu (EcoS). L'éducation aux médias ne peut pas être balayée d'un revers de main. Cela doit effectivement intervenir dès le plus jeune âge, mais nous ne pouvons que nous inquiéter, à la lumière des moyens dédiés à l'éducation nationale. Or la cohésion nationale et sociale repose aussi sur ces fondements. Je tenais à formuler ce commentaire de manière solennelle.

Mme Agnès Romatet-Espagne. Je ne minimise en aucun cas l'importance de ces enjeux. Je m'exprime ici aussi en tant que grand-mère, pleinement consciente de ce qui se joue dans l'éducation de nos enfants et de nos petits-enfants. Je pense notamment à la capacité à discerner, à distinguer le vrai du faux, et à raisonner. Cette capacité de discernement n'est pas seulement un objectif éducatif, elle est au cœur de notre résilience collective.

Tel est précisément le sens du deuxième objectif stratégique de notre RNS, consacré à une France unie et résiliente. Il prévoit l'acculturation de 10 millions de jeunes, âgés de 13 à 25 ans, aux enjeux de défense et de sécurité nationale, et notamment aux stratégies hybrides et informationnelles d'ici 2030. Ce chiffre peut sembler ambitieux, mais il constitue un premier jalon indispensable. Des initiatives concrètes sont déjà engagées, notamment à travers la diffusion de supports pédagogiques comme le guide « Tous responsables », qui vise à sensibiliser chacun aux risques et aux réflexes de bon sens à adopter.

Au-delà de la transmission des connaissances, il s'agit de favoriser une appropriation individuelle de ces enjeux. Plus nous nommons les phénomènes, plus nous expliquons les mécanismes, plus nous faisons confiance à l'intelligence de nos concitoyens, plus ils se sentiront responsables de leur sécurité et de celle de leurs proches.

S'agissant maintenant de la trajectoire des menaces à l'horizon 2030, les éléments que nous pouvons anticiper convergent vers une intensification de la pression. Celle-ci ne se traduira pas nécessairement par la prédominance d'un champ d'action particulier. Au contraire, tous les champs de l'hybridité pourront être mobilisés de manière combinée. L'enjeu pour nos adversaires est clair : détecter nos failles, identifier nos points névralgiques et intervenir là où l'impact sera maximal.

Je crains, à cet égard, une évolution dans les modes opératoires. Certains acteurs, en particulier la Russie, pourraient chercher à améliorer la qualité de leurs actions en s'appuyant sur des *proxys* plus efficaces, plus discrets, mieux intégrés, et donc plus difficiles à détecter. Cette capacité d'adaptation constitue un facteur d'inquiétude.

Plus encore, le risque réside dans la combinaison simultanée de plusieurs actions, conduites dans différents champs, mais convergeant vers un objectif commun. Ces actions pourraient se renforcer mutuellement, brouiller les lignes et compliquer notre capacité de réponse. Dans une hypothèse extrême, plusieurs acteurs distincts pourraient agir de manière concomitante. Une telle configuration, sans pouvoir être affirmée aujourd'hui, ne peut être exclue.

M. le capitaine de vaisseau Yann Briand. Il y a quelque temps, je suis allé présenter la RNS devant des *think tank* suédois, me réjouissant d'évoquer avec eux l'horizon 2030. Ces derniers m'ont interrogé sur le choix d'une échéance si lointaine, dans la mesure où nous pourrions être pris de court dès le lendemain. De fait, il est parfaitement exact que l'accélération du contexte géopolitique, les prises de position de certains de nos partenaires et la fragilisation du lien transatlantique ouvrent une « fenêtre d'opportunité » pour des actions qui ne seraient pas forcément des actions militaires massives, mais suffisantes pour déstabiliser l'article 5 du traité de l'Atlantique nord, pour essayer d'attaquer la solidarité des Européens.

En résumé, l'objectif 2030 demeure tout à fait pertinent. Simultanément, il faut être très vigilant dès à présent, face aux menaces de déstabilisation de l'Otan et de l'UE. Une Russie plus fragilisée sur le front ukrainien et le plan intérieur pourrait être tentée de mener des menaces de plus en plus prononcées dans le champ de l'hybridité, employant pour cela toute l'étendue de la grammaire stratégique à sa disposition.

M. le président Jean-Michel Jacques. Je vous remercie pour vos propos et je veux, à mon tour, souligner combien ces auditions publiques sont essentielles. Elles permettent, au-delà de nos échanges institutionnels, de rendre visibles des sujets. Or, il est important que nos concitoyens comprennent ce que nous faisons, pourquoi nous le faisons et avec quels moyens.

Vous avez raison de rappeler que ces travaux participent à une forme de pédagogie collective. À ce titre, je vous remercie d'avoir accepté que cette audition soit publique, quand parfois nos interlocuteurs se réfugient derrière le cadre du huis clos, qui peut aussi être appliqué non pas pour l'intégralité de l'audition mais seulement pour quelques questions spécifiques, en fin d'audition. Notre pays a besoin de comprendre et nos compétiteurs doivent entendre que nous nous organisons et que nous les voyons.

Mme Agnès Romatet-Espagne. Il me paraît également utile de rappeler que le sujet des stratégies hybrides est également pleinement intégré dans les travaux de l'Otan. Cette prise en compte remonte à un moment charnière, l'année 2014, marquée par l'invasion du Donbass et l'annexion de la Crimée. Dès l'année suivante, en 2015, les alliés ont adopté une première stratégie visant à définir le rôle de l'Otan dans la lutte contre les pratiques de guerre hybride. L'objectif était clairement énoncé : « *faire en sorte que l'Alliance et les alliés soient suffisamment préparés à contrer les attaques hybrides quelles qu'elles soient et exercer une dissuasion propre à prévenir toute attaque de ce type contre l'Alliance et, si nécessaire, défendre les alliés concernés* », étant entendu que l'Otan reconnaît pleinement la primauté de la compétence nationale sur ces sujets.

Une nouvelle stratégie révisée – et classifié – a été adoptée par les ministres de la défense en juin 2025. Néanmoins, le véritable tournant remonte au sommet de Varsovie de 2016, lorsque les alliés ont affirmé publiquement qu'une attaque hybride contre un ou plusieurs alliés pourrait être un des motifs d'invocation de l'article 5 du traité de Washington. Cette orientation a été confirmée à plusieurs reprises.

Lors du sommet de Bruxelles de 2018, l'Otan a créé des équipes dédiées, les *Counter Hybrid Support Teams*. Ces équipes peuvent être déployées à la demande d'un État membre afin de l'assister face à une campagne hybride. Elles ont déjà été activées, notamment au Monténégro en amont des élections de 2019, puis en Lituanie en 2022, face à une instrumentalisation des flux migratoires par la Biélorussie.

Lors de son audition devant vous, Xavier Brunetière vous a présenté le plan de défense et de sécurité nationale (PDSN). L'un des enjeux consiste pour nous à pouvoir le nourrir à partir de nos mesures, nos évaluations. Ensuite, la décision relève la fois de nos politiques, mais aussi de nos alliés, dans un cadre qui n'est plus le mien.

M. le président Jean-Michel Jacques. Nous passons à présent aux questions des députés à titre individuel.

M. Thomas Gassilloud (EPR). Madame la directrice, j'aimerais connaître votre regard sur notre architecture interministérielle de défense. Quelles relations entretenez-vous avec les ministères régaliens, comme le ministère des armées, le ministère de l'Europe et des affaires étrangères, le ministère de l'intérieur ou la direction générale de l'armement ? Comment évaluez-vous ce modèle ? Quelle est la plus-value spécifique de votre direction ?

Ensuite, nous assistons à l'effondrement du cadre multilatéral post-guerre froide. Je pense notamment au traité Ciel ouvert, au traité sur les forces nucléaires à portée intermédiaire. Quelle est votre vision concernant la reconstruction de ce cadre multilatéral pour assurer la paix et la sécurité en Europe ?

J'ai très grande confiance dans la manière dont les démocraties font usage de leur force et estime qu'elles doivent être transparentes à ce sujet. Travaillons-nous à des scénarios d'après-crise ? Il faut bien entendu utiliser la force, être en mesure de résister et de faire mal. Mais il faut aussi proposer, y compris aux adversaires que l'on désigne, des chemins de sortie. Comment évaluez-vous notre capacité collective à proposer également ces chemins de sortie à nos adversaires ?

Mme Natalia Pouzyreff (EPR). Madame la directrice, l'année dernière, en compagnie de ma collègue Marie Récalde, nous avons remis un rapport sur la lutte contre la manipulation de l'information et sur la fonction influence. À cette occasion, nous avions travaillé avec le SGDSN et les différents ministères. Ma question rejoint en quelque sorte celle de Thomas Gassilloud. Qu'en est-il de l'opérationnalisation ? Je pense à l'opérationnalisation de la stratégie de lutte contre les manipulations d'information ; à son volet académique, comme en témoigne le projet d'Académie de Viginum, à destination des jeunes publics ; mais aussi à l'opérationnalisation juridique aussi. En tant que législateurs, il nous semble intéressant d'en savoir plus.

Mme Agnès Romatet-Espagne. Je ne voudrais pas m'élever au-delà de mes attributions propres, et je souhaite, d'emblée, faire preuve d'une certaine humilité dans mes réponses.

S'agissant de l'architecture interministérielle de défense, et pour répondre de manière concrète à votre interrogation, je vais vous exposer de façon simple à quoi sert la direction des affaires internationales, stratégiques et technologiques (AIST). Nous intervenons, pour l'essentiel, en amont de la menace, là où la direction Protection et sécurité de l'État (PSE) est davantage mobilisée dans la phase aval. Notre mission centrale repose sur l'anticipation. Elle se traduit notamment par l'animation d'un comité interministériel dédié à l'hybridité, qui permet de fédérer les expertises des différents ministères autour des études prospectives qui nous sont demandées, définies conjointement par les directeurs de cabinet. Ces travaux débouchent tous sur des recommandations opérationnelles.

À titre d'exemple, nous collaborons à une étude en cours sur la géo-ingénierie solaire, c'est-à-dire la capacité, non pas à modifier la météo, mais à changer le climat. On mesure aisément les implications potentielles, tant les effets sur certains territoires pourraient être majeurs. J'attends avec impatience les conclusions de l'étude.

Par ailleurs, notre direction contribue à la préparation de certains conseils de défense et de sécurité nationale et anime des dialogues stratégiques dans de nombreux domaines. Elle constitue également un point nodal en matière d'exportation de matériels de

guerre, puisque nous présidons la commission interministérielle pour l'étude des exportations de matériels de guerre (Cieemg), mais également la commission interministérielle des biens à double usage (Cibdu). Nous présidons par ailleurs le comité de liaison de sécurité économique, du groupe de travail sur le *lawfare*.

Nous travaillons plus particulièrement à la prévention de certaines menaces. Tout sujet pouvant nous conduire à mieux lutter contre les risques de prolifération d'armes de destruction massive est traité, à un moment donné, par le SGDSN.

Nous menons l'expertise technique dans les quatre régimes de contrôle sur les armes de destruction massive : le régime de contrôle de la technologie des missiles (RCTM) sur les technologies missilières, le groupe des fournisseurs nucléaire (NSG) sur le nucléaire, le groupe Australie sur les armes biologiques et bactériologiques et l'Arrangement de Wassenaar.

J'insiste sur ces éléments à dessein. On pourrait imaginer que demain, une zoonose soit utilisée pour déstabiliser complètement l'économie d'un pays. Vous pouvez imaginer quels seraient les effets sur notre territoire d'une épidémie qui affecterait très gravement notre économie, mais également le tissu social.

Enfin, ma direction est en appui à la préparation des conseils de politique nucléaire et mène un rôle dans le domaine spatial. Nous avons ainsi coordonné la rédaction de la stratégie spatiale, mais plus techniquement, nous sommes chargés de nous assurer de la sécurité des liaisons spatiales.

M. le capitaine de vaisseau Yann Briand. La force du SGDSN, pensée par des personnes qui avaient connu la guerre et qui ont conçu la V^e^ République avec des outils capables de gérer les crises, consiste à pouvoir rassembler autour de la table, avec la légitimité d'un service du premier ministre, l'ensemble des ministères et de les forcer à trouver une solution la plus intelligente possible.

Chez les Britanniques, le leadership est plutôt assuré par le Foreign, Commonwealth & Development Office (FCDO), avec un certain succès. En Allemagne, le ministère fédéral de l'intérieur (BMI) semble prendre effectivement une forme de prééminence, qui reste à vérifier sur le long terme. En Italie, le ministère de la défense a lancé une initiative sur l'hybridité, mais sera-t-il légitime, dans la durée ?

Lorsque nous discutons avec nos partenaires étrangers et européens, ils valorisent tous le rôle et la place du SGDSN, en tant qu'organisation légitime pour faire travailler le plus grand nombre.

Mme Agnès Romatet-Espagne. La force du SGDSN repose précisément sur une expertise de très haut niveau, concentrée, mais dont la qualité confère une légitimité reconnue aux analyses et aux avis que nous produisons. Cette crédibilité tient également à sa position singulière : nous ne sommes pas perçus comme un acteur défendant l'intérêt d'un ministère en particulier, mais bien comme un arbitre cherchant à éclairer la décision publique de la manière la plus objective possible.

C’est précisément cette neutralité qui permet de créer un cadre de travail spécifique. Les ministères que vous avez mentionnés, monsieur le député Gassilloud, viennent à nos réunions dans une disposition intellectuelle tournée vers la construction collective. Nous sommes en quelque sorte une « fabrique de consensus ».

M. Thomas Gassilloud (EPR). Pour en revenir à ma première question, je suis un grand partisan de la défense globale des années 1960, du caractère l’interministériel des questions de défense. Je pense à ce titre qu’il faut aller plus loin, aujourd’hui. C’est la raison pour laquelle je vous demandais de repréciser votre place dans l’architecture globale, notamment sur les questions de relations internationales.

Mme Agnès Romatet-Espagne. Sur la question du scénario de l’après-crise, je souhaite d’abord faire preuve de clarté et de modestie. Ce sujet est évidemment travaillé de longue date par les administrations compétentes, et je ne doute pas qu’il existe, notamment au ministère des affaires étrangères comme au ministère des armées, de très nombreux scénarios détaillés consacrés au « jour d’après ».

Pour autant, je dois vous indiquer que, pour ce qui concerne ma direction, le sentiment d’urgence nous porte plutôt vers le court et le moyen terme. Nos travaux d’anticipation se situent aujourd’hui sur des horizons de dix-huit à vingt-quatre mois, tandis que la RNS fixe des perspectives à l’horizon 2030. Notre mandat consiste d’abord à être prêts pour faire face à la crise elle-même. Cela étant dit, des travaux existent déjà, notamment sur la reconstruction de l’Ukraine. Une représentante spéciale du président de la République, rattachée à la direction générale du Trésor est d’ailleurs mobilisée sur ce sujet.

Madame Pouzyreff, le souci de l’opérationnalisation figure au cœur des priorités du secrétaire général. Nous ne sommes pas dans la contemplation : notre rôle consiste à analyser, produire des recommandations et surtout à veiller à leur mise en œuvre effective. Les études d’anticipation que nous conduisons débouchent sur des recommandations concrètes, et celles-ci font l’objet d’un suivi rigoureux.

Dès leur validation, nous réunissons immédiatement l’ensemble des ministères concernés, nous désignons des chefs de file et nous fixons des échéances précises. Nous assurons un suivi extrêmement attentif pour vérifier que les engagements pris sont bien tenus. Cette logique d’exécution est une priorité absolue.

Il existe déjà un cadre stratégique très fourni, avec la revue nationale stratégique et les différentes stratégies produites depuis 2024. L’enjeu n’est plus d’accumuler des documents, mais d’appliquer les décisions que nous avons prises. Cette exigence d’opérationnalisation est portée avec une très grande détermination par Nicolas Roche, notre secrétaire général.

M. le président Jean-Michel Jacques. Dans le même ordre d’idées, la RNS formule des objectifs clairement définis. J’ajoute que le travail et le volontarisme du secrétaire général et de toute son équipe sont soutenus aussi par la représentation nationale, qui veillera à ce que la politique publique soit convenablement déployée.

La séance est levée à douze heures vingt-huit.

*

* *

Membres présents ou excusés

Présents. - M. Édouard Bénard, Mme Anne-Laure Blin, M. Yannick Chenevard, Mme Caroline Colombier, M. Michel Criaud, M. Thomas Gassilloud, M. José Gonzalez, Mme Catherine Hervieu, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Thibaut Monnier, Mme Natalia Pouzyreff, Mme Marie Récalde, M. Arnaud Saint-Martin, M. Jean-Louis Thiériot, Mme Sabine Thillaye, M. Romain Tonussi, Mme Corinne Vignon

Excusés. - Mme Delphine Batho, M. Frédéric Boccaletti, Mme Cyrielle Chatelain, M. Yannick Favennec-Bécot, M. Moerani Frébault, M. Perceval Gaillard, M. Damien Girard, M. Bastien Lachaud, Mme Nadine Lechon, Mme Lise Magnier, Mme Alexandra Martin (Alpes-Maritimes), Mme Mereana Reid Arbelot, Mme Catherine Rimbert, Mme Marie-Pierre Rixain, M. Sébastien Saint-Pasteur, Mme Isabelle Santiago, M. Mikaele Seo, M. Boris Vallaud, M. Laurent Wauquiez