ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Mercredi
13 juillet 2022
Séance de 11 heures

Compte rendu n° 5

SESSION EXTRAORDINAIRE DE 2021-2022

Compte rendu

Commission de la défense nationale et des forces armées

— Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale.

Présidence de M. Thomas Gassilloud, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures.

M. le président Thomas Gassilloud. Monsieur le secrétaire général, nous tenions à vous auditionner sans tarder devant cette commission renouvelée à près de 80 %, puisque vous êtes une des personnes les plus importantes au sein de l'architecture de l'organisation de défense et de sécurité globale de notre République. Vous êtes de ceux qui en ont la vision la plus complète, puisque vous êtes le chef d'une administration dépendant organiquement du Premier ministre et dont les travaux sont à l'articulation des responsabilités relevant du Président de la République et du Premier ministre. Vous êtes notamment le secrétaire des conseils de défense et de sécurité nationale. Vous préparez des dossiers qui sont remis aux participants. Vous êtes responsable de l'établissement du projet de relevé de décisions.

Au-delà de cette mission à proximité immédiate du Président de la République, chef des armées, vous avez la responsabilité de la coordination interministérielle dans le champ de la défense et de la sécurité nationale, au nom du Premier ministre. Vous avez notamment la charge de la conception, de l'animation et de la planification de la sécurité nationale, de la réglementation sur le secret de la défense nationale, de l'anticipation et du suivi des crises internationales, de la protection du patrimoine scientifique et technique. Il nous intéresse de voir comment se fait l'animation du travail de défense à l'échelle interministérielle.

Nous savons qu'il y a dans les principaux ministères des hauts fonctionnaires à la défense et à la sécurité, mais comment les sujets de défense nationale sont-ils pris en compte à l'échelle de chaque ministère ? Puisqu'on parle beaucoup du retour de la haute intensité, dans ce contexte, les armées ne livreraient pas la guerre seule. Quelle est l'implication du ministère de la santé dans la prise en charge des blessés ? Comment notre approvisionnement alimentaire est-il garanti ? Comment le ministère de l'intérieur ferait-il face à des troubles sur le territoire national ? Le concept de défense globale, qui date des années 1950, reste-t-il pertinent pour être à la hauteur de nos enjeux de défense nationale ?

Par ailleurs, vous êtes responsable de la politique de cybersécurité des systèmes d'information classifiés interministériels et de la lutte contre les ingérences numériques étrangères. Pour ces missions, vous disposez de l'agence nationale de sécurité des systèmes d'information (ANSSI), qui représente quelque 600 personnes, soit quasiment la moitié de vos effectifs, de l'opérateur des systèmes d'information interministériels classifiés (OSIIC) et de Viginum, service de création plus récente destiné à détecter d'éventuelles ingérences numériques étrangères, notamment dans le champ informationnel.

Ces derniers mois, vous avez beaucoup travaillé sur une stratégie nationale de résilience visant à tirer les enseignements de la crise sanitaire et à renforcer notre capacité collective à réagir après un choc, de quelque nature qu'il soit : attaque cyber, choc sanitaire, choc énergétique, choc climatique…

Notre défense est efficace si elle est globale. C'est pourquoi, au-delà de l'effort militaire, nous sommes sensibles au fait que l'ensemble du Gouvernement et même l'ensemble des acteurs de la nation soient impliqués dans la défense nationale.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Monsieur le président, Mesdames et Messieurs, je suis heureux de faire la connaissance de la plupart d'entre vous, et de retrouver d'autres d'entre vous que j'ai connus dans différents départements et à l'Assemblée. Le SGDSN est à votre disposition pour vous rendre compte de son action, vous informer et travailler avec vous sur l'ensemble des enjeux qui vont nous concerner dans les prochaines années.

À l'origine, structure de coordination des moyens des ministères en charge de la défense nationale, c'est devenu, dans les années 1930, une sorte d'état-major des armées, au sein duquel le commandant de Gaulle avait d'ailleurs séjourné. À la suite d'un livre blanc sur la sécurité intérieure, c'est devenu le secrétariat général de la défense et de la sécurité nationale, évolution marquante, puisqu'un préfet est actuellement à sa tête et qu'il est amené à prendre en compte à la fois les sujets intérieurs et extérieurs.

Le SGDSN comprend environ 1 300 agents, dont une petite moitié pour l'ANSSI. Il est en charge du secrétariat du conseil de défense et de sécurité nationale (CDSN), de la protection du secret de la défense nationale, incluant la classification et la déclassification qui représentent un lourd travail. Il est chargé de la planification de sécurité et de quinze plans, dont Vigipirate, Piratair, Piratmer, Piranet, des risques nucléaires, radiologiques, biologiques et chimiques (NRBC), des drones, dans la perspective des Jeux olympiques de 2024, ainsi que du suivi des crises internationales et de la sécurité économique des entreprises sensibles. Nous agissons au côté de la direction générale des entreprises (DGE) pour protéger notre patrimoine scientifique et technique mais aussi, en liaison avec les préfets de régions, les entreprises plus ou moins grosses comme celles qui se trouvent dans vos départements, lorsqu'elles sont menacées par des investisseurs étrangers hostiles ou des prédateurs de matière grise : nous essayons de les aider, de les protéger et de mettre en place au niveau interministériel un dispositif à même de les soutenir pour préserver nos intérêts.

Nous suivons quelques sujets spécialisés à teneur interministérielle comme le nucléaire, le spatial, qui prend de plus en plus de force, ou les câbles sous-marins, sujet porteur en développement.

Je reviendrai sur les trois services à compétence nationale placés sous mon autorité.

Nous gérons le groupement interministériel de contrôle (GIC), mais nous ne le dirigeons pas, puisque le Premier ministre et son cabinet dirigent l'ensemble des techniques de renseignement que les services de renseignement mettent en œuvre sous le contrôle de la commission nationale de contrôle des techniques de renseignement (CNCTR). Par conséquent, même si je peux être entendu par la délégation parlementaire au renseignement (DPR), nous ne sommes pas un service de renseignement, mais une structure interministérielle qui coordonne, fait faire et fait lorsque la mission ne peut être rattachée à un seul ministère ou nécessite l'autorité du Premier ministre.

Nous nous situons à cheval entre le Président de la République et le Premier ministre, en vertu de l'article 21 de la Constitution qui dispose que le Premier ministre est responsable de la défense nationale, ce qui va au-delà de la défense militaire et est complémentaire de l'article 15 de la Constitution qui dispose que le chef de l'État est chef des armées.

Cela relève aussi du rôle de direction du gouvernement par le Premier ministre. L'article 114-1 du code de la défense dispose : « Chaque ministre est responsable, sous l'autorité du Premier ministre, de la préparation et de l'exécution des mesures de défense et de sécurité nationale incombant au département dont il a la charge ». Autrement dit, chaque ministère doit participer à la défense globale et chaque ministère a en son sein un haut fonctionnaire de défense et de sécurité qui travaille avec nous, pour nous, sous notre direction pour l'interministériel et est amené à œuvrer quotidiennement sur les difficultés qui peuvent se poser. La notion de défense globale est valorisée, puisque chaque ministre y participe et que ce n'est, en aucun cas, la seule affaire du ministre des armées.

Cela va au-delà de la distinction entre militaire et civil. Le Livre blanc sur la défense et la sécurité nationale de 2008 avait souligné les multiples interconnexions entre les stratégies et les politiques de la France pour la sécurité des Français dans tous les domaines. En droit, nous disposons d'un outil pour assumer et soutenir la défense globale, c'est le concept des intérêts fondamentaux de la nation. Je l'évoque en début de propos parce que vous faites le droit et que nous ne pouvons agir qu'à partir d'un cadre juridique, conformément au principe démocratique.

Ce concept apparaît dans le Code pénal en 1994, à l'article 410-1, qui en donne une définition large et non exhaustive : « Les intérêts fondamentaux de la nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel. » Cela mêle la défense du pays, de ses institutions, les moyens de son action, ce qui fait le patrimoine de la France dans tous les domaines et, d'une certaine manière, la protection des intérêts fondamentaux de la nation est la vie de la nation.

Cela a été repris en 2009 dans le code de la défense, qui dispose que « L'ensemble des politiques publiques concourt à la sécurité nationale ».

En novembre 2011, le Conseil constitutionnel a jugé que la défense des intérêts fondamentaux de la nation était une exigence constitutionnelle.

En complément, la loi de juillet 2015 relative au renseignement a intégré dans la liste précédemment indiquée la lutte contre le terrorisme, la lutte contre la prolifération des armes de destruction massive et la prévention des atteintes à la sécurité publique, le tout sous le contrôle des juges et du Parlement.

Quelle en est la traduction concrète ?

La menace a changé. Vous avez reçu, la semaine dernière, le ministre des armées. Je m'occupe plus particulièrement des crises, lesquelles ont changé de dimension. Auparavant localisées et courtes, dites « à cinétique courte », les plans étaient faciles, cela ressemblait parfois à un film américain avec une *happy end* : une crise survenait, les moyens de renfort arrivaient, les vaccins arrivaient, tout le monde était guéri et la vie reprenait son cours normal. La crise du Covid a bouleversé ce schéma. Les crises sont devenues de longue durée, généralisées, leurs effets sont très étendus sur nos territoires et au-delà. Dès lors, la planification est remise en cause. Lors de la crise du Covid, nous avons appliqué à 95 % le plan de lutte contre la pandémie grippale, mais au bout d'une dizaine de jours, il était devenu inapplicable faute de vaccins et d'autres moyens. Nous étions débordés, en dépit du bon fonctionnement des structures, et de la mobilisation intense de tous les personnels concernés.

En outre, la mondialisation est remise en cause. On a longtemps considéré que, faute de moyens à tel endroit, on pouvait en importer de tel autre. Les plans sanitaires et autres prévoient de faire venir des matières premières ou des médicaments d'autres pays. Mais durant la crise, l'Inde ne livrait plus de curare, la Chine ne livrait plus de masques. La guerre en Ukraine provoque la pénurie de certaines matières premières et en matière d'énergie. La mondialisation, telle que pensée après la chute du rideau de fer, a disparu. On est revenu à un système d'égoïsmes d'État et de fermeture des frontières auquel nous devons nous adapter en termes de planification.

Le droit international qui permettait de résoudre les crises et de discuter avec les uns et les autres est remis en cause. La réponse est désormais apportée d'État à État, par alliances et par groupes d'États. Elle doit donc être systémique en prenant en compte toutes les conséquences dans tous les domaines. Nous nous y employons en matière de planification pour faire face aux crises sanitaires, aux crises climatiques et à la guerre en Ukraine, dont les conséquences sont à la fois militaires, économiques et géopolitiques, eu égard à la pénurie alimentaire.

Le SGDSN se penche aussi sur les nouvelles formes de conflictualité, dites menaces hybrides, et sur le concept « comment gagner la guerre sans avoir à combattre », théorisé par le chef d'état-major des forces armées russes, le général Guerassimov, qui reprenait la théorie ancienne de Sun Tzu (même si celui-ci ignorait les attaques cyber).

Les attaques cyber sont les plus connues puisqu'elles nous touchent tous : citoyens, petites entreprises, entreprises moyennes, grands groupes sont victimes des rançongiciels via le chiffrage des données et des escroqueries. Nous assistons à l'explosion du nombre d'attaques et d'extractions de fichiers, d'espionnage, d'attaques en sabotage par des États et des proxies d'État. En 2021, l'ANSSI a constaté 1 082 intrusions avérées, soit une augmentation de 37 % par rapport à 2020. Et encore, en 2020, en raison du Covid et du recours accru à des moyens numériques, cela avait-il déjà beaucoup augmenté par rapport à l'année précédente. Nous avons en mémoire des affaires célèbres, comme le blocage des systèmes informatiques des hôpitaux, le blocage des services publics et des collectivités locales, l'impossibilité d'émettre ou d'imprimer des journaux pour les grands médias, l'interruption de l'activité des entreprises et des transports. Les smartphones sont de plus en plus touchés. On se souvient de l'affaire Pegasus. Sur les messageries chiffrées comme Telegram ou Whatsapp, il devient alors facile de s'emparer des données d'un smartphone piégé, y compris celles en mémoire et dans le Cloud qui transiteraient sur le smartphone en question. Certains groupes et certains États sont capables d'utiliser ces vulnérabilités contre les uns et les autres. D'ailleurs, avant la campagne pour l'élection présidentielle, nous avions réuni les représentants de tous vos partis pour les mettre en garde sur ces menaces.

Les attaques en désinformation, c'est-à-dire les manipulations de l'information, sont un autre type d'attaques non conventionnelles. Lors de la préparation du service de lutte contre les ingérences numériques d'origine étrangère Viginum, nous avions rencontré les présidents de commissions et les chefs des principaux partis politiques. Il ne s'agissait nullement de s'intéresser à la vie politique française, mais d'observer les attaques numériques de l'étranger ou de proxies de l'étranger visant à porter atteinte à l'ordre public, à la sincérité des élections ou à la stabilité de la société. Après l'attentat contre Samuel Paty, nous avons subi des attaques venant d'un État étranger, qui ont eu pour objectif de déstabiliser la population et de permettre au dirigeant de ce pays de réassoir son autorité sur sa communauté. Lors des élections, nous avons été attentifs à des attaques de l'ultra-droite américaine visant à mettre en cause la sincérité de nos scrutins et de notre système électoral. Nous subissons aussi de fortes attaques de la Russie contre la présence française en Afrique.

D'autres attaques peuvent viser les entreprises. Danone avait fait l'objet d'attaques fortes sur les médias et plateformes en ligne, fomentées par un pays étranger à l'aide de concurrents, qui avaient nui à son chiffre d'affaires et à sa capacité à réagir. Je reviendrai sur le dispositif que nous avons mis en œuvre, sachant encore une fois que nous ne nous intéressons qu'aux ingérences numériques d'origine étrangère.

Le troisième type de menace hybride est les attaques par détournement du droit, ou « Law Fare », à l'encontre de nos entreprises. Il s'agit de l'application par un État étranger de

sa loi dans notre pays. Les Américains sont experts en ce domaine, au moyen de différentes règles comme l'ITAR ou l'EAR. La présence d'un composant américain, ne serait-ce qu'une puce, dans le produit d'un État étranger, ouvre le droit aux Américains de demander des explications sur la manière dont il est produit, même si cela relève du secret professionnel, voire de poursuivre l'entreprise et ses dirigeants. En outre, le *Cloud Act* permet aux services de renseignement américains de plonger dans les *Clouds* fournis par des entreprises installées aux États-Unis, les cloud pouvant être n'importe où dans le monde, pour y rechercher des informations sans que personne n'en soit informé et sans autorisation. Le *Defence Act* permet de bloquer des exportations contraires aux intérêts des États-Unis. Les Chinois sont en train de copier ces lois presque mot pour mot. Tout cela complexifie une partie de nos exportations.

Nous faisons face à l'édiction de normes défendant les intérêts d'un seul État.Nombre de pays essaient d'imposer leurs propres normes dans les instances internationales afin de favoriser leurs entreprises ou leur économie ou prendre le contrôle sur d'autres. À quoi s'ajoutent la judiciarisation des relations commerciales et les possibilités de poursuites.

Une autre menace hybride est les attaques contre la sécurité économique. Cela va du stagiaire qui traîne après la fermeture des bureaux pour copier des dossiers, à la visite d'une délégation étrangère qui oublie des petits objets sous la table ou prend des photos. Si les très grandes entreprises y sont sensibilisées, en revanche, les petites et moyennes, qui sont parfois des pépites sans le savoir, sont d'une grande vulnérabilité. Ajoutons la prédation par la captation de matière grise, les attaques réputationnelles et les attaques en Bourse.

Les attaques cyber et en désinformation sont celles du faible au fort. Face à des attaques de pays petits ou moyens, nous n'avons guère de capacité de réponse. Confronté à des autocraties sans presse libre, où les accidents sont couverts par la censure, il est difficile de réagir. En France, une attaque cyber dirigée contre des moyens de transport est connue immédiatement, tandis que dans les pays à régime autoritaire, elle restera inconnue. Par ailleurs, l'organisation des médias dans ces pays interdit toute réaction à la désinformation !

Enfin, le principe est d'agir sous le seuil de conflictualité, afin que l'attribution d'une attaque ne puisse être associée à tel État ou à telle organisation.

La guerre au terrorisme n'a cependant pas disparu. Nous rencontrons toujours des menaces en Afrique, dans le Nord-Est syrien. Al-Qaïda et l'EIS veulent toujours se tailler des domaines, prendre le contrôle d'États, imposer leurs règles, envoyer des commandos dans nos pays, manipuler les esprits fragiles, au travers d'internet, pour les inciter à commettre des attentats.

Je ne m'étendrai pas sur le retour des conflits de haute intensité. La guerre en Ukraine est une forme de retour aux conflits du XXe siècle avec leurs horreurs, la guerre mécanisée et l'utilité de la dissuasion nucléaire pour éviter qu'aucun État ne puisse imposer sa volonté aux autres en les menaçant de destruction totale.

Il faut se préparer aux conflits du XXIe siècle et au réchauffement climatique. L'accès à l'eau et à la nourriture, l'accès aux matières premières entraîneront une forme de conflictualité qui aura des conséquences dans notre vie quotidienne, et pas uniquement sous l'angle militaire.

Que faisons-nous face à ces menaces ? Je ne reviendrai pas sur les réponses militaires. Le délégué général de l'armement vous a parlé de nos fortes attentes vis-à-vis de la base industrielle et technologique de défense. Le SGDSN étant responsable des exportations de matériels de guerre, et nous avons des rapports à vous faire sur ce sujet, nous sommes très

vigilants à nos livraisons et la possible dissémination qui pourrait en résulter, non seulement au regard des traités internationaux, de nos engagements, mais aussi de notre propre sécurité. Nous sommes attentifs à la situation en Ukraine et aux armes qui y sont livrées.

Face aux nouvelles formes de conflictualité, l'ANSSI, qui dispose de 176 millions d'euros au titre du plan de relance, a aidé 600 entités. Des projets de loi viseront à renforcer ses prérogatives pour obliger les plateformes à signaler à leurs clients les vulnérabilités et les attaques. Si, à partir de 130 km/h, la direction de la voiture que je viens d'acheter se met à faseiller, le constructeur a l'obligation de me prévenir. Mais si j'utilise un système informatique vulnérable, exposé à une prise de contrôle extérieur ou au sabotage, l'entreprise n'a pas obligation de me le dire.

Nous allons multiplier le nombre de centres agréés pour aider les entreprises et les particuliers à faire face aux attaques. Nous avons déjà développé des centres dans les régions. Nous allons accroître le contrôle sur les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE) afin de les obliger à réaliser les investissements nécessaires pour protéger leur sécurité informatique et à renforcer leur sécurité en tant qu'établissements recevant du public. Cela implique une progression des moyens de l'ANSSI, si vous en décidez ainsi lors de l'examen du prochain projet de loi de finances.

La création du service Viginum marque une étape importante. Par deux décrets pris en Conseil d'État, nous avons créé un dispositif, placé sous le contrôle du Parlement, et doté d'un comité éthique et scientifique veillant à la fois à une bonne exploitation scientifique des recherches et au strict respect des textes. Viginum ne fait que de la détection, de la veille, de la caractérisation. Il transmet les menaces recensées aux autorités, auxquelles il revient de saisir la justice, de faire du contre-discours et, le cas échéant, de réagir auprès d'un État étranger. Pendant les campagnes électorales pour l'élection présidentielle et pour les élections législatives, Viginum a travaillé activement et exclusivement pour le compte et sous l'autorité du Conseil constitutionnel, de la commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle et de l'autorité de régulation de la communication audiovisuelle et numérique (ARCOM). L'ensemble des éléments que nous avons relevés leur ont été transmis.

En matière de law-fare, nous essayons, aux niveaux national et européen, de faire de la contre-législation et de mieux défendre les entreprises soumises à des enquêtes extérieures.

Nous conduisons le comité de liaison en matière de sécurité économique (Colisé) avec le ministère de l'économie et des finances pour protéger nos entreprises. Nous avons mis en place des groupes de travail pour trouver des solutions face aux restrictions en énergie, en matières premières, en céréales.

La réponse aux crises généralisées passe par la refonte de la planification. Après la planification grippale, nous travaillons sur une planification pandémique générique prenant en compte l'ensemble des problèmes.

Nous sommes attentifs au risque de black-out de longue durée. Même lorsqu'on dispose de groupes électrogènes, pour les faire fonctionner, il faut s'assurer que les dépôts pétroliers principaux et secondaires disposent d'électricité pour remplir les camions.

Nous préparons à la gestion de crise des dirigeants d'administration centrale et des dirigeants des cabinets ministériels. Lors de la survenue d'une crise, le ministre ou son directeur de cabinet n'est pas forcément préparé. Or il doit être rapidement opérationnel et chacun doit pouvoir être relevé en cas de crise durable. Il en va de même pour les préfectures.

La stratégie nationale de résilience est un sujet que vous connaissez bien, Monsieur le président, puisque vous avez été rapporteur de la mission d'information sur la résilience nationale. Permettez-moi de vous citer : « La résilience de la nation est d'abord celle de ses citoyens unis autour d'un projet collectif ». Nous devons être capables d'anticiper, d'imaginer les crises inimaginables, de rechercher nos vulnérabilités, s'y préparer, se mettre en état de réagir et d'organiser un retour à la normale.

Nous préparons un plan au niveau de l'État, par des études de vulnérabilités structurelles, en vérifiant les plans de continuité pour s'assurer qu'ils soient véritablement opérationnels. Nous nous penchons sur la formation des agents de l'État et réalisons des exercices. Nous prévoyons une démarche capacitaire interministérielle, en termes de recherche, d'innovation et de stocks stratégiques. En matière agricole et énergétique, les « stocks de la SAGESS » fonctionnent bien. Concernant le gaz, nous avançons. Nous nous penchons sur les stocks sanitaires et d'autres, y compris ceux nécessaires à la vie quotidienne.

Nous souhaitons associer les collectivités locales. Des contacts ont été pris avec les présidents d'association, comme nous l'avons fait au cours de la crise du Covid, afin de mieux travailler avec les communes, les départements et les régions, dans le cadre de leurs responsabilités, utiliser leurs moyens, répondre à leurs attentes et agir avec la population.

Il convient de renforcer la communication vers la population et le grand public. Il faut réimpliquer le citoyen comme acteur de sa propre résilience. Cela existe déjà. Dans le Var, les comités communaux de protection contre les feux de forêt sont sur le terrain. Les plans communaux de sauvegarde pour aider les populations à évacuer lorsque le feu menace fonctionnent bien. Il en va de même, dans d'autres départements, en cas d'inondation. Ce dispositif fonctionne avec les associations agréées de protection civile, les citoyens et d'abord les municipalités. Nous devons systématiser ce domaine, afin, lors de la survenue d'une prochaine crise, d'agir avec tout le monde, de l'État à la collectivité locale en passant par les entreprises spécialisées dans la gestion de crise et le citoyen.

En conclusion, tout cela fait la défense globale, en quelque sorte, le glaive et le bouclier. Au SGDSN, nous mettons en œuvre le bouclier, c'est-à-dire la capacité de la nation à faire face aux difficultés. Nous travaillons sur les principes juridiques, les moyens matériels, les professionnels et le citoyen. C'est ainsi que nous nous préparons aux crises et manifestons le concept de défense globale sur lequel vous m'avez interrogé.

M. le président Thomas Gassilloud. Merci, Monsieur le secrétaire général pour cette riche introduction qui nous permet de mesurer le périmètre des travaux sur lequel notre commission pourra se pencher.

Mme Anne Genetet. Monsieur le secrétaire général, le décret fixant votre périmètre liste un nombre de missions considérable. Comment parvenez-vous à coordonner l'ensemble ?

Basée en Asie, j'ai travaillé sur le plan pandémie de l'OMS et français entre 2006 et 2008, à l'époque où l'Asie s'inquiétait d'un risque de pandémie respiratoire. Nous ne pouvions pas avoir de vaccin, puisque la mise au point d'un vaccin antigrippal nécessite au moins six mois et nécessite des œufs, donc des poules, dont le nombre était insuffisant pour ce faire.

La Chine faisant partie de ma circonscription, j'ai été contactée par un sinophone dont l'acharnement à intégrer mon équipe comme stagiaire a éveillé ma vigilance. Je comprends votre appel à la plus grande prudence.

Au début de la guerre en Ukraine, nous avons à juste titre interdit à RT France de diffuser ses contenus. Les Britanniques interdisent qu'un média impliquant un parti politique diffuse sur le sol britannique, ils ont interdit à la chaîne chinoise CGTM de diffuser sur leur territoire. La CGTN a basculé sur l'espace français pour diffuser en Europe. Comment mettre en place un dispositif identique à celui des Britanniques afin de contrôler la diffusion de la CGTN sur notre territoire ?

Mme Caroline Colombier. La situation sécuritaire de la France est au cœur des préoccupations de nos concitoyens. Un article du *Télégramme* du 3 juillet dernier soulignait l'intérêt porté par les services de renseignement chinois à nos installations militaires et de défense en Bretagne. Dès 2019, un article du *Point* relevait l'étrange implantation d'un centre universitaire chinois dans l'ancienne base militaire de Châteauroux, à proximité du centre de transmissions de la marine de Rosnay, position majeure pour notre souveraineté nationale. Quelles mesures sont prises pour contrôler le risque d'ingérence de ce centre universitaire et pour détecter les implantations étrangères susceptibles de nuire à notre souveraineté ? Comment sensibiliser les acteurs privés et publics à ce risque d'ingérence étrangère ?

Mme Murielle Lepvraud. Monsieur le secrétaire général, nous traversons une énième canicule. Le dérèglement représente une menace terrible pour la stabilité mondiale et la santé de notre population. La multiplication des phénomènes climatiques extrêmes, leur accumulation et leur survenue simultanée pourraient mettre la société à l'arrêt. Toutes nos infrastructures sont susceptibles de pâtir de ce phénomène. Les rendements agricoles peuvent être affectés et les infrastructures de la défense éprouvées. Les matériels militaires pourraient être inutilisables d'ici quelques années du fait de pénuries de carburant. Quels sont les plans élaborés par le SGDSN pour préparer la société à faire face à ces périls ?

Mme Nathalie Serre. Le service Viginum est entré en fonctionnement. Son effectif est-il complet ? Quels sont les profils de ses agents ? Dans quel cadre avez-vous agi pour l'élection présidentielle et la campagne pour les élections législatives ?

Concernant la communication avec la population, nous avons tous dans nos territoires et nos conseils municipaux des correspondants défense. Comment pouvons-nous les intégrer ? Dans quelle mesure pouvons-nous contribuer au lourd effet collectif de défense globale ?

Mme Anna Pic. Le dérèglement climatique aura un effet majeur dans les prochaines années, provoquant le doublement du nombre des migrants. Les réfugiés environnementaux pourraient représenter 150 millions à 1 milliard de personnes dans les années 2050. Les effets de l'augmentation de la température se font déjà sentir directement sur les populations, dont l'environnement se détériore rapidement. Qu'ils soient internes ou internationaux, les migrants contribueront à déstabiliser des zones déjà affectées par la pauvreté ou des actions terroristes. Avons-nous envisagé des stratégies pour y faire face, non seulement en amont, pour améliorer les conditions de déplacement, mais aussi pour élaborer des conditions d'accueil de nature à éviter d'aggraver les conflictualités mondiales ?

M. Loïc Kervran. Je suis frappé de constater que des pays voisins du nord de l'Europe considèrent que certains États sont devenus des narco-États à haut niveau de violence et de corruption, notamment dans les zones portuaires Quelle est votre opinion sur le niveau de menace et de pression de la criminalité organisée dans notre pays ?

Nous constatons une évolution de la menace. Les auteurs se situent souvent plus bas dans le spectre qu'il y a quelques années et les cibles sont réparties sur tout le territoire. Quel est votre regard sur la place du renseignement dans les territoires ?

Enfin, après que mon département du Cher eut subi un phénomène climatique violent, les pompiers ont demandé des renforts mais de très nombreux autres départements ayant été touchés au même moment, aucun n'était disponible et les moyens de la sécurité civile étaient également tous employés. Ne faut-il pas redimensionner les bases et le nombre de personnels de la sécurité civile pour faire face à certains épisodes ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Nous ne sommes pas une très grosse maison et nous faisons de la coordination. Le principe de notre action, c'est de faire travailler l'ensemble des ministères, de faire faire les uns et les autres, de ne pas faire à leur place mais de vérifier qu'ils font. En plus du secrétariat du conseil de défense et de sécurité nationale, j'assure le suivi des décisions prises pour m'assurer de leur effectivité. Lorsque des actions et des plans sont lancés, nous veillons à ce que les ministères fournissent les éléments nécessaires. Cela demande du temps et du personnel, mais c'est mieux que de le faire par nous-mêmes, et les directions sont bien engagées en ce sens.

En tant que service du Premier ministre, nous pouvons nous appuyer sur son autorité vis-à-vis des autres pour engager et mener des actions. Notre maison travaille beaucoup et a la chance de disposer d'un niveau de qualification élevé. Je travaille au milieu de généraux, de colonels, de capitaines de vaisseau, d'ingénieurs généraux de l'armement, d'administrateurs civils, d'ambassadeurs, de préfets et d'une série d'autres cadres et techniciens experts en leur matière. C'est stimulant et réjouissant et c'est une preuve de qualité des effectifs, y compris au regard de services qui peuvent être soumis à concurrence.

Pour Viginum, nous parvenons à recruter des agents de toutes catégories et de tous niveaux, même si nous les payons moins bien que dans le secteur privé. D'abord, parce que les gens y trouvent une vocation à être utile au service général, et il est toujours intéressant de savoir pourquoi on travaille et de le faire dans l'intérêt général. Ensuite, ils bénéficient d'une vision globale d'un secteur d'activité. Au lieu de s'occuper d'une entreprise, ils s'intéressent aux médias, aux entreprises de transport, aux entreprises d'énergie, à des particuliers, ce qui est diversifié et formateur. Enfin, après leurs quelques années à l'ANSSI, à l'OSIIC ou au sein de Viginum, des entreprises privées vont se battre pour leur proposer une intéressante carrière dans le secteur privé.

Le recrutement de Viginum est très diversifié. Nous avons des analystes, donc des universitaires, des « geeks à poil long » capables de scruter des écrans de télévision ou d'ordinateurs, des militaires de différentes administrations et parfois des services de renseignement. On a parfois l'impression d'être dans un campus universitaire, mais ce sont des gens habilités, retenus après toutes les vérifications nécessaires.

Le renforcement du contrôle des chaînes de médias comme RT et CGTN nécessite de modifier la loi au nom de la liberté de l'information. Toute mesure doit être limitée et proportionnée, et le conseil constitutionnel y veille. En Grande-Bretagne, plus dure qu'en France, elle permet à l'autorité administrative de couper purement et simplement la diffusion d'ondes sur le territoire. Chez nous, la loi l'interdit et RT, CGTN et d'autres médias peuvent parfaitement utiliser des satellites pour arroser notre territoire. La loi de 1986, complétée par la loi de 2018, permet à l'ARCOM de demander aux opérateurs de corriger, interdire, modifier ou sanctionner des médias, mais le principe reste la liberté. Si elle est mal utilisée, la sanction est mise en œuvre. Si vous souhaitez modifier la loi, nous pourrons en discuter.

De nombreux Chinois s'intéressent à nos intérêts en pratiquant l'infiltration et l'espionnage. Pendant la guerre en Ukraine, on s'attendait à de nombreuses cyberattaques de la part de la Russie, mais nous en avons eu très peu à ce jour. La seule attaque notable était dirigée

contre un satellite de VIASAT, géré par Eutelsat, qui permettait aux forces ukrainiennes de communiquer entre elles et qui arrosait l'Europe de l'Ouest. Il a été atteint, probablement par les Russes, en grillant tous les modems. Chez nous, cela a touché des relais de secours du 15, du 18. En Allemagne, une bonne partie des éoliennes se sont arrêtées.

Dans le même temps, des Chinois espionnent à tire-larigot et s'en donnent à cœur joie en matière d'entrisme, de pénétration et de tentatives de captations. À chaque arrivée dans les universités de stagiaires ressortissants de certains pays – nous sommes attentifs à la Chine et à l'Iran qui s'intéressent à la physique et à la chimie, et à quelques autres États - nous faisons systématiquement réaliser une enquête par les services de renseignement et, le cas échéant, refusons un droit d'accueil de tel ou tel, voire mettons fin à son séjour. Nous surveillons aussi les centres de type Confucius ou Lagrange et autres, et leur système de fondation.

Nous faisons en sorte que certaines entreprises, en particulier chinoises, ne puissent pas accroître à l'excès leur importance en France. Nous leur avons interdit l'accès, en matière de téléphonie, à certaines zones considérées comme sensibles. Vous aurez probablement à retravailler sur la loi de 2019. C'est un des points sur lesquels nous pourrons intervenir.

La sensibilisation des acteurs publics est un sujet complexe. Tous les jours, je lis des notes d'information m'informant qu'une université ou un laboratoire a accepté de prendre tel ou tel. Lorsque j'étais en poste à Strasbourg, j'avais connu un prix Nobel de Chimie dont le laboratoire était plus ouvert que le bistrot du coin. Tout le monde y traînait, dont quelques stagiaires à l'origine indéterminée. Il m'avait dit : « La science n'a pas de frontières ». Je lui avais répondu qu'il s'était réjoui de voir son prix Nobel lui être attribué à lui et non à un de ses collègues étrangers. Nous vous soumettrons des textes de loi en matière de protection du patrimoine scientifique et technique, afin de renforcer la prudence et les précautions à prendre en ces domaines. Nous subventionnons des laboratoires et des entreprises, au travers des plans de relance, nous leur attribuons des aides pour qu'ils puissent se développer et non pour servir un État étranger.

Nous sommes très sensibles à la préparation aux crises climatiques et aux stratégies à mettre en place en amont. Nous essayons d'anticiper mais nous n'avons pas toujours les réponses. Il est hors de question de remettre en cause la notion de souveraineté des États. Au-delà des actions internationales que vous connaissez, il nous est difficile d'agir en ce domaine. La parole revient plutôt au ministère de l'Europe et des affaires étrangères qui, par son aide au développement, soutient certains pays et met en place différentes actions. À ce stade, nous travaillons fortement à la préparation de crise face aux possibilités de restrictions en eau, en électricité ou autres. Nous le faisons en liaison avec nos voisins, sachant qu'une coupure d'électricité en Allemagne pourrait provoquer un black-out en France, que les problèmes d'eau et d'approvisionnement dans différents pays auront, qu'on ne veuille ou non, des conséquences, et qu'il est malaisé de gérer les flux de population.

S'agissant de la communication en direction de la population, nous avons créé et mis en place les correspondants de défense. Il y a des référents à la défense et des correspondants dans les communes. Cette action a plus ou moins fonctionné mais elle doit être relancée avec le concours de l'association des maires. Le préfet que vous interrogez pourrait vous fournir des éléments, mais le SGDSN n'a pas compétence sur ce sujet.

Au sujet de la criminalité organisée dans notre pays ou dans les pays étrangers, je rencontre fréquemment mes homologues du *National Security Concil*, ceux des États-Unis, de Grande-Bretagne et d'autres pays en vue de mettre en place des structures et des dispositifs d'échange de lutte antiterroriste et contre la criminalité organisée. Mes responsabilités

précédentes au ministère de l'intérieur me permettent de souligner que nous faisons beaucoup d'efforts en ce domaine.

En matière de renseignement, les services du premier cercle que sont la direction générale de la sécurité intérieure (DGSI), la direction générale de la sécurité extérieure (DGSE), la direction du renseignement militaire (DRM), la direction du renseignement et de la sécurité de la défense (DRSD), la direction nationale du renseignement et des enquêtes douanières (DNRED) et Tracfin travaillent en étroite coopération. En ce moment même se tient une réunion placée sous l'égide du coordonnateur national du renseignement, destinée à faire le point sur l'ensemble des actions de coopération dans ce domaine. Les services du deuxième cercle sont censés étudier la prévention des crises sociales, des crises agricoles, des problèmes sociaux et sociétaux qui peuvent apparaître sur l'ensemble du territoire. Les services de renseignement de la police nationale et de la gendarmerie se coordonnent pour aboutir à une évaluation destinée aux préfets. La coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT) coordonne les uns et les autres, lesquels sont amenés à faire remonter des éléments.

J'ai vécu une expérience de mise en œuvre de moyens de sécurité civile quand j'étais préfet des Bouches-du-Rhône. Dans le cadre de l'entente interdépartementale en vue de la protection de la forêt contre l'incendie contre les feux de forêt, quatorze départements, sous l'égide d'un élu, mettent en commun leurs moyens de services départementaux d'incendie et de secours (SDIS), décident de faire ensemble leurs investissements et de coordonner leurs interventions. L'État met à leur disposition des moyens aériens et des renforts militaires (UISC), mais ils sont capables d'agir. Compte tenu du réchauffement climatique, le sujet des feux de forêt va devenir de plus en plus présent et il conviendrait de mettre en place, par zone de défense, des structures comparables, y compris contre les inondations, afin que les SDIS mutualisent leurs équipements lourds, au bénéfice d'un équipement renforcé de fourgons pompe-tonne contre les feux de forêt et de moyens d'intervention contre l'inondation.

Le service Viginum comprend une petite cinquantaine d'agents, dont des analystes placés sous la direction d'un ingénieur des télécoms membre de la Cour des comptes, donc magistrat, qui a travaillé dans différents services. Son équipe est composée de militaires, de civils, de veilleurs, d'analystes et des chercheurs qui, pour les élections, ont travaillé sous l'autorité du juge de l'élection et des autorités de contrôle du scrutin. J'ai présenté à deux ou trois reprises nos actions devant le Conseil constitutionnel et devant la commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP). Nous leur envoyions chaque soir des éléments sur ce que nous voyions ou sur ce que nous ne voyions pas, au sujet de ce qui pouvait menacer la sincérité du scrutin. Nous n'avons guère rencontré de difficultés, hormis des tentatives d'attaque visant à discréditer le système des votes électroniques et des attaques en désinformation de la part de différents États.

À ce jour, nous n'avons eu que quelques petites attaques mais rien de très sérieux, ce dont je me réjouis sur le fond et en termes d'efficacité. En venant vous présenter le projet, il y a un peu plus d'un an, je vous ai indiqué qu'il s'agissait d'appliquer le principe en œuvre contre les feux de forêt. Il faut arrêter la *fake news* le plus tôt possible pour éviter l'embrasement car, une fois propagée, on ne peut plus l'arrêter. Notre rôle n'est pas de dénoncer un mensonge, mais d'alerter sur le fait qu'on n'est pas en train de discuter avec M. ou Mme Dupont mais avec un agent des services de renseignement de tel pays et qu'on reprend un Tweet que l'on croit repris par 200 000 ou 300 000 personnes, alors que ce sont 200 000 ou 300 000 clics faits d'un bloc entre 1 h 05 et 1 h 07 du matin, vraisemblablement d'un endroit où les fonctionnaires travaillent, donc pas chez nous et vraisemblablement le fait d'un *bot*. Nous devons faire comprendre qu'une information en train de s'étendre peut être artificiellement amplifiée,

construite et développée et que l'on ne discute pas avec des gens comme vous et moi mais avec des agents qui reprennent un discours de propagande. Nous le voyons à la présence de fautes d'orthographe, d'anglicismes, de russicismes ou de mêmes faux accents aux mêmes endroits. Nous le faisons savoir, puis les gens jugent. S'ils considèrent que l'information vaut la peine d'être reprise, ils doivent savoir qu'elle a été montée, utilisée, développée par un État étranger ou le proxy d'un État étranger. Viginum a pour objectif la transparence et de pouvoir présenter comme telle une information venant de l'étranger et d'en tirer les conséquences. Le cas échéant, s'il apparaît qu'elle tombe sous le coup de la loi en raison, par exemple, d'attaques antisémites, nous saisissons la justice et en revenons à la bonne vieille loi de 1880 sur la presse.

M. Yannick Chenevard. En vous entendant rappeler le large spectre des missions de la SGDSN, je me disais que nous étions passés rapidement de la candeur habituelle de nos démocraties au monde réel. Sur les 1 300 agents du secrétariat général, 600, soit quasiment la moitié, travaillent sur les questions cyber, ce qui monte l'ampleur prise par le sujet. Vous avez cité une augmentation de 37 % du nombre d'attaques, sur une période assez large. Depuis janvier et février, se sont-elles intensifiées et quelles sont les cibles principales ?

M. Aurélien Saintoul. La stratégie nationale du renseignement n'incluait pas la vigilance à l'égard des épidémies, avait répondu la ministre Florence Parly à une question de Bastien Lachaud sur la détection de l'épidémie de Covid, alors que le Livre blanc mentionnait ce risque. Des enquêtes ont-elles été conduites à ce sujet ? S'est-on demandé pourquoi la vigilance n'avait pas été de mise ?

Où en est la mise en œuvre de la doctrine « Cloud au centre », présentée il y a un an ? Il semble que certains ministères ne se soient pas résolus à renoncer à l'utilisation du matériel Microsoft, comme on le leur avait pourtant suggéré avec insistance.

Quels sont les risques de dissémination d'armements en Ukraine, notamment de nos propres livraisons ? Je rejoins ainsi la préoccupation de notre collègue en matière de crime organisé. Nous avons connu une expérience douloureuse depuis les Balkans. Quels moyens sont mis en œuvre pour lutter contre cette dissémination ?

Mme Anne Le Hénanff. Dans les mois et les années à venir, les cyberattaques seront diffuses et simultanées. Quelle est votre réponse à de telles cyberattaques visant tous les pans de la société ?

Quel sera le rôle du SGDSN dans la gestion de la sécurité intérieure dans le cadre de l'événement que nous allons accueillir en 2024, qui va attiser les appétits et provoquer des risques ?

M. Frédéric Mathieu. La politique française d'exportation d'armements est fondée sur les principes de défense de la paix, de non-prolifération au travers de conventions internationales auxquelles nous sommes parties, et de sécurité nationale, forte de la constatation de bons que plus on vend d'armes aux quatre coins du monde et plus on a de risque de les voir nous revenir en pleine figure. Il en résulte un principe général de prohibition assorti de quelques exceptions. Force est de constater que la France est un grand exportateur d'armes. Songeons aux frégates multi-missions (FMM) destinées aux Russes, qui ont été revendues à cette grande démocratie qu'est l'Égypte, aux canons Caesar qui ont servi contre des civils yéménites ou à la vente à la Russie après l'embargo de 2014 par de nombreux pays européens, la France en tête, d'armes conventionnelles et de systèmes optroniques. Des responsables politiques et économiques n'hésitent pas à parler d'économie de guerre – je ne fais pas référence aux récents propos ambigus du Président de la République. Certains théorisent le fait que cela tire la

croissance vers le haut et beaucoup pensent que les armes sont des marchandises comme les autres qui peuvent être exportées aux quatre coins de la planète.

Vous présidez la commission interministérielle pour l'étude des exportations de matériel de guerre. Quel est le nombre annuel de licences attribuées ? Quel est le nombre de refus ? Qu'est-ce qui guide la politique d'exception au principe général de prohibition ?

M. le président Thomas Gassilloud. Nous aurons à la rentrée une audition dédiée aux exportations d'armement, après que le Gouvernement aura rendu son rapport annuel.

M. Xavier Batut. J'ai fait partie de la mission d'information sur l'incendie du site Lubrizol. Grâce aux personnels de l'entreprise, aux hommes du SDIS 76 et à nos sapeurs-pompiers, on a évité que cet incident industriel devienne une catastrophe. Les langues commencent à se délier sur la gestion de cette crise bien gérée au plus haut niveau de l'État et par le préfet. Des services de l'État ont bloqué les décisions, la réactivité et la programmation de décisions sur le terrain. Avez-vous un retour sur ces dysfonctionnements ?

J'avais interpellé plusieurs personnes sur le matériel qui, prépositionné au Havre dans le cadre du plan Polmar, avait permis d'éviter une pollution majeure de la Seine. Une réflexion avait été engagée à propos de la centralisation de ces moyens en Bretagne. Où en êtes-vous ?

Proche du centre nucléaire de Paluel et de Penly, je fais partie de la commission locale d'information (CLI) et de la commission locale d'information nucléaire (CLIN), censée informer et sensibiliser la population aux risques nucléaires dans le périmètre des plans particuliers d'intervention (PPI). Sans mésestimer l'action de cette dernière, l'information de la population est quasi inexistante, en particulier concernant l'extension des PPI à dix kilomètres. On est plus informé sur les incidents d'exploitation des sites nucléaires que sur la manière de régir par la population en cas d'incident, qui en est l'objectif premier.

Lors du dernier mandat, j'ai interpellé plusieurs responsables au sujet de la sécurité en Manche. Navigation, migrations, tourisme, plaisance, pêche, Brexit, environ mille bateaux se croisent tous les jours et les moyens de secours sont à Cherbourg ou à Dunkerque. A-t-on avancé sur ce sujet ?

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Je dis souvent à mes collaborateurs et à mes interlocuteurs que nous sommes payés pour être paranoïaques. Nous développons notre paranoïa en essayant de savoir ce qui ne va pas et ce qui va mal aller, ce qui est aussi un réflexe de préfet.

Les effectifs de l'ANSSI seront de 575 agents à la fin de l'année et, chaque année, ceux-ci augmentent d'une cinquantaine. Nous allons essayer d'accélérer ce rythme pour faire face aux évolutions, notamment à l'arrivée prochaine de la directive NIS (Network and Information System Security). Je vous communiquerai les chiffres exacts depuis les débuts de l'année (joints en annexe). En matière de rançongiciels, les grands fleurons économiques mais aussi les PME sont toujours ciblés.

Des cyberattaques par la criminalité organisée touchent de très grosses entreprises. Ce fut le cas d'un gros armateur qui a son siège sur la Côte d'Azur. Les rançons sont très fortes, mais on se protège. Certains groupes de criminalité organisée commencent à s'intéresser davantage à des entreprises moins protégées, comme des PME et des TPE. Nous avons observé un petit creux après le début de la guerre en Ukraine. Ils se sont employés à se frapper de chaque côté de la frontière, donc un peu moins sur nous. Moins d'hôpitaux ont été visés, parce que les cybercriminels se sont rendu compte que les hôpitaux n'ont ni le droit ni la capacité de payer.

Des menaces importantes continuent de peser sur les grandes infrastructures étatiques, administratives. Il s'agit souvent d'attaques d'État à État, visant à nuire et à placer des chevaux de Troie. La plus grosse difficulté dans ce domaine, c'est l'installation, dans les grands services publics ou ailleurs, de dispositifs que personne ne décèle et, le jour venu, on appuie sur un bouton et tout s'arrête. C'est un point sur lequel nous essayons vivement de réagir.

Les épidémies étaient exclues de la stratégie nationale de renseignement, parce que le renseignement s'intéresse d'abord aux risques d'attaques par certains États. Bien que nous travaillions beaucoup sur le risque nucléaire, bactériologique, chimique et radiologique, nous étions loin d'imaginer une telle épidémie. Nous essayons d'être paranoïaques, mais quand on parvient à anticiper un risque, par définition, on n'en parle pas, mais parfois, nous n'y arrivons pas.

L'ANSSI avec le MEFSIN travaillent à mettre en place des « Clouds de confiance », c'est-à-dire des Clouds qualifiés et répondant à des critères de sécurité et de protection détaillés dans un référentiel produit par l'ANSSI (SecNumCloud). Nous négocions et travaillons avec de gros opérateurs comme Microsoft et avec des entreprises françaises afin qu'ils mettent en place des offres « hybrides » qualifiées par l'ANSSI et supportant certains outils développés par des acteurs étrangers France France sans permettre aux pays d'origine d'avoir accès à des données sensibles (pour la sécurité économique, pour la protection des données à caractère personnel, etc.). Nous progressons avec certains, prenons du retard avec d'autres. Pour les Jeux olympiques de 2024, une négociation est en cours avec Alibaba, fournisseur officiel de Cloud pour les Jeux olympiques. Nous avons imposé d'avoir un Cloud souverain en France, qui nous permettra d'héberger et donc protéger en France toutes les données sensibles.

Concernant les risques de dissémination d'armements livrés à l'Ukraine, le SGDSN agit en coordination interministérielle et internationale. Nous essayons de mettre en place un dispositif pour assurer un meilleur contrôle. Nous encourageons la mise en place de ce dispositif, possiblement au niveau européen, en vue d'engager des discussions avec l'État ukrainien, les États voisins, l'ensemble des services de police et les autorités ukrainiennes pour organiser un traçage et un suivi de ces armements. Il ne faudrait pas que des éléments livrés puissent être utilisés contre nos intérêts. Je peux vous assurer que ce point est abordé chaque fois que nous parlons de l'Ukraine.

Nous sommes inquiets de l'évolution vers des cyberattaques diffuses et simultanées. Grâce à ses moyens renforcés, l'ANSSI, serait certes capable de faire face à quelques attaques simultanées menées par quatre ou cinq grandes unités identifiées, mais après, ce serait beaucoup plus complexe. Nous prévoyons de travailler plus efficacement avec des sociétés privées comme Orange, Thales, Atos ou Sopra Steria, qui proposent des services qualifiés et donc vérifiés par l'ANSSI sur différents segments. En fonction de leur expertise, elles peuvent agir au profit de différentes entreprises et les soutenir sur les questions de cybersécurité et cyberdéfense. Nous mettons en place avec les conseils régionaux des accords visant à créer des centres de réponse aux attaques dans chacune des régions, afin de développer un dispositif de cybersécurité au profit des PME, TPE, des entreprises locales et petites entreprises.

Pour les JO de 2024, selon l'accord passé entre la France et le comité international olympique, le ministre de l'intérieur est en charge de tous les aspects de sécurité, dans le cadre de ses responsabilités globales, ce qui ne nous n'empêche pas de travailler sur des sujets comme la protection face aux drones et aux attaques par drone, y compris sur le plan juridique. Un texte de loi a été adopté et nous nous penchons sur les décrets. Sur les sujets cyber, nous assurerons

la coordination nationale de l'ensemble des actions à mener. Bien entendu, nous travaillons aussi avec la délégation interministérielle aux jeux olympiques et paralympiques (DIJOP) et le comité d'organisation des Jeux olympiques (COJO).

Vous avez raison de souligner que les exportations de matériel de guerre sont, par principe, interdites. Nous ne le faisons que lorsqu'une qu'une autorisation ou une licence a été accordée ou renouvelée par l'État au profit de tel ou tel État, en tenant compte des engagements internationaux auxquels nous sommes soumis, des traités que nous avons signés, des risques d'utilisation de certains matériels. Par exemple, est exclue la vente de matériels pouvant servir, dans certains pays, au maintien de l'ordre public. Nous ne vendons plus rien qui puisse concerner le Yémen. Il y a un certain nombre d'autres États auxquels nous ne vendons pas ou sur lesquels nous mettons des réserves obligatoires pour faire en sorte que l'armement ne soit pas utilisé à autre chose que ce à quoi il est destiné.

Notre pays a une base industrielle de défense qui lui permet de ne pas dépendre d'États étrangers pour sa propre défense. La France essaie d'être un État autonome et indépendant.

M. Frédéric Mathieu. On en discutera à la rentrée !

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Je suis à votre disposition pour venir en parler. Les deux ministres concernés viendront vous présenter leurs rapports. Il importe que la France puisse disposer, pour son indépendance nationale, d'armements qu'elle produit et pour lesquels elle ne dépend pas du bon vouloir d'États étrangers qui décideraient de les fournir, de ne pas les fournir ou de les bloquer à un moment ou à un autre. Cela fait partir de notre vision de l'indépendance nationale. Si nous voulons préserver cette indépendance, nous devons vendre un certain nombre d'armements à certains pays.

La commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG) que je préside fait intervenir un certain nombre de ministères et opère un certain nombre de blocages en fonction de critères opérationnels, juridiques, internationaux, de respect des droits de l'homme. Vous trouverez les statistiques annuelles dans le rapport en cours de préparation, indiquant à qui nous avons refusé et à qui nous avons accepté. Nous pourrons vous faire le point, mais je vous garantis que le sujet avait été examiné lors de la précédente législature. Les présidents des deux commissions de la défense avaient demandé à Jean Castex un rapport plus fourni. C'est un sujet sur lequel nous sommes toujours très sensibilisés et pour lequel nous pourrons revenir devant vous.

Concernant Lubrizol, il est parfois compliqué de ne pas rencontrer d'obstacles de la part de certaines administrations. Lors de la crise Covid, on a interdit la mise sur le marché de masques considérés comme obsolètes. Il a fallu faire admettre qu'il valait mieux un masque dont l'élastique pouvait claquer plutôt que de les mettre à la poubelle et d'en manquer. De même, certains considèrent qu'on ne peut mettre tel médicament sur le marché parce qu'il pourrait avoir un effet secondaire, alors qu'on en a un besoin immédiat. En tant que préfet, il m'est arrivé de prendre des dizaines de décisions dont je savais qu'elles pourraient me conduire devant le tribunal, mais je préférais risquer un effet secondaire plutôt que de ne pas résoudre un problème. Cela veut dire aussi qu'il faudra revoir la planification en matière de catastrophe naturelle. Si le principe de précaution aboutit à ne rien faire en cas d'urgence on se met en situation de danger. Il faut concevoir différemment l'application du principe de précaution

Pour avoir été un « préfet nucléaire », ayant à présider des commissions locales d'information, je me plaignais déjà suffisamment de ne pas avoir d'information ou de les

découvrir en écoutant la radio le matin pour comprendre ce que vous voulez dire. Des améliorations sont en cours mais beaucoup reste à faire pour améliorer l'information. Cela fait partie des points dont nous discutons régulièrement avec EDF et les ministères concernés.

Nous échangeons souvent avec les Anglais sur la sécurité en Manche et en mer du Nord. Je ne parle pas des « small boats », sujet conflictuel sur lequel il est difficile de discuter, mais nous avons signé l'an dernier un accord intergouvernemental en vue d'examiner ensemble les conditions de sécurité des traversées transmanche, de mettre en place des moyens de réaction face à une attaque terroriste ou une attaque de criminalité organisée et pour mieux coordonner nos actions et nos informations. Dans le prolongement du Brexit, la pêche est un autre thème bien plus difficile à traiter.

En matière de secours, nous sommes convenus, la semaine dernière, avec mes homologues anglais de mettre en place des exercices pour s'assurer de la capacité des dispositifs de secours français et anglais d'intervenir ensemble de manière coordonnée sans être redondants.

M. Le président Thomas Gassilloud. Monsieur le secrétaire général, merci de vos réponses complètes et de votre action globale au service de la défense nationale.

*

* *

La séance est levée à douze heures quarante.

*

* *

Membres présents ou excusés

Présents. - M. Jean-Philippe Ardouin, M. Xavier Batut, M. Christophe Bex, M. Benoît Bordat, M. Hubert Brigand, M. Yannick Chenevard, Mme Caroline Colombier, M. François Cormier-Bouligeon, Mme Christelle D'Intorni, M. Emmanuel Fernandes, Mme Stéphanie Galzy, M. Thomas Gassilloud, Mme Anne Genetet, M. Frank Giletti, M. Christian Girard, M. José Gonzalez, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Loïc Kervran, Mme Anne Le Hénanff, Mme Murielle Lepvraud, Mme Alexandra Martin, Mme Pascale Martin, M. Frédéric Mathieu, Mme Lysiane Métayer, Mme Anna Pic, M. François Piquemal, M. Julien Rancoule, M. Aurélien Saintoul, Mme Isabelle Santiago, Mme Nathalie Serre, M. Michaël Taverne, M. Jean-Louis Thiériot, Mme Mélanie Thomin, Mme Corinne Vignon

Excusés. - M. Julien Bayou, M. Pierrick Berteloot, Mme Yaël Braun-Pivet, M. Steve Chailloux, M. Yannick Favennec-Bécot, M. sJean-Marie Fiévet, M. David Habib, Mme Delphine Lingemann, M. Olivier Marleix, Mme Michèle Martinez, M. Pierre Morel-À-L'Huissier, Mme Natalia Pouzyreff, Mme Valérie Rabault, M. Fabien Roussel, M. Mikaele Seo