ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
4 décembre 2024
Séance de 9 heures

Compte rendu n° 27

SESSION ORDINAIRE DE 2024-2025

Compte rendu

Commission de la défense nationale et des forces armées

— Nomination d'un rapporteur pour avis sur le projet de loi autorisant la ratification du traité sur la coopération dans le domaine de la défense entre la République française et le Royaume d'Espagne (n° 621).

— Nomination d'un rapporteur sur la proposition de résolution tendant à la création d'une commission d'enquête relative à la politique française d'expérimentation nucléaire, à l'ensemble des conséquences de l'installation et des opérations du Centre d'expérimentation du Pacifique en Polynésie française, à la reconnaissance, à la prise en charge et à l'indemnisation des victimes des essais nucléaires français, ainsi qu'à la reconnaissance des dommages environnementaux et à leur réparation (n° 311).

— Audition, ouverte à la presse, de M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale, sur les enjeux de l'économie de guerre.

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

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

M. le président Jean-Michel Jacques. Monsieur le secrétaire général, mes chers collègues, mesdames, messieurs, avant de commencer notre audition, je vous propose, comme cela est prévu à l'ordre du jour, de désigner deux rapporteurs.

● D'une part, nous devons nommer un rapporteur pour avis sur le projet de loi autorisant la ratification du traité de coopération dans le domaine de la défense entre la République française et le Royaume d'Espagne.

Je rappelle que je suis favorable au fait que la commission se saisisse pour avis de tous les projets de loi de ratification des traités ayant des implications pour la défense. Notre commission est susceptible de porter, me semble-t-il, un regard tout à fait complémentaire à celui des affaires étrangères, qui reste la commission compétente au fond pour tous les traités.

J'ai reçu une candidature de M. Sébastien Saint-Pasteur.

En l'absence d'autres candidatures, *M. Sébastien Saint-Pasteur est donc désigné comme rapporteur pour avis sur le projet de loi autorisant la ratification du traité sur la coopération dans le domaine de la défense entre la République française et le Royaume d'Espagne (n° 621).*

● D'autre part, nous devons nommer un rapporteur sur la proposition de résolution tendant à la création d'une commission d'enquête relative à la politique française d'expérimentation nucléaire, à l'ensemble des conséquences de l'installation et des opérations du Centre d'expérimentation du Pacifique en Polynésie française, à la reconnaissance, à la prise en charge et à l'indemnisation des victimes des essais nucléaires français, ainsi qu'à la reconnaissance des dommages environnementaux et à leur réparation.

Cette mission d'enquête, qui a fait l'objet d'un droit de tirage du groupe parlementaire Gauche démocrate et républicaine, avait été mise en place sous la précédente législature avec M. Didier Le Gac (EPR) comme président et Mme Mereana Reid Arbelot (GDR) comme rapporteure. Les travaux de cette précédente commission avaient été interrompus avec la dissolution.

Notre collègue Didier Le Gac a fait acte de candidature pour rapporter cette proposition de résolution. Il pourra ainsi nous faire un point sur l'état d'avancement des travaux lors de la présente législature. Mme Mereana Reid Arbelot m'a informé qu'elle soutenait cette candidature.

En l'absence d'autres candidatures, *M. Didier Le Gac est nommé rapporteur sur la proposition de résolution tendant à la création d'une commission d'enquête relative à la politique française d'expérimentation nucléaire, à l'ensemble des conséquences de l'installation et des opérations du Centre d'expérimentation du Pacifique en Polynésie française, à la reconnaissance, à la prise en charge et à l'indemnisation des victimes des essais nucléaires français, ainsi qu'à la reconnaissance des dommages environnementaux et à leur réparation (n° 311).*

● Nous poursuivons maintenant notre cycle d'audition dédié à l'économie de guerre en accueillant pour la première fois depuis cette nouvelle législature M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale.

Monsieur le secrétaire général, je rappelle, pour nos nouveaux collègues qui ne vous connaissent pas encore, qu'avant d'exercer vos fonctions actuelles, vous avez passé

pratiquement toute votre carrière au ministère de l'Intérieur comme préfet, mais aussi comme directeur de cabinet du ministre à deux reprises, de 2011 à 2012 et de 2018 à 2020.

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) est notamment chargé de la préparation des plans gouvernementaux et de l'organisation de l'État en temps de crise, ce qui en fait un acteur central dans notre préparation à l'économie de guerre.

La dimension interministérielle du SGDSN est particulièrement adaptée à l'économie de guerre. Celle-ci doit en effet mobiliser l'ensemble des ministères et pas seulement le ministère des armées et des anciens combattants. Je pense par exemple au financement de la base industrielle et technologique de défense *(*BITD*)* ou à la question des stocks stratégiques, qui sont des sujets sur lesquels le SGDSN est fortement mobilisé.

Enfin, il sera également intéressant de vous entendre, monsieur le secrétaire général, sur l'action menée en matière de sécurisation des sites industriels de notre BITD, qu'en tant que députés, nous connaissons bien lors de nos déplacements dans les différentes entreprises situées sur nos circonscriptions. Ces entreprises constituent en effet une véritable cible potentielle pour nos compétiteurs stratégiques dans le contexte actuel, comme l'ont rappelé de récents incidents en Allemagne.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Monsieur le président, mesdames et messieurs les députés, je parle au nom des 1 600 agents qui, dans toutes les missions du SGDSN, sont au service de la Nation.

Monsieur le président, vous avez souhaité que j'apporte notre contribution au travail de revue de l'économie de guerre, qui avait été entamé par votre prédécesseur, M. Thomas Gassilloud.

J'aborderai le sujet un peu différemment du ministre des armées et des anciens combattants, des industriels de la BITD ou du délégué général pour l'armement, puisque mon action s'inscrit à la fois dans le champ de l'action interministérielle et dans celui de la défense civile aux côtés de la défense militaire.

La première fois que l'expression « économie de guerre » a surgi dans le débat public, c'était lors du discours du Président de la République au salon Eurosatory en 2022. Il avait, compte tenu de la guerre en Ukraine, souligné la nécessité pour notre base industrielle de défense de changer de paradigme économique afin d'être en mesure de faire face aux besoins et à nos engagements, mais également de renforcer et revoir notre sécurité, dans la mesure où nous avions davantage une « armée de vitrine » qu'une armée capable de produire en quantité l'ensemble des moyens nécessaires.

Nous avons donc repris cette ambition au travers de l'un des dix objectifs stratégiques qui étaient retenus dans la revue nationale stratégique, laquelle a permis de préparer la loi de programmation militaire (LPM) 2024-2030, votée en 2023.

La LPM a d'ores et déjà permis de moderniser et d'adapter le régime des réquisitions en temps de paix et en temps de guerre. Le texte organise par ailleurs la possibilité de constituer des stocks stratégiques de matières ou composants d'intérêts stratégiques au profit des armées. Elle établit aussi la possibilité de procéder à une priorisation de la livraison de biens et services aux bénéfices des armées. Toute une série d'outils juridiques a donc été mise en place et vise à contribuer au développement de cette économie de guerre.

Plusieurs entreprises ont ainsi réussi à accélérer significativement leur cadence de production et à démontrer les premiers effets de ces mesures. C'est notamment le cas de Nexter, qui a réduit de moitié les délais de production des canons CAESAR, ou de Dassault, qui a triplé sa capacité de production mensuelle de Rafales.

Je n'évoquerai pas les questions de cadences industrielles, de goulets d'étranglement ou de simplification des normes de production. Ma plus-value sera plutôt de vous parler de l'économie civile face à la guerre économique et donc, d'une certaine manière, l'économie en guerre.

Dans cette perspective de l'économie en guerre, le SGDSN travaille bien sûr en étroite coopération avec le ministère des armées et des anciens combattants, la direction générale de l'armement (DGA), le ministère de l'économie et des finances et la direction générale de l'entreprise (DGE).

Nous avons contribué et nous suivons évidemment la programmation militaire, comme l'ensemble des dispositifs qui visent à accélérer et à améliorer la préparation de la Nation à faire face à un engagement majeur. À ce titre, nous avons participé de près à la préparation de la dernière LPM, nous avons rédigé la revue stratégique et nous avons coorganisé la phase 3 de l'exercice Orion, qui a justement traité de la capacité de l'économie à venir en soutien à nos forces armées dans le cadre d'une opération. Ce travail sera répété pour l'exercice 2026.

Le SGDSN est un service du Premier ministre, chargé, aux côtés de son cabinet militaire et civil, de lui permettre d'assurer les responsabilités que l'article 21 de la Constitution lui confie. Le SGDSN travaille également pour le compte du président de la République, garant de l'indépendance nationale, de l'intégrité du territoire et du respect des traités selon l'article 5 mais aussi président du conseil de défense et de sécurité nationale selon l'article 15. Concernant ce dernier point, nous sommes chargés de la préparation de ses conseils et de leurs secrétariats, puis du suivi des décisions qui ont pu être prises.

En 2010, ce qui était auparavant le secrétariat général de la défense nationale (SGDN) est devenu SGDSN, c'est-à-dire qu'il a reçu dans ses missions le suivi de la sécurité nationale. L'objet était bien d'intégrer la nécessaire complémentarité entre défense à l'extérieur et sécurité à l'intérieur, ce qu'on appelle le continuum de sécurité.

Dans ce domaine, tout le dispositif de préparation de notre économie à une situation conflictuelle rentre en ligne de compte, y compris la préparation ou la protection de notre économie face à une situation de plus en plus conflictuelle, à la fois au niveau visible mais aussi au niveau invisible, à travers les menaces hybrides, les tentatives de prédation ou de sabotage, comme les attaques cyber. L'organisation du SGDSN a pour objectif de répondre à ces éléments.

La direction de la protection et de la sécurité de l'État planifie, forme et entraîne les acteurs de la gestion de crise, ce qui couvre non seulement les administrations de l'État, mais aussi les opérateurs d'importance vitale, c'est-à-dire les entreprises essentielles au bon fonctionnement de nos services publics qui doivent pouvoir être, en tout temps et en toutes circonstances, capables de réagir. Cette direction rédige et met à jour les plans antiterroristes de la famille Vigipirate, les plans sanitaires et plans de réaction aux accidents, quels qu'ils soient. C'est à ce titre qu'elle pilote depuis 2021 une stratégie nationale de résilience, approuvée par le Premier ministre et visant à mobiliser toute la Nation pour faire face aux crises. Cela touche aussi à l'économie de guerre. Votre commission ayant longuement

travaillé sur ces sujets ces dernières années, nous sommes donc régulièrement amenés à venir vous expliquer où nous en sommes et comment tout ceci fonctionne.

La direction des affaires internationales, stratégiques et technologiques, également importante en matière de sécurité économique, suit les crises internationales, mène des travaux interministériels d'anticipation et anime la lutte contre la prolifération. Dans tous ces domaines, nous sommes donc amenés à réfléchir en matière d'anticipation sur l'impact que pourrait avoir une extinction des satellites ou encore un *blackout* électrique ou d'Internet sur la situation de notre pays, et donc sur le fonctionnement des entreprises.

Avec la DGE du ministère de l'économie et des finances, cette direction protège le patrimoine scientifique et technique de nos entreprises et de nos laboratoires de recherche. Ainsi, nous veillons au fait que nos laboratoires de recherche soient mieux protégés et que nos principales entreprises respectent un minimum de règles de sécurité pour éviter qu'il puisse y avoir de l'espionnage, du sabotage ou tout simplement le « pompage » de la matière grise à l'intérieur de l'entreprise.

Cet après-midi encore, nous aurons une réunion avec la DGE pour regarder la situation dans un certain nombre d'entreprises convoitées par l'étranger, qui pourraient être rachetées et sur lesquelles nous sommes amenés à mettre en place tout un système avec Bpifrance et des moyens de sécurité afin de les protéger.

Nous assurons également le secrétariat de la commission interministérielle pour l'exportation d'armes de guerre et le secrétariat de la commission pour l'exportation de biens à double usage. Cela représente environ 4 000 à 5 000 nouvelles demandes de licences et environ 2 500 demandes de modifications de licences émises chaque année par les sociétés exportatrices d'armement. Permettre à nos entreprises d'exporter des armements, c'est leur permettre d'avoir la capacité économique de produire et de pouvoir garantir notre propre indépendance en la matière. Il est donc absolument indispensable que, sur les biens à double usage et sur l'exportation de matériel de guerre, nous puissions veiller à ce qu'il y ait un niveau d'exportation suffisant pour garantir la viabilité de nos entreprises.

Évidemment, nous veillons à ce que ces exportations soient faites dans le respect des traités ainsi que des règles françaises et que cela puisse prendre en compte le bon fonctionnement des entreprises. Il s'agit de tout un travail d'arbitrage qui m'amène, pour le compte du Premier ministre, à décider d'autoriser ou d'interdire une exportation.

Le travail de ces directions se fait en commun avec les ministères. Le SGDSN coordonne, synthétise, propose des points de sortie et d'arbitrage au Premier ministre ou à son cabinet avec pour objectif de protéger les intérêts fondamentaux de la Nation, donc son économie.

À côté de ces directions d'administration centrale, pour faire face à l'économie de guerre, nous avons plusieurs services à compétences nationales qui sont opérationnels et qui s'occupent des menaces hybrides, pour lesquelles nous sommes chefs de file.

Les menaces hybrides sont des attaques, menées en dessous des seuils de conflictualité et d'attribution, qui visent à désorganiser un pays — dans son économie, ses forces stratégiques, ses institutions ou encore lors des élections — de façon à pouvoir gagner sans avoir eu à combattre, comme le disait Sun Tzu. Le premier exemple de ces menaces hybrides est bien sûr les attaques cyber.

Au regard de ces menaces, une agence nationale de sécurité des systèmes informatiques (ANSSI) a été créée en 2009 et constitue l'autorité nationale de cybersécurité,

qui est de fait le bouclier cybersécuritaire du pays, son pompier, le régulateur national et l'autorité de police administrative du cyberespace. Cela vaut non seulement pour nos administrations, régulièrement attaquées par des entités étrangères qui visent donc à espionner, à pénétrer nos systèmes pour interrompre nos services publics ou tout simplement à séquestrer des données *via* des rançongiciels et, le cas échéant, les revendre sur le *dark web*. Tous les jours, nous en avons des exemples, à l'encontre d'administrations, des services publics, ou des entreprises privées, telles que Norauto ce matin encore. On peut en trouver bien d'autres, qui sont parfois très sensibles et stratégiques.

À ce titre, la directive européenne *Network and Information Security (NIS 2*), dont la transposition en droit français vous sera soumise en 2025, accroît à la responsabilité de l'ANSSI en lui donnant à suivre la cybersécurité d'environ 15 000 opérateurs utiles à la cyber-résilience du pays, c'est-à-dire non seulement des entreprises et des administrations mais aussi des collectivités locales. En effet, si le service informatique d'une commune ou du conseil départemental est bloqué, tout s'arrête. Or, l'investissement en cybersécurité représente 10 % du montant de l'investissement total en informatique. En revanche, un sabotage des systèmes d'information représenterait entre 200 000 euros et 300 000 euros de remédiation, au moins. En outre, les investissements de remise à niveau en cybersécurité demeureraient à faire, car les cybercriminels n'hésitent pas à revenir là où c'est facile. Pour une entreprise, la remédiation d'une attaque qui arrête les systèmes d'information, c'est la perte de 10 % du chiffre d'affaires. On parle donc bien d'un impact extrêmement important.

Un autre service rattaché au SGDSN est l'opérateur des systèmes d'information interministériels classifiés.

Enfin, le dernier-né des services rattachés au SGDSN est VIGINUM, chargé de la détection et de la caractérisation des ingérences numériques étrangères, c'est-à-dire la manipulation de l'information menée par des entités ou des États étrangers contre nos institutions, notre démocratie et notre équilibre sociétal. Nous ne nous occupons évidemment que des ingérences numériques étrangères d'origine étrangère, ce qui suffit largement à occuper ce service, déjà très sollicité avec les jeux Olympiques et Paralympiques, le rapport sur les activités en la matière de l'Azerbaïdjan sorti lundi, les difficultés que nous avons pu rencontrer avec le projet russe Lakhta au Sahel ou encore l'ensemble des attaques qui peuvent également être menées contre des entreprises.

Concernant les menaces hybrides, la pratique du *lawfare* - c'est-à-dire la capacité pour un État étranger à imposer l'extraterritorialité de ses lois et donc à imposer celles-ci en France — entre également en ligne de compte. Les réglementations *International Traffic in Arms Regulations* (ITAR) et *Export Administration Regulations* (EAR) des États-Unis sont connues dans ce domaine. Si un équipement américain relevant de la réglementation ITAR est compris dans votre matériel, vous devez demander l'autorisation des Américains pour pouvoir l'utiliser.

Les Chinois recopient, presque mot à mot, l'ensemble de cette réglementation. Ainsi, de nombreux contrôleurs chinois veulent venir visiter nos entreprises stratégiques ou essentielles à notre puissance économique pour contrôler que l'activité y correspond aux lois chinoises et avoir accès à certains secrets de nos entreprises.

La loi de blocage de 1968, revue et améliorée, permet d'entraver ce type d'action, ce que nous nous efforçons de faire. Toutefois, en matière d'économie en guerre, ces capacités des États étrangers à venir vérifier dans nos entreprises la conformité à leurs propres règles posent évidemment un problème de souveraineté et d'équilibre. Il faudra que nous

puissions avancer et continuer à protéger au niveau français, mais aussi européen avec les directives qui sont en cours, la capacité de nos entreprises à résister à cela. L'arrivée de la prochaine administration Trump devrait encore renforcer cette nécessité.

Pour éviter de renseigner nos adversaires, le dispositif de sécurité des activités d'importance vitale est classifié. Il regroupe plusieurs centaines d'opérateurs d'importance vitale qui sont répartis en 12 secteurs d'activité et près de 1 500 points d'importance vitale. Ils sont soumis à des obligations spécifiques de sécurité physique, périmétrique et de cybersécurité. Ainsi, ils doivent non seulement être en état de résister à des attaques, des sabotages ou des tentatives d'espionnage mais aussi d'éviter de se retrouver confrontés à des crises environnementales, des inondations ou des feux de forêt.

La directive européenne « Résilience des entités critiques » (REC), dont le projet de loi de transposition est actuellement entre les mains de la Haute assemblée, permettra aussi de renforcer, sur la base de nos préconisations, la sécurité de nos entreprises dans ce domaine.

Demain, les opérateurs devront réaliser une cartographie de leurs vulnérabilités d'approvisionnement. L'économie de flux tendus ayant été remise en question par la crise liée à l'épidémie de Covid-19 puis par la guerre en Ukraine, nos entreprises doivent se protéger et un système d'approvisionnement leur permettant de ne plus dépendre d'un seul État ami ou partenaire. En effet, dans ce domaine, les États ne sont pas toujours des amis ou des partenaires. Il est donc nécessaire que nous opérions une diversification des sources d'approvisionnement, une relocalisation de production à l'intérieur de notre pays et que nous ayons la capacité à pouvoir chercher partout l'énergie qui nous est nécessaire mais aussi les matières premières ou les terres rares. La disposition nécessaire pour pouvoir se mettre en guerre et tenir collectivement et solidairement dans la durée se situe au niveau national, mais aussi au niveau européen.

Ces éléments apparaissent dans la stratégie nationale de résilience que je vous avais présentée à nouveau au mois de juin dernier. Forte de 73 actions, cette stratégie comprend aussi un volet économique pour nous redonner une épaisseur stratégique, et ainsi pouvoir absorber le premier choc et réagir à la crise.

Nous avons aussi, dans ce cadre, des plans de continuité d'activité pour lesquels le SGDSN a rédigé un guide *ad hoc* à disposition de tous les types d'entités, en plus de l'animation du dispositif du plan de suivi des plans de continuité du côté de l'État.

Nous essayons aussi de faire en sorte que l'ensemble de nos concitoyens ne soient pas seulement consommateurs de sécurité mais aussi acteurs de leur sécurité dans différents domaines, ce qui signifie qu'il faut que nous puissions réfléchir à la mise en place des stocks stratégiques mais également de réserves nécessaires pour que nos entreprises puissent fonctionner.

Dans les plans des opérateurs d'importance vitale, il y a un plan de rappel de leurs ingénieurs et de leurs acteurs essentiels à la sécurité de l'entreprise. Ce sont souvent des volontaires ayant déjà exercé auparavant des fonctions de militaire, de policier, de gendarme ou encore d'infirmier. Si, un jour, nous nous retrouvons confrontés à une crise, nous demanderons à ces volontaires de rejoindre l'hôpital, les armées ou de rester dans leur entreprise afin d'assurer son bon fonctionnement. Nous voudrions constituer une forme de recensement, à partir de chaque département, avec la possibilité de remonter au niveau national pour identifier les compétences et les volontariats — tout ceci ne pouvant fonctionner que sur le volontariat — afin d'organiser un dispositif nous permettant, en fonction de la nature, de l'étendue et de la « systémicité » de la crise, de déterminer avec l'ensemble des

autorités comment affecter ces réservistes, avec l'accord de l'intéressé, au bon endroit et au bon moment.

Nous souhaitons travailler sur ce point absolument majeur avec la garde nationale et le ministère des armées et des anciens combattants. Nous avons commencé à y réfléchir dans le cadre de l'exercice ORION 23 et nous continuerons à y réfléchir pour préparer le prochain car c'est, en termes d'efficacité opérationnelle, un point absolument essentiel. Quand nos armées ont besoin de bouger vite d'un endroit à un autre, les camions militaires ou les moyens de transport militaires peuvent certes être utilisés mais les logisticiens du secteur privé sont aussi parfaitement capables de nous trouver les trains, les camions et, le cas échéant, les bateaux pour pouvoir aller d'un point à un autre vite et bien, en ayant parfaitement réglé ce genre de sujet.

Il faut que nous arrivions à mettre en place ce type d'initiatives pour essayer de renforcer notre capacité à faire face à une économie de guerre. Nous aurons beaucoup à faire sur ce sujet, même si nous avons déjà assez bien commencé à agir, avec l'exercice ORION 23, nos avancées concernant ce sujet des réserves et le début du travail des opérateurs d'importance vitale concernant les stocks stratégiques. Il reste que nous avons encore un certain nombre de vulnérabilités.

Je rappelle la bonne nouvelle que représente le rachat d'Alcatel Submarine Network par l'État, en faveur duquel le SGDSN s'est beaucoup battu. Ce groupe, appartenant auparavant à Nokia, fait partie des trois seules entreprises de la planète spécialisée dans la fabrication, la maintenance et la pose de câbles sous-marins. Les deux autres entreprises pratiquant également cette activité sont respectivement chinoise et américaine. Ce rachat est donc essentiel pour notre souveraineté et notre capacité à pouvoir faire travailler Orange avec nous sur ce sujet.

Un autre sujet, sur lequel nous ne sommes en revanche pas encore tout à fait au point, mais sur lequel nous travaillons, est le rachat en cours par une société chinoise de la dernière entreprise française qui produit de la vitamine D et des acides aminés pour l'alimentation du bétail en Europe. Elle compte environ 80 salariés et est située dans l'Allier, à Commentry. Évidemment, ce projet de rachat nous interpelle et nous amène à considérer qu'il faudrait trouver le moyen de garder le contrôle de ce type d'entreprise de façon à ne pas nous retrouver dépendant d'un État étranger qui, le jour venu, peut décider de « fermer le robinet ».

Nous sommes vraiment engagés afin d'avancer et de progresser sur le sujet.

Néanmoins, pour qu'une économie de guerre puisse fonctionner et pour que nos armées puissent faire le travail, du financement est nécessaire. Libérer le financement des contraintes réputationnelles est aujourd'hui un des enjeux extrêmement importants auxquels il faut que nous puissions nous attaquer. Les petites et moyennes entreprises (PME) et les entreprises de taille intermédiaire (ETI) de la BITD font régulièrement état de difficulté de financement, non pas en raison de réglementations internationales puisque l'Union européenne a interrompu les projets de taxonomie sur le sujet mais en raison d'une prudence des banques qui, au titre de leur réputation, ne veulent pas se faire accuser d'avoir prêté de l'argent à une entreprise qui produit de l'armement. Des entreprises se retrouvent donc interdites de crédit par les banques pour de plus ou moins bonnes raisons et risquent de couler, même si seulement 5 à 10 % de leur activité concernent la défense nationale. Les groupements industriels dans les industries d'armement font en sorte de les soutenir mais un problème est clairement en train de se poser. Ce dernier est spécifique à la France parce qu'au

Royaume-Uni, aux États-Unis, en Allemagne ou en Italie, la question ne se pose pas. Ce vrai sujet réputationnel doit être traité afin de créer un environnement permettant l'investissement dans la BITD, tant au niveau national qu'au niveau européen. Ce sont les sujets de taxonomie sur lesquels nous travaillons. Dans ce domaine, il y aura effectivement beaucoup à faire.

En outre, concernant le financement, un certain nombre de dispositifs nationaux et européens existent et sont en train de fonctionner. La procédure dite « article 90 » est un dispositif autofinancé qui prévoit d'apporter un soutien financier aux entreprises dans leurs travaux d'industrialisation de matériel de guerre et de prospection commerciale dans une perspective d'exportation. Cette procédure représente 63 millions d'euros. Le gouvernement accorde des avances remboursables au fur et à mesure des ventes, selon des critères cumulatifs. Les matériels produits exportés doivent être classés matériel de guerre lorsque c'est nécessaire à la protection des intérêts essentiels de la sécurité de l'État. De plus, le siège social des entreprises et les unités de production de matériel doivent être situés en France. Les contrats d'avance remboursable sont conclus entre les entreprises bénéficiaires et Bpifrance et peuvent s'élever jusqu'à 65 % du montant des travaux d'industrialisation et de prospection éligibles. Évidemment, ce dispositif concerne les PME, les très petites entreprises (TPE) et les ETI.

Un autre mécanisme est le fonds soutenant l'innovation par le ministère des armées et des anciens combattants, finançant la recherche et le développement maintenant un savoir-faire. Le projet de loi de finances (PLF) 2024 prévoyait pour les études amont plus de 1 milliard d'euros à cette fin.

Il existe aussi des dispositifs et des mécanismes européens.

Je vous parlais d'une moindre frilosité au niveau européen, sauf peut-être à la Banque européenne d'investissement (BEI), où nous poussons l'élargissement du champ d'intervention de la banque au bénéfice des secteurs industriels de la défense, alors que celle-ci, jusqu'à présent, était réticente à élargir son activité au-delà des activités duales.

L'Union européenne s'est par ailleurs dotée d'un fonds européen de défense avec un budget de 8 milliards d'euros sur la période 2021-2027 pour favoriser la coopération entre entreprises et centres de recherche au niveau européen, pour renforcer la compétitivité, l'efficacité et la capacité d'innovation de notre base industrielle de défense européenne.

Dans le cadre de la mise en place de la stratégie industrielle européenne de défense, dite EDIS, un nouveau règlement baptisé E*uropean Defense Investment Program* (EDIP) est en cours d'élaboration afin de renforcer l'autonomie, la résilience et la compétitivité de la BITDE. Plusieurs points visent à soutenir l'industrie de défense, tels que l'acte de soutien à la production de munitions (ASAP), initié en mars 2023 avec 500 millions d'euros. La somme a été débloquée en mars 2024 et 31 projets provenant de 15 pays, dont la France, vont être soutenus.

Un autre instrument, destiné à aider l'industrie de défense au moyen d'acquisitions conjointes, est l'*European Defense Industry Reinforcement Through Common Procurement Act* (EDIRPA), adopté par le Conseil et le Parlement en octobre 2023 et s'élevant à 310 millions d'euros pour financer des projets conjoints dans les munitions, la défense aérienne et antimissile ainsi que les systèmes et plateformes héritées. La Commission a annoncé que cinq projets avaient été sélectionnés.

Dans tous ces domaines, nous veillons à ce que l'Union européenne prenne bien en compte la nécessité de favoriser l'industrie européenne. Pour l'instant, le règlement prévoit

qu'il faut au minimum 65 % de composants conçus dans l'Union européenne dans la valeur du produit final des matériels, les 35 % restants pouvant bénéficier à des entités extra-européennes. Il a fallu que nous nous battions pour avoir ces 65 %, puisque certains pays considéraient que 50 % auraient pu suffire. Lorsque je discute avec mes homologues dans différents pays, ils se disent qu'il faut acheter beaucoup d'armement à tel ou tel pays — et je pense plutôt à un pays —, pour compenser le fait que ces pays ne sont pas encore au 2 % du produit intérieur brut (PIB), et qu'il vaut donc mieux acheter beaucoup. Je leur réponds que nous allons tuer notre industrie de défense et perdre notre souveraineté, à ce compte.

La France soutient l'idée qu'un bonus puisse être accordé aux matériels dépassant ce seuil de 65 %, à défaut d'avoir réussi à atteindre le seuil de 80 %. En outre, elle demande que la définition de l'autorité de conception soit également prise en compte, pour que le savoir-faire et les droits de propriété industrielle de nos États puissent être respectés, et donc qu'il soit enfin impossible de recourir à des composants provenant de pays tiers, si des alternatives issues d'États membres existent.

En termes de sécurité et d'approvisionnement, nous sommes aussi en train de travailler sous l'angle européen.

Le SGDSN est donc le bouclier et veille à ce que les entreprises se protègent elles-mêmes et assurent un minimum de protection dans la mesure où elles concourent à la souveraineté de l'État ou à la défense des intérêts fondamentaux de la Nation. Nous veillons également à ce qu'existe une bonne coopération au niveau européen.

M. le président Jean-Michel Jacques. Je vous remercie pour cette présentation. Je cède la parole aux orateurs de groupe pour leurs questions.

Mme Stéphanie Galzy (RN). Monsieur le secrétaire général, le rôle de votre mission est d'anticiper, de prévenir et de protéger. Il s'agit d'une mission ô combien importante. Dans un contexte mondial incertain, l'économie de guerre reprend une nouvelle dimension avec l'essor de la cyberdéfense et de l'espionnage industriel.

Alors que les conflits traditionnels sont toujours présents, une autre guerre se déroule dans l'ombre, où nos entreprises deviennent des cibles. En plus d'être créatrices d'emplois, elles détiennent également des données sensibles. Les cyberattaques peuvent viser à voler des informations, à compromettre des systèmes ou à saboter des opérations. Les conséquences économiques peuvent être gravissimes, allant de pertes financières directes à des atteintes à la réputation.

D'un autre côté, l'espionnage économique est une réalité, à laquelle les entreprises doivent faire face. Des acteurs, étatiques ou non, cherchent à obtenir des informations sur les innovations technologiques et notre savoir-faire.

La protection des entreprises contre l'espionnage et les cyberattaques est essentielle pour garantir non seulement leur survie, mais aussi la stabilité économique de ce secteur. La cybersécurité est aujourd'hui un pilier central de la stratégie économique de ces entreprises. C'est un enjeu majeur pour l'avenir de notre économie et de notre sécurité.

Afin de garantir la compétitivité et la sécurité de nos entreprises, quelles mesures mettez-vous en place pour les aider et quelle est votre vision sur cette problématique pour les années à venir ?

M. Stéphane Bouillon, **secrétaire général de la défense et de la sécurité nationale**. Pour protéger la compétitivité de nos entreprises face aux menaces hybrides, notre

principe est vraiment celui du bouclier. Nous nous assurons que la règle du jeu est respectée par nos compétiteurs et qu'il n'y a pas un détournement de procédures à leur encontre. Par exemple, lorsque des marchés publics sont ouverts par des entreprises publiques, nous veillons à ce que soient admises à l'appel d'offres des entreprises venant de pays qui ont passé des accords commerciaux avec la France. S'il n'y a pas d'accord commercial, nous pouvons très bien dire à ces entreprises qu'elles ne sont pas autorisées à participer à ce marché. Cela a été fait à plusieurs prises, par exemple pour des équipements de sécurité dans des aéroports. Il s'agit d'une disposition européenne, transcrite dans le droit français, qui fonctionne. Nous veillons vraiment à ce que la règle du jeu soit totalement respectée et que nous nous trouvions ainsi à égalité de compétition et de concurrence entre les uns et les autres.

Le deuxième élément en matière de protection de la compétitivité des entreprises est d'essayer à notre niveau de faire en sorte que les règles, y compris celles que nous imposons ou qui sont imposées au niveau européen, le soient avec discernement et intelligence. Nous essayons de faire en sorte que l'objectif soit atteint, mais d'éviter que les différentes administrations, au fur et à mesure, ne sur-appliquent pas une règle pour protéger les fonctionnaires chargés de la faire respecter. Il ne faut pas se tromper d'objectif.

Par exemple, lors des premiers mois de la crise sanitaire liée à la pandémie de Covid-19, nous disposions de masques qui étaient considérés comme périmés car leurs élastiques, ayant plus de cinq ans, risquaient de se rompre. Il a alors été recommandé de ne pas se servir de ces masques parce que des fonctionnaires chargés de cette question avaient peur qu'une personne contaminée par la Covid-19 se retourne contre l'administration en raison d'un élastique défectueux. Nous nous sommes donc retrouvés dans une situation où il était interdit de se servir des masques et où nous étions exposés au virus. À l'époque, j'étais au ministère de l'Intérieur, je suis passé outre et j'ai pris la décision de distribuer les stocks de masques dont nous disposions. Je reconnais que, lors d'une réunion à l'Élysée, l'élastique de mon masque s'est rompu. Je l'ai alors mis dans ma poche et j'en ai sorti un autre.

La compétitivité, c'est parfois du bon sens.

M. Thomas Gassilloud (EPR). Monsieur le secrétaire général, je suis ravi de vous recevoir à nouveau dans cette commission, pour nous rappeler la pertinence de notre Constitution, et notamment de l'article 21, disposant que le Premier ministre est responsable de la défense nationale. Je crois que ce rappel est plus que jamais pertinent au regard des menaces, notamment hybrides, auxquelles la Nation est confrontée.

Je suis également ravi que vous puissiez nous sensibiliser à nouveau sur l'importance du SGDSN, qui gère des domaines extrêmement vastes, à savoir le cyber au travers de l'ANSSI, la gestion du secret du champ informationnel avec VIGINUM, l'espace, la sûreté nucléaire ou encore le suivi des *opérateurs d'importance vitale*.

Ces éléments exigent de nous, parlementaires, une grande responsabilité, notamment en tant que membres de la commission de la défense. Aujourd'hui, il nous sera présenté une motion de censure. Or, face aux menaces à 360 degrés qui nous guettent et à l'instabilité du monde, chacun d'entre nous est appelé à assumer ses responsabilités, pour savoir s'il nous faut ajouter de l'instabilité et du retard dans les décisions, notamment de mise en œuvre de la LPM, et s'il est pertinent de revenir sur les 3 milliards d'euros d'augmentation de crédit prévus dans le PLF 2025 — visant à poursuivre la modernisation de notre dissuasion, lancer le chantier du porte-avions de nouvelle génération et améliorer la protection de nos soldats de l'armée de terre avec le programme Scorpion — ou de revenir sur les 700 recrutements et 100 millions d'euros prévus pour la revalorisation des soldes.

Mes chers collègues, depuis 2018, en tant que membres de l'ensemble des groupes politiques, nous avons toujours veillé au respect à l'euro près des deux LPM. En cas de censure, cette marche de 3 milliards d'euros prévue dans le budget 2025 serait probablement perdue. Nous sommes tous des patriotes préférant l'intérêt de notre pays à l'intérêt de nos partis. Nous avons donc chacun un rôle à jouer pour sensibiliser nos groupes politiques aux graves conséquences en matière de défense en cas de censure du gouvernement.

Monsieur le secrétaire général, pourriez-vous évoquer l'importance de la commission interministérielle de défense nationale (CIDN), créée pour une meilleure coordination des efforts interministériels sur les questions de défense, et l'avancée de ses travaux ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. La CIDN, présidée par le Premier ministre ou son directeur de cabinet, rassemble l'ensemble des ministères concernés pour vérifier que chacune des administrations assure l'essentiel de ses responsabilités en matière de protection pour faire face à une crise, à savoir un plan de continuité d'activité, une organisation de la cybersécurité dans leurs locaux et la formation des cadres et des agents à la gestion de crise.

Ce dernier point est motivé par le fait que, si les experts sont formés, les dirigeants du ministère, qui seront à la manœuvre en cas de crise, ne le sont pas toujours. Il faut s'assurer que ces personnes sont formées à la gestion de crise et qu'une relève est assurée si la crise dure plusieurs semaines.

Une commission est réunie en principe chaque année.

M. Christophe Bex (LFI-NFP). La guerre en Ukraine a souligné qu'une armée doit agir avec les moyens et l'industrie dont elle dispose. Lorsque le conflit s'engage, il faut faire avec ce que nous avons, et non avec ce que nous souhaitons. Cette situation nous impose d'être en mesure d'anticiper une capacité de réaction en cas de dégradation rapide des relations internationales.

Pour cela, nous avons besoin d'une stratégie et d'une politique industrielle de défense permettant d'avoir la profondeur industrielle nécessaire pour accompagner les forces armées, non seulement par la qualité des matériels fournis, mais aussi par la capacité à les approvisionner dans la durée.

Pourtant, après l'invasion de l'Ukraine par la Russie, nos décideurs ont eu l'air surpris par la longueur des délais nécessaires pour augmenter la production de matériel militaire. Selon les derniers rapports parlementaires, la France n'aurait pas les munitions suffisantes pour tenir plus de quelques semaines seulement à un conflit de haute intensité.

Le passage à une économie de guerre demandée par Emmanuel Macron en 2022 s'annonce donc de plus en plus difficile. L'utilisation de ce concept n'a aucune valeur quantifiable. À partir de quel moment peut-on considérer que nous sommes en économie de guerre ? Lorsque la population est massivement mobilisée dans l'industrie de l'armement ? Lorsque la taille et l'ampleur des moyens et des opérations conduisent à un niveau de dépenses incomparable avec un temps de paix ? Ou lorsque l'industrie mobilisable est effectivement mise au service des armées ? La France ne coche aucune de ces cases. Mais le souhaitons-nous réellement ?

Alors que des plans sociaux menacent des milliers d'emplois dans des secteurs stratégiques de la défense, notamment l'espace, avec 1 000 emplois menacés chez Thales

Alenia Space et 2 500 emplois menacés chez ADS, pouvez-vous nous dire si toutes les actions sont prises afin de garantir une stratégie d'armement sur le long terme ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. En 2022, il est clair que notre armée n'était pas prête à faire face à une guerre de longue durée et dans les conditions dans lesquelles celle-ci s'est engagée, avec le retour des conflits à haute intensité. Nous étions en train de profiter des « dividendes de la paix » et personne ne s'attendait à ce qu'un État, qui avait signé tous les traités de paix depuis 1945, puisse utiliser sa puissance nucléaire pour imposer aux uns et aux autres de ne pas bouger et attaquer un État indépendant et souverain.

Notre dissuasion nucléaire efficace et performante a été importante pour faire baisser un peu le ton.

Il a fallu se réadapter. En effet, la LPM qui a été votée prévoit toute une série d'investissements, d'aménagements et de réorganisations pour se préparer aux situations de guerre que nous connaissons.

Comme vous, je ne souhaite surtout pas que l'économie de guerre implique une mobilisation de l'ensemble des entreprises et des économies, avec 20 ou 30 % du PIB au profit des armées, comme en Russie, et des difficultés pour le reste de la société, notamment en raison de l'inflation. Il faut donc anticiper.

Nous devons pouvoir continuer à aider nos entreprises à investir, à disposer de matériel suffisant et à pouvoir réagir dans le cadre d'une alliance. Nous ne sommes pas seuls puisque nous faisons partie de l'Organisation du traité de l'Atlantique nord (OTAN) et de l'Union européenne. Des dispositifs de défense sont mis en place pour que nous puissions avoir une coordination et une cohérence dans les moyens entre les uns et les autres. Une répartition et un partage de l'effort doivent donc être décidés entre alliés afin de jouer efficacement cette capacité à réagir.

Tout notre objectif est de faire en sorte que nos entreprises continuent à produire et à créer de l'emploi, parce que c'est non seulement une question de souveraineté pour notre État, mais aussi car ces entreprises constituent des employeurs extrêmement importants pour la vie quotidienne sur nos territoires.

J'ajoute également qu'en matière de recherche et développement (R&D), tous les travaux qui peuvent être engagés sont également particulièrement importants pour diffuser une recherche de qualité qui servira à l'ensemble de l'économie civile.

Mme Isabelle Santiago (SOC). Nous vous rejoignons bien évidemment sur l'importance d'une diffusion de culture de la continuité d'activité auprès de l'ensemble des acteurs, publics comme privés.

Or l'étude ImpactCyber, dont les résultats ont été publiés en octobre dernier, a dressé un état des lieux préoccupants du niveau de maturité cyber des PME et des TPE. Nous savons que les 4 000 entreprises de la BITD, dont 1 600 sont considérées comme critiques, font partie des cibles prioritaires. M. Emmanuel Chiva, délégué général pour l'armement, a d'ailleurs dit dans une récente commission que les cyberattaques augmentaient significativement et qu'elles étaient surtout liées à des intérêts de nos compétiteurs dans les domaines particuliers, comme le spatial et le naval. Évidemment, ces questions ont été abordées dans le cadre de la LPM et de tous les sujets que nous avons évoqués ces derniers temps.

Le 15 octobre dernier, le gouvernement a présenté le projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier. Ce projet de loi vise à transposer trois textes. Une commission spéciale avait été mise en place au Sénat. Pouvez-vous revenir sur les mesures préconisées ? Dans quelles mesures permettront-elles d'accompagner les entreprises de la BITD afin d'améliorer leur résilience et leur maturité cyber ?

Par ailleurs, dans son avis du 6 juin 2024 sur le projet de loi, le Conseil d'État relevait que la charge reste un défi, en termes financiers mais aussi en compétences à acquérir, pour les entités qui devront s'identifier elles-mêmes et se mettre en conformité. Pouvez-vous revenir sur ce qui est envisagé pour aider nos TPE, sachant que tous ces points ont été abordés souvent dans le cadre de la LPM ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Je partage évidemment fondamentalement votre préoccupation sur le niveau de maturité dans les PME et les TPE.

Nous avons créé des *Cyber Incident Response Teams* (CIRT) régionaux, c'est-à-dire des centres régionaux d'alerte et de soutien aux entreprises, en dotant les conseils régionaux qui le souhaitaient de moyens pour mettre en place ces dispositions. À travers la stratégie cyber, nous souhaiterions beaucoup pouvoir continuer ce travail et les aider à avancer car, dans le cadre de ses responsabilités économiques, la région doit pouvoir jouer un rôle non seulement éducatif, mais aussi d'accompagnement physique des entreprises pour pouvoir avancer. La gendarmerie, à travers son commandement dans le cyberespace (COMCyberGEND), mène aussi des actions. De plus, nous essayons de travailler avec les chambres de commerce et d'industrie pour informer les chefs d'entreprise et les pousser à renforcer leur cybersécurité.

L'investissement revient aux entreprises et représente environ 10 % du coût global des systèmes d'information.

Toutefois, ce qui compte pour un certain nombre d'autres entreprises, ce sont les mesures d'hygiène, à savoir changer régulièrement les mots de passe, faire en sorte que des personnes ne puissent pas approcher des équipements, organiser une forme d'étanchéité entre les différents systèmes ou encore s'assurer de l'existence de redondances et de sauvegardes. Dans la plupart des cas, ces mesures d'hygiène suffisent, notamment pour les petites entreprises et collectivités locales.

La directive REC concerne les opérateurs d'importance vitale, c'est-à-dire les grosses structures auxquelles nous demandons de faire des efforts et, en tant qu'entité essentielle, nous leur demanderons également d'essayer de garantir et d'améliorer la sécurité de leurs infrastructures informatiques. Pendant les jeux Olympiques et Paralympiques, nous avons aidé les principaux partenaires à s'organiser, se protéger et se renforcer pour faire face à la situation.

Concernant NIS 2, toute une série de mesures est prévue en matière de dispositifs de détection des attaques, de pare-feu et d'architecture de sécurité des systèmes. Nous jouons beaucoup sur l'aspect technique, de façon intelligible par un chef d'entreprise, mais aussi sur l'aspect éducatif et le conseil.

Enfin, nous avons aussi, notamment pour les très gros acteurs, la capacité à infliger des sanctions si ceux-ci n'ont pas fait les investissements nécessaires. La sécurité

informatique, c'est un peu comme quand vous imposez des barreaux aux fenêtres, des verrous aux portes et un coffre où ranger vos biens les plus précieux. Les intéressés doivent faire ces efforts. Ils en seront les premiers bénéficiaires.

Concernant les petites collectivités, la dotation de soutien à l'investissement local (DSIL) et la dotation d'équipement des territoires ruraux (DETR) peuvent évidemment apporter leur concours aux investissements qui seront décidés par les élus locaux dans ce domaine.

Mme Valérie Bazin-Malgras (DR). Dans un contexte international marqué par des tensions géopolitiques croissantes, la notion d'économie de guerre revient au cœur des réflexions stratégiques françaises et européennes. Cette nouvelle donne exige une adaptation rapide et efficace de notre modèle industriel et logistique pour répondre aux exigences d'un conflit de haute intensité.

Tout d'abord, comment l'État anticipe-t-il la montée en puissance de notre industrie de défense pour garantir une production rapide et suffisante d'équipements critiques en cas de besoin ?

Ensuite, quelles sont les mesures concrètes mises en place pour sécuriser nos chaînes d'approvisionnement, notamment dans les secteurs technologiques nécessitant des matières premières stratégiques, pour lesquels notre dépendance à des pays tiers demeure préoccupante ?

Enfin, face aux enjeux de recrutement et de formation dans les filières liées à la défense, comment le SGDSN accompagne-t-il la mobilisation des compétences humaines indispensables pour garantir notre autonomie stratégique et soutenir l'effort national ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Concernant l'anticipation de la montée en puissance, deux points entrent en ligne de compte : le souhait des entreprises d'effectuer de la R&D et la nécessité de pouvoir produire de la quantité.

Pour produire, ces entreprises doivent avoir des commandes, étalées dans le temps, d'où l'importance de la LPM et des moyens qui, chaque année, sont mis à sa disposition afin de garantir aux entreprises qu'elles pourront effectuer les investissements nécessaires sur les chaînes d'approvisionnement. Cela a été le cas pour le CAESAR et le Rafale de Dassault. Il faut maintenant que nous continuions à le mettre en œuvre pour bon nombre d'autres entreprises.

Concernant les mesures concrètes pour sécuriser nos chaînes d'approvisionnement, tout notre objectif est de diversifier les approvisionnements. Par exemple, un délégué interministériel aux métaux rares a été mis en place et vise à regarder où se trouvent les métaux indispensables pour nos technologies. Pour l'instant, l'essentiel de ces métaux se trouve en Chine. Le délégué interministériel va essayer de regrouper l'ensemble des entreprises pour aboutir à une vision globale des besoins, afin d'être davantage en position de pouvoir discuter, négocier et obtenir des contrats avec différents États étrangers ; l'objectif étant surtout d'éviter de se retrouver dépendant d'un seul et même État le moment venu. Il s'agit d'un travail concret sur lequel nous avançons et sur lequel nous essayons, avec les uns et les autres, de trouver la solution le plus vite possible.

Par ailleurs, nous rencontrons effectivement des difficultés pour recruter des professionnels dans les différentes administrations.

C’est moins le cas à l’ANSSI, qui a une telle réputation en matière de cyberdéfense que les *geeks* sont très heureux de venir y travailler, y compris en sortie d’études. En effet, même si la rémunération y est plus basse que dans le privé, ils y acquièrent une compétence et une réputation qui leur permet, après quelques années, de valoriser ce dispositif dans le privé.

Il n’en demeure pas moins que notre pays connaît des difficultés de féminisation des métiers du numérique et, d’une manière plus générale, d’attractivité, notamment dans les petites entités ; les mêmes qui ont pu être victimes de cyberattaques. Beaucoup d’entités victimes n’avaient pas suffisamment investi, d’un point de vue technique mais également en matière d’experts et de sachants permettant de faire fonctionner ce dispositif.

Nous devons impérativement parvenir à remonter le niveau de recrutement ainsi que le niveau d’investissement. C’est pourquoi le plan CaRE a été mis en place par le ministère de la santé et de l’accès aux soins, à hauteur de 150 millions d’euros cette année encore, pour aider les hôpitaux à pouvoir se protéger et donc à investir dans ce domaine. La question des ressources humaines sera majeure.

M. Damien Girard (EcoS). Les dommages causés à des câbles sous-marins dans les eaux suédoises de la mer Baltique, les 17 et 18 novembre, nous rappellent la vulnérabilité de ces infrastructures. Plus largement, les fonds marins sont de plus en plus de réels terrains de rapports de force. Ce sont autant des espaces d’échanges et de commerce que des réserves de ressources. Du gaz, du pétrole, de l’électricité, des parcs éoliens ainsi que des connexions à Internet et des échanges d’informations en tout genre s’y trouvent en quantité importante.

Plusieurs innovations et ruptures technologiques conduisent ces fonds sous-marins à devenir un terrain accessible jusqu’à 6 000 mètres de profondeur. Les forces armées des États-Unis, de la Chine ou encore de la Russie développent des moyens concrets pour accroître leur capacité d’action.

La marine nationale considère également ce secteur comme un domaine prioritaire, alors que notre pays possède le deuxième domaine maritime au monde. Ce chantier comporte de multiples dimensions : renseignements, protection des infrastructures, lutte anti-sous-marine, drones, sous-marins, mines, recherche scientifique ou encore gestion des ressources. Le ministère des armées s’est saisi de ce sujet avec sa stratégie de maîtrise des fonds marins de février 2022. J’ai également eu l’occasion d’interroger le délégué général pour l’armement dans le cadre de cette commission sur la montée en puissance de nos capacités en la matière. De même, la nationalisation par l’État de la société de production et de pose de câbles Alcatel Submarine Network est une nouvelle à saluer.

Le besoin d’un cadre stratégique complet demeure cependant. Quelle approche publique globale construire dans le cadre de la notion d’économie de guerre pour s’assurer que la France demeure souveraine, sur les plans militaires mais aussi scientifiques, économiques et écologiques, au sujet de ces fonds marins ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Le sujet des fonds marins est en effet un enjeu de compétition internationale, qui est véritablement en train de monter en vigueur.

Pour le moment, nous ne savons pas encore si l’arrachage des câbles sous-marins par le bateau chinois dans la mer Baltique a été volontaire ou involontaire. L’enquête est toujours en cours et je ne peux donc pas préjuger du résultat. Il n’en demeure pas moins que cela fait plusieurs fois que des câbles sont arrachés dans cette mer et que cela commence à

faire beaucoup. Des câbles sont également arrachés entre le Royaume-Uni et le continent ainsi que dans différents autres endroits.

La solution sur ce sujet est évidemment la redondance et la multiplication des câbles. Entre la Suède et l'Allemagne, le trafic a été interrompu quelques microsecondes. Nous essayons d'investir, y compris au niveau européen, pour multiplier les câbles et, par exemple, disposer d'un câble qui fera le tour de l'Afrique et évitera ainsi de passer par le canal de Suez et la Mer rouge, passages assez risqués.

De la même manière, la LPM investit dans des robots qui doivent permettre de descendre à 6 000 mètres de profondeur. Les armées sont d'ores et déjà en train d'avancer sur ce point.

En outre, nous regardons les questions de droit international. La France s'oppose farouchement à l'exploitation des nodules marins ou à grande profondeur, qui représenterait un risque absolument considérable pour notre planète. Nous essayons donc, à travers toutes les instances internationales, de faire veiller à cette « sanctuarisation » de ces fonds marins. Faire en sorte que ce qui est aujourd'hui une terre préservée de toutes les ambitions et de tous les problèmes de prospection puisse le rester serait peut-être déjà la première stratégie. Il faut que nous parvenions à y travailler avec l'Europe mais aussi au niveau international.

Au niveau national et européen, des groupes de travail sont mis en place pour réfléchir sur cette protection des grands fonds marins. Nous essayons d'éviter qu'ils se militarisent trop vite — ce qui est parfois un peu compliqué — et qu'ils deviennent un enjeu d'exploitation économique donnant lieu à des enjeux militaires.

M. Fabien Lainé (Dem). Je voudrais vous interroger sur la possible vulnérabilité de nos apports en matière d'hydrocarbures.

Durant l'été 2017, nous avons voté de bonne foi la loi n° 2017-1839 du 30 décembre 2017 mettant fin à la recherche ainsi qu'à l'exploitation des hydrocarbures et portant diverses dispositions relatives à l'énergie et à l'environnement. Il s'agit d'une loi d'exemplarité dont on peut comprendre le sens : une grande Nation européenne mettait fin à l'extraction de pétrole en France.

Nous avons ensuite connu la crise liée à l'épidémie de Covid-19 puis la guerre en Ukraine, qui ont révélé toute la vulnérabilité de nos pays quant aux apports de gaz et de pétrole. Or, en France, nous produisons sur notre sol 1 % de nos besoins nationaux. Nos armées ont à ce jour besoin de cette quantité pour fonctionner. Il semble peu probable que le pétrole synthétique ou l'électrification s'y substituent rapidement.

J'avais interpellé le président de la République lors de ses vœux aux armées à Mont-de-Marsan, dans ma circonscription, en janvier 2023. Il avait trouvé cette problématique intéressante. J'avais évidemment saisi le ministre des armées, qui s'est tourné vers le SGDSN.

Le pétrole que nous importons émet trois fois plus de CO_2 lors de son transport et de son extraction dans d'autres pays. Au regard des effets de cette loi, je constate que le mieux est l'ennemi du bien. Nous avons besoin d'améliorer notre autonomie stratégique et notre résilience. Quel est votre avis sur ce sujet ? Comment peut-on avancer ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Monsieur le député, vous me rappelez un vieux dossier, dont nous avions effectivement parlé à un moment. En effet, l'idée avait été d'utiliser ce pétrole, exploité

notamment dans le Sud-Ouest et en région parisienne, au bénéfice de nos armées. Un groupe de travail a été mis en place à cette époque, a conclu au fait que ce n'était pas rentable et n'est pas allé beaucoup plus loin. Rappelons que nous ne parlions pas encore d'économie de guerre mais de rentabilité. J'ai souvenir — mais je vérifierai — que cette option a été assez largement écartée par le ministère des armées, encore une fois pour des raisons de coût.

Faut-il remettre ce sujet sur la table ou, s'il y a une question de rentabilité, faut-il en tout cas garder la possibilité, en cas de crise d'approvisionnement, de pouvoir garantir l'utilisation d'un certain nombre d'approvisionnements minimaux en pétrole ? Oui, il faut sans doute que nous continuions à travailler sur cet aspect. Toutefois, nous n'y sommes pas encore.

Je ne résiste pas, par ailleurs, à vous dire que la décarbonation — c'est-à-dire pouvoir utiliser du matériel qui fonctionne à l'électricité en bénéficiant de notre parc de centrales nucléaires aujourd'hui et demain pour un certain nombre d'équipements, y compris militaires — est sans doute également un point sur lequel il faut que nous puissions continuer à travailler.

M. Loïc Kervran (HOR). Vous avez évoqué le rôle du SGDSN dans la sécurisation de l'économie et sa contribution pour accompagner « l'économie civile face à la guerre économique ».

La plateforme PLACE, par laquelle transitent les appels d'offres de l'État et des organismes de sécurité sociale, était gérée par une PME française ayant remporté de nombreux appels d'offres. Or, au printemps dernier, l'État a décidé de confier, en dehors de tout processus d'appels d'offres, la gestion de cette plateforme au groupe nord-américain CGI. Sur cette plateforme transitent les réponses financières mais aussi techniques de nombreux appels d'offres, notamment du ministère des armées et des anciens combattants. Les réponses à ces appels d'offres peuvent être relatives, par exemple, aux drones sous-marins ou à l'équipement GSM des hélicoptères.

Hier, en réponse à une question au gouvernement, Laurent Saint-Martin, ministre chargé du budget et des comptes publics, a malheureusement accumulé les contre-vérités sur ce sujet. Il a en effet parlé d'appels d'offres perdus par ATEXO, ce qui n'est pas le cas. Il a dit que CGI n'avait pas accès aux données, ce qui n'est pas le cas non plus. Je trouve dommageable, sur un sujet aussi sensible, de répondre ainsi à la représentation nationale.

J'aimerais savoir si, au SGDSN, vous avez connaissance de cette question et si vous avez pu mener des vérifications de nature à nous rassurer sur ce sujet.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Je crains, monsieur le député, de ne pas pouvoir vous faire une meilleure réponse que celle du ministre. En tout cas, nous n'avons pas été associés et nous ne sommes pas intervenus sur cet appel d'offres et sur le passage de la plateforme Place d'une entreprise française à une entreprise nord-américaine.

Il n'en demeure pas moins que l'ANSSI vérifie quand même, dans ce domaine, qu'un certain nombre de conditions préalables en matière de sécurité sont garanties. Je revérifierai avec l'ANSSI et je vous indiquerai si ses équipes ont été amenées à travailler sur ce point. Encore une fois, nous sommes tout de même conduits à vérifier assez régulièrement le respect de nos règles de sécurité.

M. Yannick Favennec-Bécot (LIOT). Concernant la protection de nos savoir-faire industriels et de notre patrimoine scientifique et technique, comment le SGDSN décline-

t-il concrètement, en lien avec la DGE et les responsables de l'industrie de défense, les engagements pris dans la LPM ?

Quel est l'état de la menace pesant sur les PME de la défense ? Comment sensibilisez-vous ces acteurs privés à la problématique des attaques d'entreprises étrangères hostiles ?

Comment la stratégie nationale de résilience adoptée en 2022 est-elle mise en œuvre, notamment avec les entreprises ?

Enfin, compte tenu de l'ampleur et de l'évolution des menaces, qu'attendez-vous du Parlement et quelles sont vos préconisations dans la perspective de la transposition de la directive REC ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Concernant la protection de nos savoir-faire industriels en liaison avec la DGE, un rapport a été rédigé il y a quelques mois par M. Geoffroy Roux de Bézieux, sur les conditions dans lesquelles la sécurité économique dans les entreprises pouvait être partagée et mieux infuser au sein des groupements d'entreprises. Il est intéressant que M. Roux de Bézieux ait occupé la fonction de dirigeant du Mouvement des entreprises de France (MEDEF), puisque certains dirigeants et entreprises n'ont pas toujours été sensibles à ces questions.

Dans ce domaine, la DGE dispose, à travers le comité interministériel de sécurité des entreprises de l'économie (CISSE), de représentants régionaux travaillant avec les préfets et les services de sécurité, notamment la direction générale de la sécurité intérieure (DGSI), pour aller voir les entreprises les plus sensibles et recenser les pépites, afin de s'assurer que les *minima* de sécurité sont mis en œuvre. Dans un certain nombre de cas, comme lorsque des entreprises ou des laboratoires sont sensibles, nous mettons en place de zones à régime restrictif (ZRR) afin que l'accès en soit contrôlé.

Ces éléments font effectivement partie de la manière de sensibiliser les PME rattachées à la défense. Les contrats passés par l'État avec un certain nombre d'entreprises contiennent des clauses particulières, imposant une certaine hygiène en matière de système informatique, des investissements de sécurité et la préservation de secrets d'affaires, afin d'éviter que ces entreprises constituent la porte d'entrée permettant aux prédateurs d'intervenir. Nous avons eu plusieurs mauvaises surprises dans ce domaine et nous sommes donc maintenant extrêmement attentifs sur ce sujet.

Le projet de loi que vous examinerez prochainement transpose les directives européennes REC, NIS 2 et DORA.

Je suis moins inquiet sur la directive DORA, relative aux services financiers, car ces entreprises, qui connaissent les coûts des attaques dans leurs systèmes, investissent assez largement pour faire le nécessaire. Avec l'ANSSI et le système Place de Paris, nous faisons assez régulièrement du *bounty hacking* pour vérifier que tout cela tient, ce qui est le cas.

Nous avons beaucoup contribué à la rédaction des textes REC et NIS 2 pendant la présidence française en 2022. La directive REC s'inspire du dispositif des opérateurs d'importance vitale, qui existait en France et que nous avons partagé à nos alliés européens. En outre, concernant NIS 2, l'ANSSI a été souvent sollicitée car elle est l'une des agences de cybersécurité les mieux préparées pour faire avancer ce sujet en Europe.

Le texte, tel qu'il va vous être présenté, transpose ces directives. Nous avons fait en sorte de les garder au plus près, sans surtransposer. Nous avons tenu compte de la

spécificité de la France, notamment en matière de cybersécurité, entre les entités importantes et les entités essentielles. Compte tenu de notre système, nous avons beaucoup de petites et de moyennes collectivités, ce qui n'existe pas en Pologne, en Allemagne ou dans d'autres pays. Nous avons donc fait en sorte d'aider à adapter le dispositif à cette spécificité.

Nous aurons évidemment besoin que la loi soit votée mais aussi qu'elle soit suffisamment partagée et connue pour qu'il puisse y avoir une bonne publicité sur ce sujet, nous permettant ainsi de disposer des moyens pour garantir et améliorer l'attractivité. Si les gens ont conscience que le métier est porteur et qu'il va durer pendant de longues années, de plus en plus de personnes voudront se diriger vers ce domaine. Un travail important sera évidemment à réaliser avec les ministères de l'éducation nationale et de l'enseignement supérieur et de la recherche. L'éducation de la population est un sujet majeur à travers tous les canaux dont nous pourrons disposer.

M. Bernard Chaix (UDR). Lors des dernières réunions, nous évoquions l'accélération de la cadence de production d'équipements militaires nécessaires au vu de l'instabilité géopolitique inédite (intensification de la guerre en Ukraine, résurgence du terrorisme en Syrie avec la prise de la ville d'Alep par des mouvements islamistes et départs forcés de nos troupes au Tchad et au Sénégal, qui dévoilent au grand jour nos faiblesses sur la scène internationale).

Si cette nouvelle cadence est positive, au sein du groupe parlementaire UDR, nous sommes bien placés pour savoir que la quantité ne fait pas toujours la qualité et que le nombre n'est pas la seule variable d'ajustement qui nous permettra de gagner les guerres de demain.

Au regard de la nouvelle nature plurielle de la guerre, il nous incombe d'investir massivement dans les nouvelles technologies, comme les supercalculateurs, devenus indispensables pour le maintien de notre arsenal nucléaire. Par-dessus tout, un nouveau front numérique de la guerre a été ouvert, permettant à des puissances étrangères de contester nos intérêts à distance.

Dans son rapport publié lundi dernier, le service VIGINUM, placé sous votre autorité, a identifié 423 comptes X (anciennement Twitter), tous liés au pouvoir central d'Azerbaïdjan, qui appellent au soulèvement des populations kanak et corses contre la France. En moins de deux ans, VIGINUM a aussi recensé une trentaine de campagnes informationnelles hostiles de l'Azerbaïdjan qui appelaient à la « décolonisation des Outre-mer ». Je pense aussi aux nombreux appels à boycotter les Jeux olympiques de Paris.

Quels seraient les fondements d'une économie de guerre numérique qui permettrait de nous protéger de ces attaques ? Et quels sont les moyens technologiques manquants à VIGINUM qui seraient à acquérir afin de neutraliser ces nouvelles menaces en pleine expansion ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Il y aurait beaucoup à dire sur la désinformation et la manière dont nous pouvons essayer de la contrer.

Concernant l'équipement informatique de VIGINUM, nous avons obtenu les crédits nécessaires pour disposer d'un socle technique permettant de faire efficacement de la veille, de la détection et de la caractérisation. Nous partageons ces détections avec les ministères.

De plus, VIGINUM a besoin de se développer en matière de *capacity building*, c'est-à-dire de formation des autres États démocratiques. Au niveau européen, nous sommes

très engagés en la matière. Le parlement européen avait très tôt créé la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE). Je pense que la nouvelle commission poursuivra les efforts en la matière, dans son champ de responsabilité. Pour notre part, nous essayerons de poursuivre les efforts de coopération sur ce sujet, avec l'aide de l'ARCOM compétente nationalement pour l'application du règlement DSA.

En matière de désinformation, la guerre est asymétrique : nous sommes victimes de désinformation et on essaye de nous nuire ; à l'inverse, en Azerbaïdjan et dans quelques autres pays, il n'y a pas d'information libre. Notre capacité à rétablir les faits est donc limitée. De fait, ce ne peut être qu'une guerre asymétrique.

Ma mission dans ce domaine est de protéger et de favoriser une réflexion chez nos concitoyens. La meilleure des réponses n'est pas de dire qu'une nouvelle est fausse mais de dire qu'elle a été fabriquée à l'étranger par telles personnes, dont nous pouvons donner les adresses IP et les adresses de courriels. Nous donnons ces informations aux médias de qualité, aux chercheurs et à tous ceux qui les demandent, de sorte qu'ils peuvent les vérifier. La meilleure réponse est donc de jouer la transparence et l'information vers les médias et de nos concitoyens, pour que ceux-ci comprennent qu'il faut être prudent sur Internet. Dans une démocratie, le meilleur moyen de lutter contre la désinformation est d'inciter les concitoyens à se poser des questions, à réfléchir et à ne pas gober les fausses informations — ce qui risque d'arriver quotidiennement.

M. le président Jean-Michel Jacques. La question pertinente de notre collègue me permet de rebondir sur le fait que nous allons lancer une mission d'information sur l'influence, lors de laquelle cette bulle informationnelle sera bien entendu évoquée.

Je cède la parole aux députés pour leurs questions.

Mme Caroline Colombier (RN). À l'heure où les tensions géopolitiques s'intensifient, la nouvelle Commission européenne emmenée par Ursula von der Leyen annonçait vouloir faire de l'Europe de la défense le pilier de son action afin de favoriser l'autonomie stratégique de l'Union européenne, s'arrogeant ainsi progressivement le domaine de la défense au mépris des traités.

En ce sens, il ne fait pas de doute que les travaux portant sur le règlement EDIP se poursuivent. Cette proposition de règlement, étudiée depuis mars dernier, vise à définir l'industrie européenne de la défense par trois critères cumulatifs : une autorité de conception européenne, un maximum de 35 % de composants extraeuropéens et l'absence de restrictions d'utilisation.

Or, face à la prochaine prise de fonction de Donald Trump, qui ne manquera probablement pas de promouvoir l'armement américain en exigeant une plus grande contribution des membres de l'OTAN, et au regard de l'urgence opérationnelle incompatible avec les lenteurs des programmes européens, ne craignez-vous pas que cette nouvelle stratégie européenne soit mise en difficulté ou dévie de sa trajectoire, en subventionnant *in fine* l'outil de production américain au détriment de notre BITD ?

M. Sébastien Saint-Pasteur (SOC). La question des vulnérabilités est majeure dans un monde hyper-connecté. Le diagnostic est connu et partagé. Pourtant, des efforts sont encore à consentir.

Je salue le travail colossal du campus régional de cybersécurité et de confiance numérique, situé à Pessac, dans ma circonscription, mais ne peux m'empêcher de penser que

leurs moyens, bien que fortement soutenus par le conseil régional, trouvent des limites face à l'ampleur de la tâche.

Nous pouvons nous demander si les 4 000 PME et ETI de la BITD sont au niveau des exigences actuelles. Les dispositifs existants et le diagnostic cyber, notamment porté par la DGA et Bpifrance, sont-ils à la hauteur ?

Enfin, aborde-t-on suffisamment la nécessité de protéger les femmes et les hommes, au-delà des seuls systèmes d'information, car les vulnérabilités sont aussi là et qu'il convient de réduire la surface d'attaque humaine de nos entreprises, singulièrement sur les profils les plus critiques ?

M. Julien Limongi (RN). La vente d'entreprises stratégiques pour notre défense nationale est toujours une source d'extrême préoccupation pour notre souveraineté. Des fleurons industriels français vendus à l'étranger ont déjà pu être mis en coupe réglée dans le passé, d'où notre inquiétude.

Je ne vais évidemment pas revenir sur le scandale de la vente d'Alstom, qui reste impardonnable, mais je m'enquête, car une situation similaire semble se profiler pour l'entreprise Atos. Cette entreprise, qui développe des systèmes de commandement pour nos forces armées et des dispositifs d'écoute essentiels à notre souveraineté, voit ces technologies sensibles mises officiellement aux enchères.

Dans un contexte où les menaces sur notre sécurité économique et stratégique sont multiples, pouvez-vous nous détailler les procédures mises en place pour encadrer et sécuriser ce type de vente ? Quels mécanismes garantissent que les brevets technologiques critiques et intérêts stratégiques d'Atos ne seront pas cédés à des acteurs étrangers, menaçant ainsi la souveraineté et la défense de la France ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. L'arrivée de Donald Trump à la Maison-Blanche représente évidemment une grande incertitude, compte tenu de sa conception très transactionnelle des relations avec les États. Concernant les sujets liés à la défense, et notamment le règlement EDIP, la possibilité que certains pays achètent davantage d'armements aux États-Unis, au détriment de notre BITD, constitue effectivement une préoccupation. Ce sujet, et notamment le contenu d'EDIP, est évoqué lors des discussions que nous avons avec les uns et les autres.

Un autre point est que le futur président Donald Trump a évoqué l'idée d'un *Freedom of Speech Act* qui supprimerait la modération sur les réseaux sociaux. Or, le *Digital Services Act* européen réclame exactement l'inverse, c'est-à-dire des dispositifs de modération sur les réseaux sociaux, avec des sanctions. Nous aurons donc un sujet de discussion assez compliqué.

Lors de mes voyages en Europe, j'ai pu constater que mes homologues sont bien conscients de l'existence d'un sujet relatif à l'enjeu diplomatique, mais également qu'ils ont aussi des industries d'armement ainsi que des enjeux de souveraineté, et qu'ils se demandent ce que sera l'OTAN dans quelques années. Je peux donc espérer raisonnablement que le travail engagé en bilatéral avec nos principaux partenaires, y compris sur le plan industriel, mais également au niveau européen, puisse nous permettre d'avoir un front un solide face aux incertitudes.

Concernant la protection des entreprises de la BITD, nous essayons à chaque fois de faire en sorte que ces entreprises puissent bénéficier d'un audit — au niveau national, par des entreprises ou par leurs propres acteurs ou fournisseurs.

Pour autant, je ne sais pas si ces audits sont suffisants dans l'absolu. Mais, l'essentiel est quand même d'avoir le niveau suffisant pour parer aux attaques les plus fréquentes. Je citerai la fameuse phrase : « Quand on est poursuivi par un lion, il ne faut pas courir plus vite que le lion, il faut courir plus vite que le voisin ». L'idée est justement d'avoir une protection suffisante pour que les attaquants aillent s'intéresser à d'autres entreprises dans d'autres États. Jusqu'à présent, cela fonctionne relativement mais, au regard des difficultés que peuvent connaître bon nombre d'entreprises, les certitudes sont relatives.

Concernant Atos, comme sur Alcatel Submarine Network, le SGDSN et les ministères ont été à chaque fois associés, et même au premier rang, s'agissant du ministère de l'économie et des finances, pour rappeler nos intérêts fondamentaux. Nous avons beaucoup plaidé et rappelé, par exemple, que la partie d'Atos relative aux supercalculateurs devait rester chez nous, ce qui explique la proposition qui a été faite de garder cette partie, importante aussi pour nos centrales nucléaires. Deux autres outils peuvent être utilisés : la procédure Investissements étrangers en France (IEF), qui va imposer ou interdire la vente d'une entreprise à l'étranger, mais aussi, dans un certain nombre de cas, des lettres d'engagements imposant à l'entreprise étrangère — devant faire partie d'un pays allié — un certain nombre de règles de sécurité et une forme d'étanchéité entre les parties sensibles et les parties plus commerciales. Nous surveillons évidemment que cette étanchéité et ce mode de fonctionnement soient bien établis.

Mme Nadine Lechon (RN). Le 27 février dernier, le capitaine de vaisseau Yann Briand, sous-directeur des affaires internationales du SGDSN, a souligné, lors d'une audition au Sénat, l'importance de la protection de la sécurité économique dans vos missions.

Le rapport de la délégation parlementaire au renseignement (DPR) pour l'année 2022-2023 a mis en avant le fait que l'ingérence industrielle ne concerne pas que nos adversaires connus et déclarés, mais aussi nos alliés. Le rapport cite directement les États-Unis mais nous pouvons aussi penser à l'Allemagne. Toujours selon le rapport, la France ferait preuve d'une naïveté collective sur l'ingérence industrielle et l'espionnage. Rappelons qu'un vol technologique peut coûter jusqu'à quinze ans d'avantages concurrentiels, d'après le colonel Olivier Mas.

Jusqu'à présent, le SGDSN a eu pour principale action de sensibiliser les acteurs de l'armement sur ces questions. Ne serait-il pas désormais nécessaire de prendre des mesures plus approfondies ? Le cas échéant, quelles pourraient être ces mesures ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Il est vrai que l'intérêt de différents États pour nos entreprises n'est pas seulement relatif à de la compétition industrielle mais aussi de la compétition économique. De ce point de vue, nos alliés sont effectivement très intéressés par ce que nous faisons. Nous pourrions nous en sentir flattés mais cette affection est parfois un peu étouffante ou encombrante.

J'évoquais précédemment l'extra-territorialisation du droit. Je suis régulièrement en discussion avec l'ambassade des États-Unis, en liaison avec le CICE, afin que des questions posées par les autorités américaines, administratives ou judiciaires, n'aillent pas au-delà de ce qui est nécessaire à la manifestation de la justice. Parfois, ces questions poussent un peu loin.

En outre, nous essayons de pousser la notion de *cloud* souverain en Europe, c'est-à-dire un *cloud* dans lequel aucun État ou autorité ne pourra aller « pomper » sans que la justice l'y ait autorisé, permettant que nous puissions assurer la sécurité. L'Europe est plutôt en train d'essayer de basculer vers un système de *cloud* à l'Américaine, dans lequel les

autorités américaines pourront, quoi qu'en disent les promoteurs de ce système de *cloud*, « pomper » et aller chercher les données des entreprises, des particuliers et des intéressés pour se renforcer. Nous avons beaucoup d'actions à mener sur ce sujet et nous le faisons, sachant que, selon la célèbre phrase, « un État n'a pas d'amis, il n'a que des intérêts ». Nous veillons extrêmement fortement à l'intérêt qui peut être porté sur ce sujet, de la même manière et avec la même attention, à l'est, à l'ouest, au nord ou au sud.

Nous sensibilisons donc les entreprises et nos acteurs. Nous veillons beaucoup à ce que nos entreprises ne soient pas naïves. Toutefois, vous connaissez vos chefs d'entreprise comme nous. Les gens qui montent des *startups* peuvent difficilement penser à tout. Nous leur recommandons souvent de s'entourer de personnes dotées de la vision logistique, administrative, réglementaire et qui prennent en compte la sécurité, pour éviter les pièges. Lorsque nous avons des projets ou lorsque nous soutenons des appels à candidatures, comme cela a été le cas pour les *startups* du « nouveau nucléaire », nous insistons fortement sur ces points.

Néanmoins, chaque chef d'entreprise est libre de faire ce qu'il veut et on ne pourra pas, au-delà des entreprises nécessaires à la sécurité nationale, imposer des mesures de sécurité qui basculeraient sur un sujet de liberté publique, surtout s'il fallait commencer à vérifier. Premièrement, nous n'avons pas les moyens. Deuxièmement, nous n'avons pas l'envie. Troisièmement, je pense que chacun doit assumer sa propre responsabilité en matière de sécurité. Pour reprendre une expression célèbre, non seulement l'État ne peut pas tout, mais je rajouterai que l'État ne doit pas tout.

M. le président Jean-Michel Jacques. Je vous remercie, monsieur le secrétaire général. Nous avons pu apprécier votre expérience de préfet, qui enrichit vos réponses très complètes et à laquelle, en tant que députés des territoires, nous sommes sensibles.

*

* *

La séance est levée à dix heures quarante-cinq.

*

* *

Membres présents ou excusés

Présents. - Mme Delphine Batho, Mme Valérie Bazin-Malgras, M. Christophe Bex, M. Christophe Blanchet, M. Matthieu Bloch, M. Hubert Brigand, M. Bernard Chaix, Mme Caroline Colombier, M. Alexandre Dufosset, M. Yannick Favennec-Bécot, M. Emmanuel Fernandes, Mme Stéphanie Galzy, M. Thomas Gassilloud, M. Damien Girard,

M. Michel Gonord, M. Daniel Grenon, M. David Habib, Mme Emmanuelle Hoffman, M. Jean-Michel Jacques, M. Pascal Jenft, M. Loïc Kervran, M. Abdelkader Lahmar, M. Fabien Lainé, Mme Anne Le Hénanff, Mme Nadine Lechon, Mme Gisèle Lelouis, Mme Murielle Lepvraud, M. Julien Limongi, Mme Lise Magnier, M. Sylvain Maillard, M. Thibaut Monnier, M. Karl Olive, Mme Anna Pic, M. Aurélien Pradié, Mme Catherine Rimbert, M. Aurélien Saintoul, M. Sébastien Saint-Pasteur, Mme Isabelle Santiago, M. Thierry Tesson, M. Romain Tonussi, Mme Corinne Vignon

Excusés. - Mme Anne-Laure Blin, M. Manuel Bompard, M. Philippe Bonnecarrère, Mme Yaël Braun-Pivet, Mme Cyrielle Chatelain, M. Yannick Chenevard, Mme Alma Dufour, Mme Catherine Hervieu, Mme Mereana Reid Arbelot, M. Aurélien Rousseau, M. Mikaele Seo, Mme Sabine Thillaye, M. Boris Vallaud

Assistait également à la réunion. - M. Jean-Luc Warsmann