ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
20 mai 2026
Séance de 9 heures

Compte rendu n° 68

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de M. Loïc Kervran,
Vice-Président

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

M. Loïc Kervran, président. Mes chers collègues, avant de commencer cette audition, je vous prie de bien vouloir excuser l'absence du président Jean-Michel Jacques. En effet, celui-ci intervient ce matin devant un panel de haut niveau à l'Institut Choiseul sur les enjeux de défense. En conséquence, j'ai l'honneur de présider les deux auditions de cette matinée.

Je voudrais également me féliciter de l'adoption hier en première lecture de l'actualisation de la loi de programmation militaire (LPM). Ce texte permettra d'accélérer notre effort de défense, grâce à 36 milliards d'euros supplémentaires pour nos armées. Pour votre complète information, il est prévu que ce texte soit examiné en séance publique au Sénat à compter du 2 juin.

Je reviens à présent à l'audition de ce matin. Nous poursuivons notre cycle consacré à la guerre hybride en recevant deux acteurs centraux pour la souveraineté de l'État : M. Xavier Brunetière, directeur de la protection et de la sécurité de l'État au Secrétariat général de la défense et de la sécurité nationale (SGDSN) et du général de division aérienne Nicolas Leverrier, directeur de la protection des installations, moyens et activités de la défense (DPID) au ministère des armées et des anciens combattants.

La direction de la protection et de la sécurité de l'État coordonne les travaux d'anticipation des crises, anime les politiques interministérielles de prévention des risques. Monsieur le préfet, nous aimerions donc savoir quelles sont vos priorités pour améliorer la résilience de la nation face aux menaces hybrides, notamment à la lumière du retour d'expérience (RETEX) du dernier exercice Orion. De son côté, la DPID est chargée d'assurer la sécurité des emprises de la défense. Elle met en œuvre le dispositif de sécurité des activités d'importance vitale pour le ministère des armées.

En tant que député du Cher, je souligne que ce département a connu récemment deux actions antimilitaristes de nature différente. La première concerne une attaque sur des transformateurs électriques, qui visait clairement l'industrie de défense. La seconde concernait l'invasion du champ de tir et d'essai de la direction générale de l'armement (DGA) par un « Teknival », dont la dimension antimilitariste était assumée par ses organisateurs. Ce type d'évènements nous interroge sur un certain nombre de signaux faibles et sur nos vulnérabilités.

Mon général, vous pourrez aussi revenir sur l'intensification des menaces physiques et numériques auxquelles sont confrontés les sites de la défense. En tant que responsable du service du haut fonctionnaire correspondant de défense et de sécurité du ministère des armées, vous aurez sans doute à cœur de nous expliquer la mission particulière, l'organisation de ce service au sein du ministère, ainsi que les interactions de votre direction avec les hauts fonctionnaires correspondants de défense des autres ministères. À ce titre, plusieurs articles du projet d'actualisation de la LPM renforcent la résilience et la capacité de réponse aux attaques hybrides.

Vous pourrez aussi détailler dans vos champs respectifs les avancées permises par le projet d'actualisation de la LPM. Sans plus tarder, je vous cède la parole.

M. Xavier Brunetière, directeur de la protection et de la sécurité de l'État au secrétariat général de la défense et de la sécurité nationale. Dans le cadre du travail de votre commission sur les menaces hybrides et le *continuum* de sécurité, je tiens à vous présenter les trois principaux volets de la mission de la direction de la protection et de la sécurité de l'État : la planification ; les exercices, et en particulier la coopération civilo-militaire dans le cadre de l'exercice Orion de 2026 ; et enfin les entités critiques, les opérateurs, services et activités d'intérêt vital, une politique publique qui relève de ma direction. Je n'aborderai pas d'autres politiques que nous pouvons porter au sein de cette direction, et qui peuvent présenter des interactions importantes avec les thèmes de menaces hybrides et de *continuum* de conflictualité. Je pense en particulier aux enjeux de protection du secret de défense nationale ou d'innovation technologique en matière de technologie de sécurité.

S'agissant tout d'abord des enjeux de planification, notre feuille de route s'appuie sur la revue nationale stratégique (RNS) actualisée le 14 juillet 2025, et en particulier son scénario central. Ce dernier nous invite à nous préparer à l'horizon 2030 à une guerre majeure de haute intensité en Europe, hors du territoire hexagonal, qui impliquerait la France et ses alliés et verrait notre territoire exposé simultanément à des actions hybrides massives.

Dans ce cadre, nous travaillons sur un nouvel outil de planification, qui vise à répondre à deux ambitions : d'une part, être en mesure de conduire des réponses graduées face à une intensification des attaques hybrides ; et d'autre part de pouvoir accompagner les forces armées françaises et alliées, dans le cadre d'un déploiement et d'un engagement exigés par scénario de guerre majeure de haute intensité.

Ce plan est décrit en particulier au paragraphe 498 et suivants de la RNS. Il est construit de manière assez classique, en incluant des scénarios et une montée en puissance au regard de l'appréciation de la situation, qu'il s'agisse des menaces hybrides ou du déploiement des forces armées. L'analyse des risques, des menaces et des vulnérabilités conduites dans le cadre de cette démarche de planification, vise également à pouvoir construire des niveaux de défense et de sécurité interministérielle, qui sont autant de paliers au regard desquels des propositions d'action et des mesures pourront être proposées, en cohérence avec le plan.

Ces mesures décrivent les actions menées par les différents ministères chefs de file, en particulier les hauts fonctionnaires de défense et de sécurité. Cette planification constitue un élément-clé dans le dialogue entre l'échelon stratégique et l'échelon opérationnel. Elle fait aussi directement écho aux discussions que vous avez eues dans le cadre de l'actualisation de la loi de programmation militaire. Je pense en particulier à l'état d'alerte de sécurité nationale, l'un des éléments pouvant s'adapter à l'une des situations ou des étapes de montée en puissance telles qu'elles sont envisagées dans le cadre de cette planification de défense et de sécurité nationale. Ce dispositif juridique doit permettre d'assurer la montée en puissance du pays, en particulier des services de l'État et des opérateurs ; mais aussi de faciliter la remontée d'informations de la part d'opérateurs de réseaux extrêmement cruciaux, comme les opérateurs télécom ou les opérateurs de réseaux énergétiques.

La démarche de planification est en cours ; elle est également nourrie par l'exercice d'Orion 2026. Cet exercice, qui a mobilisé un très grand nombre de ministères, a été conduit par le SGDSN et par l'état-major des armées, pour sa dimension civilo-militaire. Il avait notamment pour objet de tester certaines liaisons civilo-militaires qui constituent des enjeux majeurs dans le cadre de cette planification de défense et de sécurité nationale, en particulier la dimension de soutien de la nation hôte, d'accompagnement du déploiement des forces armées, mais aussi la réponse à une intensification des menaces hybrides.

Cette séquence civilo-militaire d'Orion a ainsi fourni l'occasion de dialoguer, tester la réactivité et la capacité de mobilisation et de coordination de l'ensemble de la communauté interministérielle. À titre d'exemple, des échanges extrêmement approfondis sont intervenus entre les services de santé des armées (SSA) et la direction générale de la santé (DGS). D'autres sujets aussi ont pu être abordés, par exemple les enjeux concernant les réseaux.

Une part importante des conclusions de l'exercice Orion sont classifiées, mais je peux vous indiquer que cet exercice a fourni l'occasion de conduire un travail spécifique sur les rétroactions liées aux attaques hybrides, qu'il s'agisse de manipulation de l'information d'origine étrangère, d'attaques cyber, de sabotages ou d'usages de drones.

Cette séquence a permis de tirer un certain nombre d'enseignements. Le premier concerne l'implication de la communauté interministérielle, au-delà du seul champ des hauts fonctionnaires de défense et de sécurité. Il est essentiel de disposer d'une organisation interministérielle permanente, notamment pour faire face à ces enjeux de sécurité nationale.

Le deuxième enseignement concerne les enjeux d'articulation entre la mobilisation des réserves au fur et à mesure de l'élévation des menaces et la poursuite d'activités essentielles pour le pays. Cette articulation est essentielle pour la continuité de la vie de la nation, en particulier de la vie économique de la nation. Ce sujet fait ainsi écho à vos échanges, dans le cadre de l'actualisation de la LPM, concernant les réserves et le service de sécurité nationale.

Le troisième volet est relatif à l'enjeu de protection des réseaux dans leur ensemble, et notamment leur résilience, c'est-à-dire la faculté de rétablir rapidement des capacités. Le quatrième enseignement a trait aux interactions extrêmement étroites avec les alliés de l'Otan et les États membres de l'Union européenne (UE).

Cette séquence civilo-militaire d'Orion et les travaux que vous avez menés dans le cadre de la LPM nous permettent d'aller plus loin dans cette démarche de planification et de résilience, de nourrir le dialogue que nous conduisons par exemple sur des textes européens, comme celui sur la mobilité militaire publié par la Commission en novembre dernier.

M. le général de division aérienne Nicolas Leverrier, directeur de la protection des installations, moyens et activités de la défense au ministère des armées et des anciens combattants. Mesdames et messieurs les députés, je vous remercie à mon tour pour votre invitation à intervenir sur ce sujet de la guerre hybride et du *continuum* de conflictualité. Le fait que vous invitiez aujourd'hui conjointement le directeur de la protection et de la sécurité de l'État du SGDSN et le directeur de la protection des installations, moyens et activités de la défense démontre, s'il n'en était besoin, que ces notions ne relèvent plus uniquement du champ doctrinal ou de l'analyse académique. Elles traduisent désormais une

réalité opérationnelle à la fois quotidienne et concrète pour l'ensemble des acteurs qui concourent à la défense et la sécurité de la nation, mais aussi pour la représentation nationale et, certainement, pour bon nombre de nos concitoyens.

La direction de la protection des installations, moyens et activités de la défense est directement et quotidiennement confrontée à cette transformation profonde de notre environnement stratégique. C'est d'ailleurs sa raison d'être depuis l'origine : lors de son audition par cette même commission en novembre 2015, le premier directeur de la DPID nouvellement créée, l'amiral Renaudeau, justifiait sa création par « *un impérieux besoin de disposer d'une structure dédiée à la défense-sécurité face à la complexification et à l'intensification des menaces* » et il citait notamment « la malveillance, les cyberattaques, ou encore les drones »

Devant la nécessité de renforcer la cohérence de la défense sécurité du ministère des armées, la DPID a donc été placée sous l'autorité directe de la ministre des armées, position qui lui confère une responsabilité transversale essentielle : garantir à la ministre des armées et des anciens combattants la cohérence d'ensemble des dispositifs de protection dans ces trois domaines que sont la protection physique, la protection du secret et la cybersécurité.

La DPID est également le service du haut fonctionnaire correspondant de défense et de sécurité, dont je suis l'adjoint, ce qui lui donne effectivement toute la légitimité nécessaire pour interagir en permanence, au niveau interministériel, avec l'ensemble des hauts fonctionnaires de défense et de sécurité et le SGDSN. Le périmètre d'action de la DPID, s'il inclut bien évidemment les installations et activités les plus sensibles, dépasse largement les seules emprises militaires. Son action couvre de nombreux organismes relevant du ministère des armées, qu'il s'agisse des établissements publics placés sous sa tutelle ou de certaines entreprises de la base industrielle et technologique de défense (BITD). À ce titre, j'entretiens naturellement des relations étroites avec la DGA, ainsi qu'avec la direction du renseignement et de la sécurité de défense (DRSD).

Il est important de rappeler ce périmètre, parce qu'il correspond à une évolution fondamentale de la conflictualité contemporaine. Comme l'illustre très clairement la RNS, notre représentation de la conflictualité a évolué. L'environnement stratégique s'est largement complexifié, notamment depuis 2022 et encore très récemment, et les échanges se sont considérablement dématérialisés. Aujourd'hui, les capacités de défense de la nation reposent sur un ensemble d'interdépendances complexes, qui associent aussi bien les acteurs publics que les industriels, les infrastructures physiques que des réseaux numériques, des flux logistiques que des flux de données.

Le périmètre des responsabilités qui me sont confiées au sein du ministère des armées, qu'il s'agisse du périmètre fonctionnel ou du périmètre physique, en fournit une illustration concrète. Ceci est d'autant plus important et pertinent que la guerre hybride s'inscrit dans cette évolution. En effet, une attaque hybride cherche à exploiter les vulnérabilités d'un écosystème. Ainsi, elle cible rarement les installations les plus sensibles, les plus visibles, car ce sont souvent les plus défendues. En revanche, elle vise le maillon faible, qui peut désormais se situer dans une chaîne de sous-traitance chez un prestataire, ou directement dans un système industriel connecté. Le maillon faible peut également être une faille organisationnelle ou humaine.

L'attaque hybride cherche également à combiner et synchroniser des modes d'action, qui sont parfois sophistiqués – par exemple dans le cas d'une attaque cyber –, parfois assez basiques : vols, sabotages, actions d'espionnage ou de repérage ; des modes d'action connus, qu'on pensait dépassés, mais dont l'efficacité peut désormais être dopée par l'hyper connectivité, à la fois physique et numérique, des différents acteurs.

Enfin, l'attaque hybride vise à produire des effets stratégiques tout en restant sous le seuil d'une confrontation militaire ouverte, mais aussi sous le seuil de visibilité, sous le seuil de l'attribution. Dans cette logique, la défense et la sécurité ne peuvent plus être pensées comme la juxtaposition de dispositifs qui seraient cloisonnés et qui relèveraient chacun d'une compétence sectorielle. La défense et la sécurité reposent aujourd'hui sur une approche de plus en plus globale, intégrée, permanente, qui associe protection physique, sécurité numérique et protection du secret, mais plus largement la résilience, la continuité d'activité et la capacité de gestion de crise.

Concrètement, comment nous adaptons-nous à cette nouvelle réalité ? Trois points doivent être mentionnés. En premier lieu, puisque les stratégies hybrides visent moins désormais des cibles isolées que de grands systèmes interconnectés qui structurent le fonctionnement de nos sociétés, notre défense et notre sécurité reposent nécessairement sur une coopération étroite entre les armées, les différents services de l'État, les opérateurs d'importance vitale (OIV), les industriels, les acteurs du numérique, et les collectivités.

C'est pourquoi nous échangeons en permanence, au sein du ministère des armées, avec les établissements publics placés sous notre tutelle et avec les entreprises. En outre, nous échangeons très régulièrement, notamment avec les services du ministère de l'intérieur, et nous veillons à assurer la plus grande continuité entre la protection interne de nos sites et les forces de sécurité intérieure qui agissent sur l'ensemble du territoire. Nous travaillons bien évidemment en liaison étroite avec le SGDSN, dans le cadre des multiples actions dont certaines ont déjà été citées par le préfet.

Ensuite, la notion de résilience revêt, dans ce contexte, une importance particulière. La première stratégie nationale de résilience a été adoptée en 2022 sous l'autorité du premier ministre, puis recentrée en 2025 sur deux priorités et onze actions opérationnelles. Cette évolution démontre également que la résilience ne peut être réduite à une simple capacité de réaction après une crise.

Ainsi, la résilience se caractérise aujourd'hui par une capacité structurelle d'anticipation, d'absorption des chocs, d'adaptation et de continuité. Tel est le sens des travaux que nous menons avec le SGDSN. De plus, nous avons bien évidemment été très largement associés aux travaux portant sur la transposition nationale des directives européennes portant sur la résilience des infrastructures critiques (REC) et le renforcement de la cybersécurité (NIS 2), dans le cadre du projet de loi Résilience.

Enfin, je tiens à insister sur notre aptitude à détecter et analyser les signaux faibles. Dans la logique d'une guerre hybride, toutes les actions visent à rester sous le seuil de la conflictualité, voire de la visibilité. Ainsi, pris isolément, certains événements peuvent sembler mineurs. Mais lorsqu'ils sont corrélés entre eux, ils pourraient révéler des stratégies de déstabilisation beaucoup plus larges. C'est vrai des incidents physiques, c'est encore plus vrai lorsque vous conjuguez ces incidents avec ceux du domaine numérique. Une tentative de

phishing ou des comportements anormaux sur des systèmes informatiques peuvent ainsi constituer les indices précurseurs d'actions plus structurées.

Les attaques cyber ne constituent plus un domaine séparé du reste de la conflictualité. Elles peuvent préparer, accompagner ou prolonger des opérations physiques, informationnelles ou économiques. C'est pourquoi nous travaillons à collecter l'ensemble des incidents qui surviennent sur les emprises, et nous échangeons en permanence avec les services de renseignement dont l'expertise et la connaissance des menaces nous sont absolument essentielles.

Nous en avons besoin pour connaître l'état réel de protection de nos installations, moyens et activités à un instant donné, pour proposer d'éventuelles actions ou émettre des directives adaptées, en nous appuyant souvent sur le réseau des officiers de sécurité, que ce soit dans le domaine physique ou numérique, ou les délégués pour la défense et la sécurité des opérateurs d'importance vitales. Nous en avons besoin plus largement pour organiser les périmètres et les responsabilités de la défense-sécurité ministérielle, pour entretenir et adapter le corpus doctrinal, pour orienter les contrôles, coordonner les inspections et, au-delà, piloter le retour d'expérience des incidents de sécurité et des contrôles. *In fine*, il s'agit de contribuer au développement d'une culture de sécurité partagée au sein de l'ensemble de l'écosystème ministériel.

Enfin, il nous faut anticiper les menaces futures et préparer dès aujourd'hui les moyens dont nous aurons besoin demain. Les progrès de l'intelligence artificielle, l'automatisation croissante des systèmes, la généralisation des objets connectés ou encore les perspectives ouvertes par le calcul quantique constituent autant d'évolutions qui modifieront profondément les équilibres de sécurité dans les années à venir. Ces transformations créeront aussi bien de nouvelles vulnérabilités qu'il nous appartient d'anticiper dès aujourd'hui, que de nouvelles capacités et opportunités dont nous devons accompagner le développement.

Pour conclure, je tiens à insister sur cette notion temporelle de l'anticipation. Ces actions s'inscrivent dans le temps long, mais la guerre hybride est également une guerre dans la durée, une guerre de l'usure qui s'inscrit elle-même dans le temps long. Elle cherche moins le choc frontal que l'érosion progressive des capacités de résistance d'une société. Face à cette forme de conflictualité, la réponse ne peut être uniquement technique ou capacitaire, elle est aussi organisationnelle, culturelle et humaine ; et nous y travaillons au quotidien.

M. Loïc Kervran, président. Je cède la parole aux orateurs de groupe.

Mme Catherine Rimbert (RN). Au nom de notre groupe, je souhaite saluer l'engagement des services que vous représentez face à des menaces qui, aujourd'hui, visent directement la souveraineté de notre pays.

Avec la guerre en Ukraine et le retour de la guerre de haute intensité, le réarmement capacitaire est plus que jamais d'actualité. Cependant, la guerre hybride a pris une importance majeure dans les conflictualités contemporaines. Désinformation, cyberattaques, instrumentalisation des flux migratoires, pressions économiques et contestation informationnelle de notre souveraineté constituent désormais un ensemble de menaces possibles.

Dans ce contexte, je souhaiterais vous interroger sur la vulnérabilité particulière de nos territoires ultramarins. Éloignés de la métropole et ne faisant pas partie de l'Otan, dispersés sur plusieurs espaces stratégiques et parfois faiblement densifiés militairement, ils peuvent constituer des cibles privilégiées d'influence hostile ou de stratégies de contournement de notre souveraineté. Je pense notamment à l'Indopacifique, aux Caraïbes ou à l'océan Indien, où les rivalités de puissance s'intensifient.

Par ailleurs, nous observons un phénomène de plus en plus complexe. Certains de nos alliés sont à la fois dans plusieurs domaines, des partenaires économiques, mais aussi des compétiteurs stratégiques, industriels, technologiques ou d'influence. Cette ambiguïté impose d'appréhender ces éléments avec une prudence et un discernement tout particulier. Dans ce contexte, quels outils spécifiques développez-vous aujourd'hui pour mieux protéger nos outre-mer tout en tenant compte des relations internationales où les coopérations et les compétitions coexistent souvent avec les mêmes acteurs ?

M. Xavier Brunetière. Madame la députée, je peux vous le confirmer : la situation spécifique des outre-mer est pleinement intégrée dans nos dispositifs, notamment dans le cadre des exercices civils et militaires Orion. Lors de la séquence Orion 3, une attention particulière a ainsi été portée à l'intégration d'une dimension à la fois interministérielle et territoriale.

Cette approche territoriale ne concernait pas uniquement l'Hexagone, mais incluait également les territoires ultramarins. Plusieurs exercices ont ainsi été conduits en intégrant ces territoires, parmi lesquels certains présentent des enjeux stratégiques particuliers. Je pense en particulier à la Guyane, dont l'exposition est renforcée par les enjeux liés au secteur spatial.

De manière plus générale, l'ensemble des outre-mer est pris en compte dans l'analyse et la gestion des menaces hybrides. Cette prise en compte mobilise l'ensemble des départements ministériels, au-delà des seuls ministères de l'intérieur et des armées, dans une logique pleinement interministérielle. Elle s'inscrit également dans la planification de défense et de sécurité nationale, qui intègre les enjeux de continuité territoriale, en veillant non seulement à la résilience propre de ces territoires, mais aussi à leurs relations avec leur environnement régional et avec l'Hexagone.

M. le général de division aérienne Nicolas Leverrier. Les installations outre-mer revêtent, bien évidemment, une importance essentielle, et nous leur accordons une attention particulière. À cet égard, toutes les actions relevant de la défense et de la sécurité que nous mettons en œuvre sur le territoire métropolitain s'appliquent également à ces emprises ultramarines.

Concrètement, nous conduisons un ensemble d'actions structurées. Nous organisons notamment des échanges bilatéraux avec chacun des commandements supérieurs présents en outre-mer. À cette occasion, nous procédons à un examen complet des dispositifs existants, en abordant l'ensemble des sujets liés à la défense et à la sécurité, ainsi que les mesures mises en place pour garantir la protection des emprises. Par ailleurs, nous travaillons en étroite coordination avec l'état-major des armées. Les installations situées en outre-mer sont pleinement intégrées dans les cycles de contrôle et d'inspection que nous menons régulièrement, afin de nous assurer de la bonne protection des sites.

Ce travail s'inscrit dans une logique d'homogénéité avec les actions conduites en métropole. Quant aux moyens déployés, ils relèvent davantage de l'état-major des armées, qui contribue à l'appréciation globale de l'équation défense-sécurité de ces installations, lesquelles demeurent au cœur de nos préoccupations.

M. François Cormier-Bouligeon (EPR). Les menaces et les attaques s'intensifient ces derniers temps. Je pense évidemment à la menace drone, puisqu'un certain nombre d'incidents ont été signalés ces derniers mois, autour de l'Île-Longue en décembre 2025, au pôle interarmées de Creil Senlis en novembre 2025, au camp de Mourmelon, sur le site d'Eurenco à Bergerac ou, plus récemment, aux abords de notre porte-avions *Charles-de-Gaulle* lors de son escale à Malmö en février 2026.

Mais ces menaces et attaques ne se limitent pas aux infrastructures militaires. Nous l'avons vécu dans l'agglomération de Bourges il y a quelques semaines, à travers des incendies particuliers autour des infrastructures de la BITD. De fait, en 2024, 500 atteintes contre la BITD et 800 alertes de sécurité économique avaient été recensées, selon les chiffres issus du rapport de notre collègue Christophe Plassard. De plus, 80 % de ces attaques concernent les PME, soit l'échelon qui apparaît comme plus vulnérable dans la chaîne industrielle de défense.

Vous concourez, à travers vos services, à la protection sur les plans militaire, civil et industriel. Mon général, disposons-nous des moyens suffisants pour assurer la sécurité de nos infrastructures militaires ? Je pense notamment à la lutte anti-drone. Au-delà, considérez-vous que l'effort d'acculturation des femmes et des hommes qui concourent aux armées est suffisant ? Existe-t-il des plans de formation spécifiques ?

Monsieur le préfet, pouvez-vous dresser le bilan du plan de sécurité des activités d'importance vitale (SAIV) ?

M. Xavier Brunetière. S'agissant des services et des activités d'intérêt vital, je ne prétendrai pas en dresser un bilan rétrospectif sur une période de vingt ans. En revanche, nous entrons aujourd'hui dans une phase déterminante, une étape de déploiement et de relèvement de nos capacités, impliquant l'ensemble des opérateurs d'intérêt vital, quels que soient les secteurs concernés. Au cœur de cette dynamique se trouve une notion essentielle, largement mise en avant dans les réflexions communautaires, notamment à travers la directive REC, celle de vulnérabilité.

L'un des enjeux majeurs de la mise en œuvre de cette directive, comme de la stratégie de résilience, consiste précisément à diffuser et à systématiser cette approche par les vulnérabilités. Cette évolution est particulièrement significative sur la chaîne de valeur et les différents niveaux de sous-traitance. Le retour d'expérience récent, notamment issu du conflit en Ukraine, démontre de manière très claire que l'intégration de certaines fonctions clés et la prise en compte effective de la sous-traitance par les acteurs essentiels constituent un facteur déterminant de résilience.

Nous nous engageons aujourd'hui dans cette nouvelle phase, à la lumière des orientations européennes, des travaux conduits sur la résilience, ainsi que dans le cadre de l'actualisation de la LPM. Celle-ci nous fournit des outils supplémentaires pour renforcer cette démarche. Parmi ces dispositions figure notamment la possibilité de contraindre les OIV

à constituer des stocks, soit une manière de se prémunir des vulnérabilités liées à la sous-traitance.

Par ailleurs, d'autres outils viennent compléter ce dispositif, en particulier en matière de remontée et de croisement des informations, domaines déjà évoqués par le général Leverrier. Ainsi, les opérateurs sont désormais invités à considérer ces interdépendances, notamment celles liées à la sous-traitance, comme de véritables vulnérabilités à part entière.

M. le général de division aérienne Nicolas Leverrier. Je souhaite revenir sur les deux questions que vous avez posées, concernant la lutte anti-drone et la question de l'acculturation. S'agissant tout d'abord de la lutte anti-drone, la difficulté principale tient à une forme d'asymétrie. En effet, face à des drones parfois très simples, accessibles dans le commerce et dont le coût est relativement faible, de l'ordre de quelques milliers d'euros, il est souvent nécessaire de déployer des moyens de protection significatifs, notamment lorsque l'on doit sécuriser des emprises étendues.

Pour répondre à cette asymétrie, plusieurs axes d'action sont engagés, en matière d'équipements. D'une part, une montée en puissance des capacités de lutte anti-drone est prévue dans le cadre de la LPM, qui prévoit un renforcement capacitaire. D'autre part, un ensemble de travaux est mené pour évaluer l'efficacité des différents systèmes existants. Ils sont conduits au sein des armées, dans les centres experts, en lien avec la DGA, mais également dans un cadre interministériel.

Cette approche prend aussi en compte la continuité avec les forces de sécurité intérieure, notamment lorsque la protection des sites implique une articulation entre sécurité interne et sécurité externe placée sous l'autorité des préfets. Par ailleurs, des évolutions récentes offertes par l'actualisation de la LPM permettent désormais à certaines entreprises, notamment les OIV, de détecter et de neutraliser des drones menaçants. Nous travaillons en permanence sur l'évaluation de l'adéquation entre moyens et menaces.

S'agissant ensuite de la question de l'acculturation, elle revêt une importance essentielle. Des actions régulières sont menées pour passer des messages notamment à travers l'animation d'un réseau d'officiers de sécurité. Des notes de vigilance sont également diffusées pour sensibiliser à des risques spécifiques.

La culture de sécurité et la notion de défense sont de mieux en mieux comprises par nos concitoyens. Mais un enjeu majeur demeure celui de l'hygiène numérique, dans un environnement marqué par la multiplication de systèmes connectés, qu'il s'agisse des téléphones, des montres ou des véhicules. Nous sommes en effet face à des objets qui échangent en permanence des données dont le stockage n'est pas maîtrisé.

M. Christophe Bex (LFI-NFP). La direction de la protection et de la sécurité de l'État assure notamment la coordination des politiques de protection des infrastructures d'importance vitale. En France, près de 300 opérateurs d'importance vitale gèrent environ 1 500 sites stratégiques essentiels au fonctionnement de la nation. Or, la RNS et l'actualisation de la LPM identifient clairement un scénario de conflit de haute intensité à horizon 2030, incluant des attaques hybrides de ces infrastructures sensibles.

Depuis le début de l'année 2025, une trentaine de survols d'OIV par drone ont déjà été recensés. L'article 14 de l'actualisation de la LPM permet aux OIV, publics comme privés, de recourir à des agents de sécurité privés pour assurer des missions de lutte anti-drone. Cette orientation soulève plusieurs interrogations. Sur le plan des principes, la lutte anti-drone relève aujourd'hui d'une compétence essentiellement souveraine, exercée par les armées et les forces de sécurité intérieure. Comment justifier qu'une mission aussi régalienne puisse être déléguée au secteur privé pour la protection d'infrastructures vitales ?

Ensuite, il convient d'évoquer le coût. En effet, cette privatisation est justifiée par un coût excessif de la puissance publique. Pourtant, les OIV, souvent en situation de monopole, répercuteront ces dépenses sur les usagers.

Enfin, il faut mentionner l'efficacité. Le secteur de la sécurité privée connaît un *turnover* important. Comment garantir un niveau de formation, de disponibilité et de fiabilité suffisant ? La formation sera-t-elle assurée par des organismes publics, au risque de mobiliser des compétences souveraines au profit du privé ou par des structures privées agréées ? Quelle est la doctrine du gouvernement concernant cette privatisation progressive de la protection des infrastructures vitales ?

M. Xavier Brunetière. Je me permettrai de rappeler, en premier lieu, que dans le cadre de la politique que nous portons en matière de protection et de sécurité de l'État, la lutte anti-drone s'inscrit dans une approche globale et cohérente. Celle-ci couvre l'ensemble du spectre, depuis les enjeux de détection et de caractérisation jusqu'aux capacités de neutralisation, en intégrant également la nécessité d'un dialogue étroit avec l'autorité judiciaire.

S'agissant plus spécifiquement des opérateurs d'importance vitale, qu'ils soient publics ou privés, il convient de préciser que les capacités qui leur sont ouvertes relèvent d'une logique de protection de leurs propres équipements. Cette faculté, telle qu'elle a été proposée par le gouvernement, s'inscrit dans un cadre de concertation étroite avec les acteurs concernés, en particulier avec les fonctionnaires de défense et de sécurité. Le statut même d'OIV implique en effet une responsabilité particulière, liée à leur rôle critique.

Cette évolution a fait l'objet d'un examen approfondi, notamment par le Conseil d'État, dont l'avis, joint au dossier législatif, souligne le caractère proportionné et encadré de ces nouvelles prérogatives. Enfin, l'extension des capacités anti-drones s'inscrit dans une dynamique plus large, partagée au niveau européen, où plusieurs États membres développent des dispositifs comparables pour faire face à ces nouvelles formes de menaces hybrides.

M. le général de division aérienne Nicolas Leverrier. S'agissant de la délégation de certaines missions de lutte anti-drone aux opérateurs d'importance vitale, y compris privés, il convient de replacer cette évolution dans une perspective plus large. Aujourd'hui, la plupart des organisations, quelles qu'elles soient, externalisent les fonctions qui ne relèvent pas directement de leur cœur de métier. Cette logique vaut également pour la sécurité, qu'elle soit physique ou numérique, et repose sur l'intervention de prestataires spécialisés. Dans ce contexte, l'extension des capacités de protection aux opérateurs privés s'inscrit dans une continuité, en reconnaissant leur responsabilité première quant à la sécurisation de leurs installations.

Cette évolution est également dictée par la nature même de la menace. Une attaque par drone peut se dérouler en quelques minutes. Si l'OIV devait systématiquement faire appel aux forces de sécurité intérieure, le délai d'intervention pourrait s'avérer incompatible avec la temporalité de la menace, notamment sur des emprises étendues.

La question des coûts excède mon périmètre direct. Il appartiendra aux opérateurs d'en apprécier les modalités de répercussion. En revanche, sur la question de la sécurité privée, de sa formation et de sa doctrine, il importe de rappeler que ce secteur est fortement encadré. Le Conseil national des activités privées de sécurité (CNAPS) joue un rôle central à cet égard, en délivrant les agréments et en assurant le contrôle des sociétés. Ainsi, en 2025, le CNAPS a procédé à plus de 1 800 contrôles sur les sociétés privées de sécurité, et est en dialogue permanent avec elles.

M. Guillaume Garot (SOC). Je souhaite vous interroger sur Orion, le premier exercice français à intégrer le spectre complet de la menace hybride jusqu'à la haute intensité. Orion 2026 a eu le mérite d'associer, au-delà des ministères, des collectivités, des hôpitaux et des opérateurs d'infrastructures critiques.

Cette démarche est essentielle. En effet, en cas de crise majeure, l'État ne sera pas le seul acteur sollicité et la résilience du pays reposera sur la mobilisation d'acteurs civils, territoriaux, privés, qui détiennent des moyens essentiels. Je pense aux transports, à l'énergie, aux télécommunications, à la logistique ; c'est-à-dire celles et ceux qui font vivre et avancer un pays.

Cependant, certains retours de cet exercice attestent malgré tout de la persistance de fragilités en matière de logistique, de chaînes santé, de coordination civilo-militaire. Depuis Orion, avons-nous formalisé une doctrine opérationnelle d'association des collectivités et des acteurs privés à la gestion d'une crise majeure ? Ces acteurs savent-ils concrètement comment ils seraient sollicités, selon quelles chaînes de commandement et quelles obligations ?

M. Xavier Brunetière. L'un des principaux enseignements de l'exercice Orion réside dans la nécessité d'aller plus loin dans l'organisation de la montée en puissance, conformément au scénario central défini par la revue nationale stratégique. Cette exigence se traduit par un ensemble d'actions en cours.

Parmi celles-ci, la planification en matière de défense et de sécurité nationale joue un rôle déterminant. Elle permet non seulement de clarifier les responsabilités respectives des acteurs, mais également de définir les modalités d'articulation entre eux, en fonction des différentes étapes. Ce cadre intègre notamment les opérateurs critiques.

Un second enseignement concerne la territorialisation des dispositifs. L'exercice Orion a permis de tester une organisation interministérielle qui s'est traduite concrètement à l'échelle locale, en lien étroit avec les collectivités territoriales. Sur certains territoires et dans certains domaines spécifiques, tels que la logistique ou la santé, des expérimentations ont été conduites. Il s'agit désormais de passer à une phase de généralisation, afin d'étendre ces dispositifs à une échelle plus large.

Par ailleurs, la dimension des exercices elle-même constitue un levier essentiel. Il apparaît nécessaire d'intégrer désormais, de manière systématique, dans les exercices

territoriaux, notamment ceux pilotés par les préfets de zone ou de département, une composante relevant de la sécurité nationale ou des attaques hybrides. Cette intégration doit venir compléter des scénarios souvent centrés sur des événements de sécurité civile.

Orion a démontré la pertinence d'une approche globale et intégrée. L'ensemble des acteurs partage la conviction que cet exercice doit connaître des prolongements, en élargissant les dispositifs et en impliquant un nombre accru de parties prenantes. C'est précisément dans cette dynamique que s'inscrit le plan d'action actuellement déployé.

M. le général de division aérienne Nicolas Leverrier. Je vais compléter les propos du préfet en revenant sur l'exercice Orion et sur les enseignements qu'il a permis de tirer. Il s'agit, en effet, d'un exercice d'une ampleur particulièrement inédite, qui a mobilisé non seulement une dimension militaire, mais également une dimension pleinement interministérielle.

Un premier point mérite d'être souligné : la prise de conscience des hauts fonctionnaires de défense et de sécurité. Chacun, dans le périmètre qui lui est propre, notamment à travers les opérateurs d'importance vitale dont il a la responsabilité, a pu mesurer concrètement les enjeux associés à un scénario de montée en puissance sur le territoire national tel que celui envisagé dans Orion. Cette prise de conscience constitue un acquis déterminant pour la suite.

À partir de ce socle, le travail qui s'ouvre consiste désormais à décliner les enseignements d'Orion dans une logique opérationnelle. Cela passe notamment par un renforcement du dialogue entre les hauts fonctionnaires de défense et de sécurité et les opérateurs d'importance vitale. Deux axes concrets peuvent être identifiés.

Le premier concerne les plans de sécurité opérateurs des OIV. Ces plans définissent les mesures de protection mises en œuvre pour garantir la sécurité des activités essentielles. Il apparaît désormais nécessaire de les reconsidérer à la lumière des scénarios testés lors d'Orion et des retours d'expérience associés.

Le second axe porte sur les plans de continuité d'activité. Ces dispositifs, conçus pour faire face à une variété d'aléas, doivent désormais intégrer plus pleinement les enseignements tirés des situations rencontrées lors de l'exercice, dans une logique opérationnelle

M. Jean-Louis Thiériot (DR). En vous écoutant, nous nous rendons compte de la nécessité de ne pas travailler en silo ; vos propos font écho à la pensée de Marc Bloch.

Monsieur le préfet, le SGDSN contribue à l'établissement des différents stades de défense, de Stadef 1 à Stadef 5. Les Stadefs et leurs contenus sont par nature classifiés, mais nous connaissons également leur utilité. Dans les limites de ce qui peut être dit, pouvez-vous les évoquer plus longuement ?

Mon général, pourriez-vous nous préciser l'articulation entre la DPID et la DRSD, qui partagent un certain nombre d'enjeux communs ? La protection de nos infrastructures touche directement à la défense opérationnelle du territoire (DOT), dans un certain nombre de cas. Quelle est l'articulation entre la protection des infrastructures, la DOT et le commandement du territoire national ?

M. Xavier Brunetière. Je vous remercie pour votre question relative aux niveaux de défense et de sécurité interministériels. Ces niveaux s'inscrivent dans une démarche globale de planification de défense et de sécurité nationale, fondée sur une appréciation fine de la situation. Cette appréciation prend en compte, d'une part, l'intensité et la nature des menaces hybrides ; et, d'autre part, le niveau d'engagement et de déploiement de nos forces armées. Dans ce contexte, il existe un lien évident avec les stades de défense proprement dits, qui relèvent du ministère des armées et demeurent classifiées.

Les travaux en cours visent précisément à articuler ces deux dimensions, afin de définir des niveaux de défense et de sécurité interministériels ayant une portée plus agrégée. Ceux-ci auront vocation à intégrer l'ensemble des paramètres, qu'il s'agisse des menaces hybrides ou du rôle des armées, notamment dans une logique d'appui de la nation.

Ces stades présentent également une dimension interne importante, en lien direct avec les dispositifs de planification nationale. Par analogie avec le dispositif Vigipirate, qui repose sur différentes postures clairement identifiées, les futurs stades de défense et de sécurité peuvent constituer des signaux adressés à l'ensemble des acteurs concernés, afin de leur permettre d'adapter leurs mesures.

En conclusion, ces travaux, encore en cours s'inscrivent pleinement dans les orientations de la revue nationale stratégique.

M. le général de division aérienne Nicolas Leverrier. S'agissant tout d'abord de la relation entre la DPID et la DRSD, il convient d'insister sur leur complémentarité totale. La DPID constitue une entité resserrée, placée directement sous l'autorité de la ministre, dont la mission consiste à garantir en permanence la protection des moyens, des installations et des activités, selon trois axes majeurs : la protection physique, la protection du secret et la sécurité numérique. La DRSD relève du champ du renseignement ; elle exerce une mission de contre-ingérence et dispose d'une expertise spécifique en matière d'analyse des modes d'action adverses, ainsi que d'un ancrage territorial particulièrement développé.

Dans ce cadre, la coopération entre nos deux structures est constante. Nous échangeons régulièrement avec la DRSD, notamment lorsque nous analysons des incidents, afin de rendre compte au cabinet de la ministre de l'état de protection de nos installations et activités. La DRSD apporte alors une analyse des modes d'action derrière les incidents, fondée sur ses capacités propres et d'évaluation des menaces. En complément, nous échangeons également dans ce cadre avec la DGA pour évaluer quels secteurs d'activités sont davantage ciblés, ainsi qu'avec l'ANSSI et le COMCYBER à propos de la sécurité numérique. Nous menons donc un certain nombre d'actions complémentaires qui nous permettent de cartographier la menace. Pour sa part, la DRSD joue en outre un rôle opérationnel de terrain, en mettant en œuvre les mesures de protection : elle va inspecter un certain nombre de sites, parfois à notre demande, et les comptes rendus qu'elle va produire viennent nourrir notre connaissance globale de l'écosystème.

S'agissant ensuite de la défense opérationnelle du territoire et de la protection des infrastructures, il convient de distinguer clairement les périmètres. Pour ce qui me concerne, ma responsabilité porte sur la défense et la sécurité des moyens, installations et activités relevant de mon champ. Pour sa part, la DOT comporte un volet permanent, qui porte sur la protection de nos installations

La protection interne des emprises relève directement de ma responsabilité. En revanche, dès lors que l'on dépasse ce périmètre pour entrer dans une logique d'engagement des forces armées sur le territoire national, nous basculons dans le champ de la DOT, qui relève du chef d'état-major des armées.

Cette distinction est explicitement prévue par les textes, qui précisent que j'exerce mes missions sans préjudice des responsabilités du chef d'état-major des armées en matière d'emploi opérationnel des forces. Il n'en demeure pas moins qu'il existe un *continuum* entre ces deux dimensions. Nous échangeons ainsi avec l'EMA, la division emploi notamment mais également avec l'EMIA-TN, qui a piloté l'exercice Orion.

Mme Catherine Hervieu (EcoS). En tant que rapporteure du titre I du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, je tiens à partager mon regret que son examen soit repoussé en raison de l'article 16 bis.

Ensuite, dans le cadre du cycle d'auditions actuel, plusieurs questions se posent concernant l'adaptation de notre dispositif national de protection. Les attaques hybrides combinent aujourd'hui cyberattaque, désinformation, sabotage, instrumentalisation économique ou encore pression sur les infrastructures critiques. Elles brouillent la frontière entre temps de paix et temps de crise, entre sécurité intérieure et défense nationale. Comment l'État français adapte-t-il concrètement sa doctrine de protection et de résilience ?

Par ailleurs, la multiplication des vulnérabilités technologiques, en particulier dans le cyberspace, les réseaux énergétiques, les satellites ou les chaînes logistiques, semble exiger une logique de vigilance permanente. Considérez-vous que la France dispose aujourd'hui d'une véritable culture stratégique de résilience, diffusée au sein de la société civile et des institutions, dans toutes leurs dimensions ? Faut-il encore renforcer la sensibilisation de la population et des entreprises face à ces nouvelles formes de conflictualité ?

Enfin, dans un contexte international marqué par le retour des rapports de force, quelles priorités vous paraissent essentielles pour garantir à moyen terme la protection des intérêts stratégiques français ?

M. Xavier Brunetière. L'adaptation à l'évolution des menaces et attaques hybrides repose sur une démarche profondément intégrée de planification de défense et de sécurité nationale. Il ne s'agit en aucun cas d'une planification statique, ni d'un simple plan d'action figé. Cette planification consiste en un ensemble de mesures évolutives, qui s'ajustent en permanence à l'appréciation de la situation et à l'évolution de la menace. L'enjeu majeur réside donc dans notre capacité à faire face à l'intensification de ces menaces, grâce à une adaptation continue et réactive.

Le second volet que vous évoquez concerne la culture du risque et de la menace et la sensibilisation de la population. À cet égard, le guide « Tous responsables », diffusé par le gouvernement en novembre dernier, constitue un outil de référence en matière de résilience. Il présente à la fois les menaces et les risques, dimensions indissociables de toute démarche de résilience. À cela s'ajoute le guide de bonnes pratiques élaboré avec l'Association des maires de France et diffusé en avril dernier, qui contribue à renforcer la culture du risque, de la menace et, plus largement, de la résilience.

M. le général de division aérienne Nicolas Leverrier. Nous avons naturellement travaillé à la préparation du projet de loi relatif à la résilience des entités et des infrastructures critiques et NIS 2 et nous demeurons désormais dans l'attente de son vote définitif et de sa promulgation. Dès que ce cadre sera stabilisé, nous serons en mesure d'en assurer la déclinaison, dans une logique interministérielle et en coordination avec le SGDSN.

S'agissant de la multiplication des menaces et de la culture stratégique, des exercices comme Orion contribuent de manière significative à cette culture de la sécurité que j'appelle de mes vœux. De nombreuses initiatives existent, y compris au sein des entreprises. On constate aujourd'hui une diffusion réelle de cette culture, les enjeux étant désormais compris au niveau industriel. Nous-mêmes entretenons un dialogue étroit avec les industriels, au-delà du seul cadre des OIV.

Mme Geneviève Darrieussecq (Dem). Monsieur le préfet, vous avez parlé de planification, d'indispensable organisation interministérielle, de sécurité des réseaux, des sites d'intérêts vitaux. Général, vous avez souligné à juste titre que l'ennemi cherche la vulnérabilité, les maillons faibles. À cet égard, chaque citoyen français n'est-il pas un « maillon faible », en particulier en matière de cybersécurité ? Comment développer des plans de sensibilisation, de formation à très grande échelle, de façon visible ? Comment suivre, voire accompagner les évolutions technologiques ?

M. Xavier Brunetière. Un travail approfondi est conduit, notamment au sein du SGDSN, sur la capacité à innover, y compris en lien étroit avec les collectivités territoriales. Dans ce cadre, des expérimentations sont actuellement menées avec plusieurs collectivités afin d'explorer l'usage de l'intelligence artificielle dans la gestion de crise.

Au-delà de ces initiatives, l'ensemble des ministères est engagé dans cette dynamique d'innovation, qui bénéficie également d'une forte complémentarité à l'échelle européenne et dans le cadre des relations bilatérales entretenues avec certains partenaires stratégiques.

S'agissant, ensuite, de la culture stratégique et de la perception de la menace par les citoyens, il convient de rappeler que la stratégie de résilience portée par le gouvernement repose sur une approche globale, intégrant l'ensemble des risques. Elle s'appuie notamment sur des expériences déjà acquises dans les domaines des risques naturels ou technologiques, afin de développer des réflexes adaptés.

À ce titre, les collectivités territoriales disposent déjà d'une solide culture de gestion de crise, qui constitue un socle précieux. À cela s'ajoutent des dispositifs plus structurés, tels que les réserves communales de sécurité civile, un outil extrêmement intéressant pour relever le niveau de culture stratégique, mais aussi de réflexes sur lesquels peuvent s'appuyer nos compatriotes.

M. le général de division aérienne Nicolas Leverrier. Quel est le maillon faible ? En effet, l'attaquant ne cible pas nécessairement le système d'information lui-même, qui peut être difficilement accessible, mais plutôt les personnes qui y ont accès, celles qui en maîtrisent les usages ou encore celles qui évoluent au sein de l'écosystème de l'organisation.

Dès lors, la gestion de ce maillon faible repose en grande partie sur une acculturation globale. Comme l'a rappelé récemment le secrétaire général de la défense et de

la sécurité nationale, plusieurs stratégies sont aujourd'hui en place, notamment la stratégie nationale cyber, dont il convient désormais d'assurer la pleine mise en œuvre.

Sur le second point relatif à l'agilité face aux évolutions technologiques. Nous avons déjà été confrontés à des situations concrètes, par exemple des suspicions d'utilisation de lunettes connectées dans une entreprise, par un sous-traitant. Ces situations ont été traitées, notamment par l'analyse des données disponibles, ce qui montre que les responsables de la sécurité intègrent déjà ces nouveaux risques dans leurs dispositifs de vigilance.

Aujourd'hui, il s'agit d'objets connectés, tels que les téléphones ou certains équipements. Demain, ces dispositifs seront encore plus intégrés à notre quotidien. Cette évolution de l'écosystème numérique est rapide et impose une anticipation constante.

C'est dans cette perspective que nous travaillons en lien étroit avec l'état-major des armées, le COMCYBER et la DRSD. L'objectif consiste à identifier les défis émergents liés à ces technologies, d'anticiper leurs évolutions et d'en évaluer les risques, afin de déterminer dès à présent les mesures de protection appropriées.

M. Loïc Kervran, président. Cette question du maillon faible est essentielle. Il y a peu, le ministre de l'intérieur nous rappelait que lors des principales cyberattaques qui ont récemment visé la France, une défaillance humaine avait à chaque fois été mise en lumière.

Mme Lise Magnier (HOR). Députée de la Marne, de Suippes et de Mourmelon-le-Grand, je me dois d'évoquer avec vous la problématique du survol par drone sans autorisation de nos sites militaires. Le groupe Horizon et indépendants a veillé à compléter le dispositif pénal dans le cadre de l'actualisation de la LPM, pour sanctionner et réprimer plus fortement ces survols sans autorisation.

Quel lien le ministère souhaite-t-il nouer avec les capacités des opérateurs civils à accompagner ce sujet de sécurité nationale ? Je pense notamment à *Orange Cyberdefense*, qui propose de mettre à disposition le réseau national de pylônes téléphoniques, pour participer à la détection et à l'identification des drones, afin d'accélérer la qualification de la menace en cas de survol. Le ministère envisage-t-il une contractualisation de ce type, pour bénéficier de cette opportunité ?

Ensuite, nous avons déjà évoqué la transposition de la directive NIS 2. Vous avez dit être prêts, une fois que la loi serait promulguée. Pouvez-vous nous détailler les conséquences très concrètes du retard pris par la France dans cette transposition ?

Enfin, vous avez parlé d'écosystème du ministère. L'hybridité de la menace vise la sécurité des sites et emprises physiques, autant que l'environnement numérique. Vous avez complété vos propos en insistant sur une nécessaire acculturation nationale. Comment s'assurer de son caractère effectif, dans l'ensemble de l'écosystème que vous venez d'évoquer ? À titre d'exemple, nos OIV transmettent nécessairement un nombre très important de documents, de données à leurs assureurs. Comment veillez-vous à ce que ces assureurs, ces cabinets d'audit, de certification ISO, ne deviennent pas des cibles privilégiées ? Ne serait-il pas opportun d'accréditer ou de certifier aussi ces acteurs, aujourd'hui considérés comme plus que périphériques au sein de notre BITD ?

M. Xavier Brunetière. S'agissant tout d'abord de la lutte anti-drone, vous avez parfaitement identifié l'un des défis majeurs, qui réside dans la capacité de détection et de caractérisation. Cette capacité est en effet essentielle, car elle permet d'objectiver les situations et d'éviter toute forme d'intoxication.

Dans cette perspective, nous nous appuyons notamment sur les retours d'expérience acquis lors des Jeux olympiques et paralympiques de 2024. Ces enseignements nous conduisent aujourd'hui à travailler activement à l'extension de nos capacités de détection à l'échelle nationale, en particulier pour les drones dits coopératifs. Ce travail est conduit dans un cadre interministériel, en étroite coordination avec le ministère des armées, la chaîne de défense et de sécurité aérienne, ainsi qu'avec le ministère de l'intérieur. Par ailleurs, nous associons également à ces réflexions les opérateurs essentiels.

Les orientations et dispositions concrètes des directives REC et NIS 2 ont déjà été diffusées aux opérateurs. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a notamment communiqué récemment des éléments précisant de manière opérationnelle les implications de ce cadre. Ainsi, une phase de préparation a d'ores et déjà été engagée, parfois de manière discrète, permettant aux acteurs concernés d'anticiper les évolutions à venir.

Enfin, pour les OIV, ce travail s'inscrit dans une démarche continue, conduite en lien avec les hauts fonctionnaires de défense et de sécurité. Sans attendre la transposition formelle, nous poursuivons les actions visant à élever le niveau de protection de ces opérateurs, en tenant compte notamment de leurs interdépendances.

M. le général de division aérienne Nicolas Leverrier. Madame la députée, vous avez évoqué Mourmelon et la lutte anti-drones. Sans revenir sur l'ensemble des travaux déjà conduits, je rappelle que nous avons engagé une réflexion approfondie afin d'adapter notre dispositif aux spécificités de certains sites, mais surtout aux activités qui y sont exercées.

Vous avez ensuite évoqué la réponse judiciaire, notamment dans le cadre de l'actualisation de la loi de programmation militaire. La sanction doit certes demeurer proportionnelle au délit, mais elle doit également comporter une dimension dissuasive, notamment parce qu'il y a une dimension asymétrique entre les moyens que nous mettons en œuvre et ceux qu'un simple téléopérateur peut mobiliser C'est dans cette perspective que nous travaillons étroitement avec le SGDSN, afin d'intégrer pleinement la lutte anti-drones dans l'espace aérien et de la coordonner avec les grands opérateurs.

S'agissant de la directive NIS 2, vous m'avez interrogé sur les conséquences de sa non-adoption à ce stade. Là encore, nous avons choisi d'anticiper. L'ANSSI a ainsi demandé aux opérateurs de se préparer dès à présent aux exigences à venir. Cette démarche repose sur une logique d'anticipation pragmatique. Nous entretenons aujourd'hui un dialogue constant avec les opérateurs, qu'il s'agisse de déclaration d'incidents, de gestion des incidents ou encore d'évaluation et de maîtrise des risques. Bien que le cadre législatif ne soit pas encore achevé, les principaux attendus sont connus et partagés. En lien avec le SGDSN, nous veillons à encourager l'adoption immédiate des bonnes pratiques et des bons réflexes.

Enfin, vous avez mentionné l'écosystème ; votre observation est pleinement justifiée. Mon périmètre inclut les emprises militaires, mais également les établissements publics sous tutelle et certaines entreprises privées. Mon point d'entrée demeure

prioritairement les opérateurs d'importance vitale, toutefois il ne s'y limite pas. Dès lors qu'une entité détient des données sensibles du ministère des armées, au titre de la protection du secret, elle se voit soumise à des obligations strictes.

Cela concerne un ensemble large d'acteurs, y compris ceux que vous avez cités, tels que les assureurs ou les cabinets d'audit. Notre approche dépasse ainsi le seul cadre de la base industrielle et technologique de défense.

M. Antoine Valentin (UDR). Entre les sabotages de câbles sous-marins en mer Baltique, les cyberattaques contre les infrastructures énergétiques européennes, les survols de sites par des drones, ou encore les sabotages coordonnés du réseau ferroviaire, il est incontestable qu'il est désormais possible de désorganiser durablement un État sans déclencher formellement la guerre. L'objectif n'est plus nécessairement de détruire massivement, mais d'user progressivement.

Il nous faut donc regarder les choses avec lucidité : la France ne dispose ni des moyens humains, ni des moyens budgétaires permettant de protéger physiquement chaque installation sensible du territoire, même avec les 436 milliards d'euros proposés par la mise à jour de la LPM. Nous restons dans une logique de ressources contraintes face à des puissances capables d'investir des montants largement supérieurs aux nôtres, près de 950 milliards d'euros par an pour les États-Unis ou 330 milliards d'euros pour la Chine. La question stratégique n'est donc plus de savoir comment protéger tout, partout et en permanence, cela étant impossible ; mais plutôt de savoir si nous sommes capables aujourd'hui de détecter et rendre une attaque hybride inefficace.

Les retours récents montrent l'usage croissant des drones commerciaux, très simples, pour effectuer des reconnaissances discrètes avant frappe ou des opérations de sabotage. Nos infrastructures sensibles disposent-elles, à ce jour, des moyens de détection suffisamment précis pour repérer, même dans un environnement civil dense, des drones de petite taille, à faible signature ? Quelles réponses pouvons-nous aujourd'hui donner à ce type d'attaque ?

M. Xavier Brunetière. En premier lieu, nous nous inscrivons encore dans une phase d'actualisation de la loi de programmation militaire, qui fait actuellement l'objet de débats parlementaires. Ces travaux visent précisément à doter les opérateurs des capacités nécessaires, c'est-à-dire non seulement détecter les menaces, mais aussi être en mesure de les neutraliser. Dans ce cadre, il apparaît évident qu'un opérateur a intérêt à investir dans des dispositifs de détection dès lors qu'il peut disposer, en aval, des moyens de neutralisation.

En second lieu, se pose la question de l'adéquation de la réponse à la menace. C'est un axe de travail structurant que nous conduisons avec les hauts fonctionnaires de défense et de sécurité, en lien avec les différents services concernés. Il s'agit, pour chaque secteur d'activité, de caractériser avec précision la menace à un instant donné, afin de déterminer les mesures les plus appropriées et proportionnées.

M. le général de division aérienne Nicolas Leverrier. Je souhaite compléter le propos, en m'appuyant sur deux notions essentielles.

La première tient à la surface d'attaque. Lorsqu'il s'agit d'une attaque physique, le périmètre du glaive et du bouclier demeure relativement aisé à conceptualiser. En revanche,

dès que l'on aborde les attaques hybrides, la surface d'attaque se transforme, s'étend et devient nettement plus diffuse. Certains opérateurs que nous avons sensibilisés à ces menaces nous ont d'ailleurs fait observer qu'il leur paraissait logique de faire l'objet d'un grand nombre de tentatives, dès lors qu'ils sont en relation avec une multitude d'acteurs. Or, telle est précisément la logique d'une stratégie hybride : elle ne cible pas uniquement l'opérateur lui-même, mais également ses sous-traitants, ses personnels.

Cet élargissement constitue donc l'un des enjeux majeurs. En le rapprochant de la lutte anti-drones que vous évoquiez, je souligne à nouveau la forte asymétrie qui caractérise la menace. D'un côté, un drone du commerce, peu coûteux, facilement accessible, est susceptible de mettre à l'épreuve la protection de nos installations. De l'autre, les dispositifs que nous déployons doivent couvrir l'ensemble du spectre des menaces identifiées à un instant donné, avec des moyens qui s'avèrent, eux, considérables. Cette dissymétrie justifie que l'approche retenue soit désormais résolument collaborative. La question n'est pas seulement de disposer de capacités de détection, mais bien d'aller au-delà. C'est tout le sens des dispositions introduites dans l'actualisation de la LPM, qui confèrent aux opérateurs d'importance vitale la capacité non seulement de détecter, mais aussi de neutraliser.

Cette évolution marque une forme de responsabilisation accrue. Jusqu'à présent, un opérateur privé pouvait légitimement s'interroger sur l'utilité de détecter une menace sans disposer des moyens d'y répondre directement. Désormais, l'accès à un éventail complet de capacités lui permettra d'investir davantage dans ces enjeux, dont chacun mesure pleinement l'importance.

Le second point sur lequel je souhaite insister concerne cette approche collaborative, notamment avec le ministère de l'intérieur. En matière de protection des sites, nous disposons de plans internes, et dès lors que l'on franchit ce périmètre, la continuité est assurée par des plans de protection externe placés sous la responsabilité des préfets. Aujourd'hui, notre objectif consiste à renforcer cette continuité entre les deux dispositifs. Cette cohérence est particulièrement déterminante dans le cadre de la lutte anti-drones : une intrusion détectée sur un site doit pouvoir entraîner immédiatement une action coordonnée des forces de sécurité intérieure.

M. Loïc Kervran, président. Nous passons maintenant à une séquence de quatre questions individuelles complémentaires, en commençant par une première série de deux questions.

M. Thomas Gassilloud (EPR). Je voudrais commencer par saluer les évolutions entreprises sur notre stratégie de résilience ces dernières années. En 2022, j'avais commis un rapport sur la résidence nationale, dans lequel j'avais été assez critique. Cependant, je m'aperçois que la situation a bien progressé, ces dernières années. Depuis les années 1960, le concept de défense globale est établi, mais comment jugez-vous aujourd'hui les moyens des ministères sur les questions de défense, en dehors du ministère des armées ? Je pense notamment aux ministères de la santé et de l'intérieur.

À titre d'exemple, nos forces de gendarmerie disposaient il y a vingt ans de moyens pour participer à la défense opérationnelle du territoire (DOT). Malheureusement, ces moyens n'ont pas été renouvelés. À l'heure des menaces hybrides et du besoin de masse, cela demeure assez surprenant.

Ensuite, le citoyen occupe un rôle de plus en plus important dans les documents stratégiques. Il n'est plus uniquement considéré comme une cible d'effet à produire, mais comme un élément de solution. Mais dans les faits, le guide « Tous responsables », une préconisation de mon rapport, est diffusé de manière très frileuse : les jeunes qui participent aux journées défense et citoyenneté (JDC) ne le reçoivent pas.

La LPM prévoit une obligation de déclaration de compétences, mais sans aucune réelle incitation. Nous ressentons bien cette très grande frilosité à assumer ce rôle en matière de défense vis-à-vis du citoyen. Selon vous, d'où cette frilosité provient-elle ? Comment agir davantage pour progresser vers un dispositif plus proche du modèle scandinave ?

M. Romain Tonussi (RN). La guerre est un caméléon ; la guerre des normes en est aujourd'hui une facette particulièrement stratégique. Les standards techniques structurent désormais les dépendances technologiques et les rapports de puissance. Des réglementations extraterritoriales américaines comme l'ITAR en constituent une illustration concrète. Or, dans des secteurs émergents structurants comme le quantique, les acteurs européens restent manifestement à la traîne dans leur propre organisme de création des normes. Au sein de l'Institut européen des normes de télécommunication, force est de constater qu'Américains et Chinois mènent des stratégies d'influence beaucoup plus offensives et coordonnées que nous.

L'Union européenne aborde comme toujours ces enjeux essentiellement sous un angle technique ou réglementaire et la France ne saisit pas pleinement ce levier de souveraineté stratégique. Comment la France entend-elle défendre plus activement ses intérêts dans ses enseignes de standardisation ?

M. Sébastien Saint-Pasteur (SOC). Ma question porte sur la résilience des réseaux, à travers deux exemples très concrets, la fibre et la téléphonie mobile. S'agissant de la fibre, j'ai la chance de représenter un département qui a été précurseur sur cet enjeu, le département de la Gironde. À la suite des incendies de 2022, lors du RETEX sur le diagnostic de résilience, des points de vulnérabilité majeurs ont été soulevés. Bien que coûtant peu d'argent, la solution recommandée n'a pas été retenue, faute de moyens financiers et de désignation de financeurs pour la remise à niveau de la sécurité de ces infrastructures. Il en va de même pour téléphonie mobile. Nous avons pu le constater lorsque nous avons été confrontés aux problématiques de délestage, à la suite des crises énergétiques.

Je parlais de 2022, mais nous sommes aujourd'hui en 2026 et nous n'avons pas l'impression que de réels progrès ont été accomplis pour sécuriser ces infrastructures, ces réseaux. Ce constat est-il partagé ? Quelles sont vos préconisations pour trouver les moyens de remettre à niveau ces infrastructures ?

Mme Nadine Lechon (RN). Monsieur le préfet, général, lorsque nous parlons de souveraineté et de sécurité informatique, nous mentionnons très régulièrement les sociétés privées, très nombreuses, auxquelles nous faisons appel pour sécuriser les sites et le travail que nous conduisons sur nos ordinateurs ou autres smartphones. Ces acteurs privés sont nécessaires, compétents et efficaces mais de quelle façon garantissons-nous à 100 % qu'ils ne soient pas eux-mêmes sous influence étrangère ou qu'ils ne jouent pas un potentiel double jeu ? Cette question est d'autant plus importante lorsque certaines de ces sociétés peuvent être implantées dans plusieurs pays et être elles-mêmes des sociétés étrangères.

Il faut également mentionner le sujet du traitement de l'usage des données et des informations que nous pouvons leur confier. Comment assurez-vous le contrôle et la sécurisation de ces sociétés ? Quels sont les filtres en amont ? Quel suivi est-il ensuite réalisé ?

M. Xavier Brunetière. Monsieur le député Gassilloud, je vous remercie pour votre question ainsi que pour le rappel des travaux de votre commission sur la résilience, dont les apports sont particulièrement précieux pour l'action que nous conduisons au sein du SGDSN. S'agissant tout d'abord de la communication en matière de résilience, vous avez évoqué le guide récemment diffusé. Je souhaite rappeler également le guide élaboré conjointement avec l'Association des maires de France, qui recense un ensemble de bonnes pratiques en matière de résilience et qui vient d'être finalisé.

Au-delà, la question des moyens dont disposent les ministères pour faire face aux enjeux de sécurité nationale doit être rapprochée de la planification de défense et de sécurité nationale. Cette planification constitue un cadre structurant qui mobilise l'ensemble de la communauté interministérielle, et non pas seulement le ministère des armées. Elle offre ainsi aux ministères un cadre clair pour adapter et dimensionner leurs moyens en fonction des scénarios de montée en puissance envisagés.

Monsieur le député Tonussi, vous avez évoqué les enjeux de sécurité économique. Ceux-ci sont pilotés notamment par la direction des affaires internationales, stratégiques et technologiques au sein du SGDSN, en lien étroit avec le ministère de l'économie et des finances. Cette action s'articule directement avec la gestion de nos vulnérabilités et la protection de nos technologies critiques. Des dispositifs existent à l'échelle nationale, et certains ont été renforcés dans le cadre de l'actualisation de la LPM, notamment en matière de mobilisation des capacités industrielles de défense et de sécurité. Par ailleurs, un travail est également conduit à l'échelle européenne autour des fournisseurs dits à haut risque, les *high risk suppliers*, permettant d'identifier et de traiter des acteurs sensibles dans des secteurs stratégiques.

Enfin, monsieur le député Saint-Pasteur, s'agissant de la résilience des réseaux de télécommunication, nous sommes au cœur d'une problématique combinant réponse au risque et réponse à la menace. Cet enjeu est explicitement intégré dans la stratégie nationale de résilience. Des outils ont été proposés aux préfets afin de structurer l'action des opérateurs de ces réseaux à l'échelle départementale. En parallèle, un travail interministériel est conduit, notamment par la DGE, pour mieux appréhender les interdépendances critiques, en particulier entre réseaux énergétiques et réseaux de télécommunication. Des dispositions spécifiques issues de l'actualisation de la loi de programmation militaire visent également à améliorer la remontée d'informations des opérateurs télécoms en temps quasi réel, en cas de défaillance de réseau. Cet enjeu est pleinement identifié et fait l'objet d'actions continues.

M. le général de division aérienne Nicolas Leverrier. Monsieur le député Gassilloud, vous avez soulevé deux questions distinctes auxquelles je souhaite répondre de manière directe. La première portait sur les moyens relevant d'autres ministères. Il ne m'appartient évidemment pas de me prononcer sur ce sujet en dehors de mon périmètre. Toutefois, je tiens à souligner avec insistance le rôle essentiel joué par les hauts fonctionnaires de défense et de sécurité dans les autres ministères. Pour avoir eu l'occasion d'interagir régulièrement avec eux, je peux attester de leur implication remarquable. Cette mobilisation

est apparue de manière particulièrement visible lors des derniers Jeux olympiques et paralympiques, puis s'est confirmée à nouveau au cours de l'exercice Orion.

Votre seconde interrogation concernait la diffusion du guide « Tous responsables ». Sur ce point, je distinguerai volontiers deux lectures possibles. La diffusion reste certes encore perfectible, et il est toujours possible d'amplifier l'effort, notamment en lien avec le SGDSN. Pour ma part, je privilégie une lecture plus positive : ce guide existe, il a été publié et diffusé, ce qui constitue déjà une base solide. Par ailleurs, un travail est engagé pour en assurer la déclinaison vers les collectivités territoriales. Nous pourrons naturellement poursuivre cet effort de diffusion, mais l'enjeu me paraît désormais être la mise en œuvre et la déclinaison au niveau territorial de l'ensemble des stratégies que nous avons évoquées.

Ensuite, au-delà du seul aspect normatif, la technologie quantique est pleinement prise en compte dans nos réflexions et dans nos dispositifs. Elle est intégrée dès à présent dans nos systèmes et fait également l'objet d'une attention soutenue de la part des industriels avec lesquels nous collaborons. Notre objectif n'est pas seulement d'éviter un retard sur ces technologies émergentes, mais bien de nous situer en position d'anticipation, voire d'avance.

Je souhaite ensuite revenir sur la question de la résilience des réseaux que vous avez soulevée. Même si les réseaux de télécommunications n'entrent pas directement dans mon périmètre, il n'en demeure pas moins que leur problématique constitue un enjeu central. Protéger des installations ponctuelles peut apparaître relativement simple ; en revanche, sécuriser des réseaux de diffusion, quels qu'ils soient, représente une difficulté bien plus complexe. Dans le cadre des stratégies hybrides que nous avons longuement évoquées, cette dimension constitue un point d'attention majeur.

Enfin, madame la députée, vous avez abordé la sécurité des produits informatiques. La sécurité numérique est au cœur de nos préoccupations. L'ANSSI joue un rôle déterminant ; elle certifie des opérateurs, labellise des solutions et émet des recommandations précises quant à l'usage de certains produits. Nous travaillons en étroite coopération avec elle, précisément parce qu'elle porte une vision globale et émet des recommandations sur l'usage de certains produits.

M. Loïc Kervran, président. Je vous remercie.

La séance est levée à dix heures cinquante-quatre.

*

* *

Membres présents ou excusés

Présents. - Mme Delphine Batho, M. Christophe Bex, M. Christophe Blanchet, M. Matthieu Bloch, Mme Blandine Brocard, M. Bernard Chaix, Mme Caroline Colombier, M. François Cormier-Bouligeon, M. Michel Criaud, Mme Geneviève Darrieussecq, Mme Sophie Errante, M. Guillaume Garot, M. Thomas Gassilloud, M. Frank Giletti, M. José Gonzalez, M. Daniel Grenon, Mme Catherine Hervieu, M. Laurent Jacobelli, M. Loïc

Kervran, Mme Nadine Lechon, Mme Lise Magnier, Mme Josy Poueyto, Mme Catherine Rimbert, M. Aurélien Rousseau, M. Sébastien Saint-Pasteur, M. Thierry Sother, M. Jean-Louis Thiériot, M. Romain Tonussi, M. Antoine Valentin

Excusés. - Mme Valérie Bazin-Malgras, Mme Anne-Laure Blin, M. Frédéric Boccaletti, M. Manuel Bompard, Mme Yaël Braun-Pivet, M. Hubert Brigand, M. Charles Fournier, M. Moerani Frébault, M. Jean-Michel Jacques, M. Pascal Jenft, M. Bastien Lachaud, M. Abdelkader Lahmar, M. Antoine Léaument, Mme Michèle Martinez, Mme Alexandra Martin (Alpes-Maritimes), Mme Anna Pic, Mme Isabelle Rauch, Mme Mereana Reid Arbelot, M. Arnaud Saint-Martin, M. Aurélien Saintoul, M. Mikaele Seo, M. Boris Vallaud, M. Laurent Wauquiez.

Assistait également à la réunion. - Mme Corinne Vignon