ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

— Audition, ouverte à la presse, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale, sur la stratégie nationale de résilience dans le domaine de la défense et de la sécurité nationale.

Mercredi
6 mars 2024
Séance de 9 heures 30

Compte rendu n° 46

SESSION ORDINAIRE DE **2023-2024**

Présidence de M. Thomas Gassilloud, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures trente.

M. le président Thomas Gassilloud. Mes chers collègues, dans le cadre de notre cycle sur la défense globale, nous recevons aujourd'hui M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), que nous avons plaisir d'accueillir régulièrement, tant ses analyses synthétiques pertinentes et argumentées nous sont précieuses. Monsieur le secrétaire général, vous êtes placé auprès du Premier ministre, au cœur de la stratégie de défense globale, puisque vous assistez et assurez la bonne coordination interministérielle autour du triptyque anticiper-prévenir-protéger. Vous assurez également le secrétariat du Conseil de défense et de sécurité nationale (CDSN), présidé par le Président de la République et dont le champ d'intervention n'a cessé de croître ces dernières années.

Mes chers collègues, la recherche des dividendes de la paix depuis la fin de la guerre froide ne s'est pas accompagnée uniquement d'une baisse de crédits consacrés aux armées. Elle s'est également traduite par la perte d'une culture stratégique partagée au sein de la nation. Il nous semble urgent d'accompagner le redressement budgétaire permis notamment par les deux lois de programmation militaire (LPM) par une réappropriation d'un esprit de défense de la part de l'ensemble des citoyens. Tous les citoyens, tous les décideurs, tous les agents économiques doivent réapprendre qu'ils sont personnellement concernés par la défense de la nation.

Au-delà de la défense globale telle qu'elle était définie dans l'ordonnance des années 1950 et qui mobilise les services de l'État, nous devons également associer davantage les populations à cette défense, puisque nous sommes confrontés à de nouvelles exigences. Nos moyens militaires ont fondu du fait de la suspension du service national. Par ailleurs, l'hybridité des menaces concerne directement les citoyens qui peuvent être pris pour cible. À ce titre, nous avons lancé notamment deux missions d'information, l'une sur le rôle de l'éducation en matière de défense et l'autre sur le lien entre défense et territoires.

Dans le prolongement d'une mission lancée par l'Assemblée nationale en 2021, vous avez proposé une stratégie nationale de résilience (SNR). Adoptée en 2022, elle vise à mieux préparer les administrations nationales et locales, les entreprises et les citoyens à tenir dans la durée, collectivement et en profondeur, face aux crises. Pouvez-vous nous dresser un bilan provisoire de la mise en œuvre opérationnelle de cette SNR, et porter un jugement sur nos vulnérabilités face aux crises majeures ? Comment aider les acteurs concernés à mieux se préparer ?

Nous souhaitons également connaître votre regard sur le réseau des hauts fonctionnaires de défense et de sécurité et vos attentes concernant la commission interministérielle de la défense nationale (CIDN). Cette dernière me semble extrêmement essentielle pour penser le temps long au-delà de la gestion de crise, et traiter l'ensemble des sujets techniques. Enfin, le temps est venu le d'assumer le fait que les citoyens ont un rôle un peu plus important à jouer pour leur propre résilience, et que si l'État est à la hauteur de ses responsabilités, il ne peut pas tout.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. Je vous remercie de m'accueillir à nouveau au sein de votre commission. L'idée de résilience est issue des leçons que nous essayons de tirer de la pandémie de la Covid. Mais depuis lors, l'évolution de la situation géopolitique, économique, climatique, internationale élargit cette notion de résilience. Ainsi, l'impact de la guerre en Ukraine conduit à un changement profond dans notre approvisionnement en énergie, en matières premières. Tous

sont concernés : entreprises, collectivités locales, État. Cela nous conduit notamment à réfléchir sur le thème des stocks stratégiques pour faire face à une crise de cette ampleur. De même, la situation en Afrique soulève des questions d'approvisionnements et la guerre entre Israël et le Hamas engendre pour sa part une série de conséquences dont nous devons tenir compte.

Il faut également mentionner les menaces dites hybrides, celles que l'on peut difficilement attribuer. Il peut s'agir de cyberattaques ou de désinformations contre notre sécurité économique. Ces menaces s'accroissent et peuvent même nous faire perdre la guerre avant que l'adversaire n'ait montré un fusil, pour actualiser la célèbre image de SUN Tsu. Portées par les plateformes numériques, elles sont aujourd'hui plus rapides et efficaces que jamais pour faire perdre une guerre, affamer une économie, répandre les mensonges et le trouble au sein de la société, débrancher le numérique de nos activités, de nos services publics, de notre vie quotidienne. Nous le vivons tous les jours, à travers des attaques menées contre certains hôpitaux, certaines collectivités locales, certains services. Des pannes de système de cartes de paiement électronique peuvent également intervenir et celles, accidentelles, que nous avons connues récemment nous incitent à faire en sorte d'y répondre rapidement.

De fait, les adversaires sont nombreux, de plus en plus nombreux dont des États très puissants ; d'autres de taille largement inférieure ; des entreprises criminelles qui sont actives sur toute la planète ; des groupes idéologiques... Face aux menaces que représentent ces adversaires, nous nous appuyons sur le droit, la diplomatie et l'action militaire, le renforcement de nos dispositifs techniques, de nos systèmes informatiques. Mais rien ne peut aboutir si le peuple ne s'engage pas pour servir la collectivité, pour se protéger lui-même, pour être l'acteur de sa propre sécurité et pas seulement le consommateur.

De fait, l'histoire de notre défense nationale nous montre que depuis ses débuts, l'association et la prise en compte du peuple dans la défense de notre pays ont été au cœur de ces concepts. Gambetta a établi en 1871 le gouvernement de la défense nationale, avant que l'année 1932 ne voie la création d'un ministère de la défense nationale en tant que tel. C'est d'ailleurs à cette époque que s'est développé l'embryon préexistant du SGDSN actuel et qu'a débuté, à la conjonction du monde parlementaire et du monde militaire, la contribution de réflexions aux idées de défense. En 1959, lorsque Charles de Gaulle a pris l'ordonnance du 7 janvier portant organisation générale de la défense, il a rappelé le principe de la défense globale, qui confie à chaque ministère la responsabilité de préparer et d'exécuter les mesures de défense qui incombent à son département.

À la fin de la guerre froide, la période était aux « dividendes de la paix » et l'idée même de défense avait perdu sa dimension englobante, pour se focaliser sur des opérations extérieures et la lutte contre le terrorisme. Un autre concept a vu le jour : la sécurité nationale. Le Livre blanc sur la défense et la sécurité nationale de 2008 définit la stratégie de sécurité nationale comme ayant pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire, la permanence des institutions de la République et de déterminer les réponses que les pouvoirs publics doivent y apporter. C'est à cette époque que le secrétaire général de la défense nationale (SGDN) est devenu le SGDSN, intégrant cette dimension de sécurité nationale. Alors que la défense désigne une action, voire une réaction, et les moyens associés, la sécurité nationale désigne l'effet à obtenir un niveau beaucoup plus global, ce qui conduit le SGDSN à travailler sur la stratégie de résilience, mais également d'autres sujets, comme l'armement nucléaire, la politique nucléaire civile. Ainsi, un décret

paru au mois de décembre de l'année dernière et un texte de loi qui vous est actuellement soumis prévoient le rattachement au SGDSN du Haut-commissaire à l'énergie atomique.

L'article 410-1 du code pénal mentionne les intérêts fondamentaux de la nation, dont fait désormais partie la préservation de l'environnement. Nous travaillons donc à une forme élargie de la défense globale, telle qu'elle existait en 1959. Il s'agit bien de renforcer la capacité de notre pays à préserver le territoire, la défense militaire et la défense civile, notre économie, mais aussi d'autres champs, comme l'environnement et surtout, nos libertés, les valeurs qui fondent la République. La notion d'intérêts fondamentaux de la nation devient un outil essentiel pour fixer le cadre de la protection de notre pays.

Dans ce cadre, la stratégie nationale de résilience a pris une ampleur toute particulière. Nos objectifs s'organisent autour de trois axes : préparation de l'État aux crises, renforcement des ressources humaines et matérielles du pays, adaptation de la communication publique, soit soixante-treize actions pilotées par les ministères. Nous rendons compte de ces avancées au sein du Comité interministériel pour la résilience nationale, présidé par le directeur de cabinet du Premier ministre et qui s'est réuni à deux reprises en 2023.

Cependant, alors que nos stratégies sont historiquement centrées sur l'action de l'État, nous devons travailler maintenant sur l'information, l'éducation et la mobilisation des citoyens, la continuité de la vie économique et le soutien des collectivités territoriales, qui sont en première ligne sur les crises majeures. Dans le cadre de la SNR, nous œuvrons pour diffuser une culture de la continuité d'activité auprès de l'ensemble des acteurs, publics comme privés, susceptibles de s'engager dans la démarche de protection et de résilience, et les accompagner par la mise à disposition d'actions adaptées. Nous l'avons fait dans le cadre de la diffusion d'un guide de continuité d'activité, mais également par une série de réunions régulières avec les directeurs de cabinet des ministres, pour nous assurer que les plans de continuité d'activité dans les ministères sont bien en place. À ce sujet, il ne suffit pas de disposer d'effectifs spécialisés pour établir une cellule de crise. Tous les agents et les cadres du ministère doivent connaître la gestion de crise pour pouvoir organiser une relève dans le temps. Par ailleurs, tous les experts techniques doivent être en mesure de se mettre au service de la gestion de crise au niveau global.

Un deuxième élément concerne la contribution de la nation au soutien des armées engagées dans un engagement majeur, illustré par l'exercice Orion 3. Lorsque le chef d'état-major des armées (Cema) a mis en place l'exercice Orion, le plus important organisé sur le plan militaire depuis des années, il m'a proposé d'ajouter une partie sur la manière de travailler avec la société civile, pour qu'elle puisse à la fois bénéficier du soutien de l'armée, mais également se mettre à son service. Je pense notamment à la logistique, pour transporter rapidement des chars ou des approvisionnements, en faisant appel à des entreprises du secteur privé. Celles-ci sont prêtes à intervenir, mais encore faut-il pouvoir les enregistrer, les connaître et pouvoir avancer.

Deuxièmement, si nous enregistrons des blessés en grand nombre, le secteur de la santé doit pouvoir disposer d'une préparation et une organisation permettant de prendre en charge ce type de blessés résultant d'un dispositif de guerre. Troisièmement, il faut mentionner le dispositif des réserves. Nous bénéficions de gens capables et qui veulent s'engager, mais en cas de crise, il est nécessaire d'arbitrer sur les meilleures affectations possibles, c'est-à-dire celles où ils sont les plus indispensables. Or ce travail est assez compliqué. Confrontés au même sujet, les Suédois ont choisi de dresser un tableau des volontaires avant de mettre en place un dispositif, notamment à l'aide de logiciels, pour établir les affectations, le moment venu, en accord avec les personnes concernées.

La CIDN dispose de quatre groupes de travail sur la logistique, le droit, l'organisation interministérielle des réserves et de la mobilisation, les rétroactions sur le territoire national et le lien avec les territoires. Un nouvel exercice Orion aura lieu en 2026. En lien avec le Cema, le ministère des armées, mais aussi l'ensemble des autres ministères, je ferai en sorte de disposer d'une vue claire sur les personnes qui seraient disponibles.

Nous travaillons également au renforcement de la logistique interministérielle de crise et avons une cellule interministérielle logistique, dont le secrétariat permanent est assuré par le ministère de la transition énergétique. Elle a été activée pour la première fois le 25 septembre 2023, pour faire face à la pénurie d'eau à Mayotte. À ce titre, la commission a pu regarder les entreprises en France capables de produire rapidement des bouteilles d'eau en quantité et de résistance suffisantes. Au-delà des questions de logistique maritime, nous nous sommes par exemple rendu compte du risque d'écrasement des bouteilles en cas d'accumulation de palettes les unes sur les autres.

Nous travaillons également à renforcer les compétences des membres des cabinets ministériels en matière de gestion de crise, pour les sensibiliser aux enjeux de la sécurité nationale. Nous avons donc mis en place un guide particulier remis à tous les membres de cabinet pour leur expliquer les contraintes et risques auxquels ils peuvent être soumis (attaques cyber, espionnage, manipulation de l'information) et leur rappeler leur rôle dans la gestion de crise.

Nous menons en outre une série d'exercices gouvernementaux pour la préparation des jeux Olympiques et Paralympiques, qui ont pour objectif de traiter les catastrophes les plus improbables, afin d'être en mesure d'y faire face. Dans ce domaine, nous conduisons aussi une série de réunions pour vérifier que sur les sujets de téléphonie mobile, d'alimentation électrique, de sécurité internet et des paiements, nous puissions réagir de manière pertinente.

Au-delà de ces actions de professionnalisation des acteurs de la gestion de crise, il nous faut sensibiliser les populations, les collectivités et les entreprises aux risques majeurs, naturels et technologiques. Nous avons ainsi élaboré un module de sensibilisation du grand public en ligne consacré à la menace terroriste, sur le site internet Vigipirate. Mis en ligne en octobre 2023, il a été consulté à 5 000 reprises.

Nous avons également rationalisé la communication avec le service d'information du gouvernement (SIG) sur les risques et les menaces, à travers le portail https://www.gouvernement.fr/risques. Il présente également les informations concernant l'engagement citoyen, avec la réserve et le bénévolat. Nous travaillons avec le Centre national d'enseignement à distance (Cned) sur un module de sensibilisation par internet, à destination des élus locaux et des agents territoriaux. Nous ferons de même avec la direction de l'administration de la fonction publique. Nous allons par ailleurs essayer d'élaborer des guides semblables à ceux qui existent aujourd'hui en Suède ou en Allemagne concernant les réflexes de comportement, afin que la population puisse agir avec le minimum d'information et constituer les stocks adéquats, non superflus.

Enfin, nous avons refondu la planification de défense et de sécurité nationale. La nouvelle directive générale interministérielle a été adoptée le 23 janvier 2023. Nous y avons associé un outil numérique, Athéna, qui abrite l'ensemble de la planification de défense et de sécurité nationale, que nous avons déjà fait fonctionner lors des différents exercices. Ce dispositif facilite l'accès au plan pour l'ensemble de la communauté interministérielle et permet de mobiliser de manière plus agile l'ensemble des briques de planification. Nous nous

efforçons de produire des plans plus génériques accessibles, avec des fiches réflexes associées, particulièrement en matière sanitaire et travaillons avec le ministère de la santé à ce sujet. Par ailleurs, nous avons adopté un référentiel interministériel pour l'anticipation opérationnelle de la crise. Il s'agit d'avoir une équipe qui réfléchit sur ce qu'il faut faire « le jour d'après ».

Ensuite, nous allons devoir fortement travailler sur les stocks stratégiques. Il faut que nous puissions identifier, avec les ministères de l'économie et des finances et celui de l'agriculture, les approvisionnements critiques pour notre pays, en mettant à profit les données douanières, en bénéficiant d'une cartographie des vulnérabilités d'approvisionnement et en regardant la manière de mettre en place – et pour quelle durée – un dispositif de stocks. De manière corrélée, nous devons réfléchir aux conséquences économiques (immobilisations, bâtiments pour le stockage) pour les opérateurs d'importance vitale (OIV) de la constitution de tels stocks.

Ensuite, je souhaite revenir sur la question du réseau des hauts fonctionnaires de défense et de sécurité. Existant depuis 1959, il fonctionne plus ou moins selon les ministères et dispose de moyens variables. Les grands ministères régaliens (intérieur, défense, économie et finances) bénéficient ainsi d'équipes solides, de même que les ministères de l'agriculture et de la santé. Chaque mois, des réunions sont organisées au SGDSN pour les tenir informés de l'actualité et prendre en compte leurs besoins et leur dresser un état d'avancée de nos travaux. Je les rencontre également plusieurs fois par an. Nous devons cependant améliorer un certain nombre d'actions de formation, pour renforcer des éléments. De plus en plus, la responsabilité du service du haut-fonctionnaire de défense d'un ministère n'est plus un aboutissement dans la carrière, mais un point de passage utile pour pouvoir progresser et avancer. Là aussi, des efforts et des progrès considérables ont été accomplis. Autre accomplissement notable, le CIDN. Ce comité représente ainsi un des atouts du SGDSN, auquel nous tenons beaucoup.

Je souhaite également évoquer la directive européenne REC adoptée en décembre 2022, en même temps que la directive *NIS2* et le règlement *DORA* sur les services financiers ; trois textes portant sur le thème de la résilience. La directive REC concernera avant tout les OIV et, de manière marginale, les collectivités locales, si elles assurent elles-mêmes en régie des activités d'OIV sur l'eau, les transports, l'énergie. Nous avons beaucoup travaillé au niveau national sur cette directive et l'avons assez largement influencée son écriture à Bruxelles. Elle reprend les secteurs que nous avions proposés, les cadres d'action que nous avons pu mettre en œuvre, le corpus de règles communes déjà appliqué en France. L'objectif consiste ici à renforcer et améliorer l'interconnexion entre États, entre opérateurs, en matière de réseaux, de chaîne d'approvisionnement, de logistique et de réaction.

À cet effet, nous avons prévu plusieurs mesures, en complément de celles qui existent déjà dans le code de la défense. À l'intérieur de ces opérateurs d'importance vitale, la planification sera simplifiée et renforcée autour de l'objectif de continuité d'activité, avec une meilleure articulation entre la résilience physique et la résilience cyber. En cas d'absolue nécessité et de manière concertée, nous envisageons de demander à l'OIV de constituer des stocks stratégiques. Nous allons aussi renforcer le dispositif d'enquêtes administratives de sécurité, y compris sur les salariés étrangers de ces opérateurs d'importance vitale, de façon à pouvoir s'assurer que ceux qui sont présents ne posent pas de problèmes de sécurité. Nous pourrions enfin instaurer une obligation de notification des incidents majeurs qui, curieusement, n'existait pas, ni en informatique, ni en matière de sécurité.

Un dispositif de sanction sera en outre établi pour les OIV qui ne respecteraient pas les obligations. À ce sujet, le Parlement devra débattre du montant de ces sanctions. À

titre de comparaison, la directive en matière d'informatique prévoit jusqu'à dix millions d'euros ou 2 % du chiffre d'affaires mondial de l'entreprise.

La directive a été négociée pour respecter les prérogatives nationales et les enjeux de souveraineté. L'État reste le seul interlocuteur de ces OIV et nous avons évidemment pour instruction d'éviter de la surtransposer, exercice national auquel nos administrations ont parfois du mal à résister. Il a donc fallu que je retranche un certain nombre d'éléments, pour faire en sorte que le texte soit proportionné et adapté aux besoins.

Nous travaillons beaucoup avec nos voisins européens, mais tout particulièrement avec le Royaume-Uni, l'Allemagne la Finlande et la Suède, pays disposant également d'un dispositif sur la mise en œuvre des actions de résilience, l'adaptation au grand public, la capacité de pouvoir utiliser un certain nombre de leviers et des centres de gestion de crise efficaces. Nous devons continuer à échanger et partager avec eux.

M. le président Thomas Gassilloud. Je vous remercie pour cette présentation très complète, qui montre l'étendue de votre travail, et cède à présent la parole aux orateurs de groupe.

Mme Patricia Lemoine (RE). Monsieur le secrétaire général, au nom du groupe Renaissance, je vous remercie pour cette présentation très intéressante qui souligne la qualité de vos travaux, notamment sur l'élaboration de la stratégie nationale de résilience. Je profite également de l'occasion pour saluer l'excellent rapport produit en février 2022 par le président de notre commission sur ce sujet crucial de la résilience de la nation. Il était en effet indispensable d'entamer une réflexion sur son degré de préparation face à l'ensemble des dangers auxquels elle est exposée. À ce sujet, le contexte géopolitique particulier que nous connaissons actuellement et les nouvelles menaces hybrides dont vous nous avez parlé tout à l'heure, nous confortent dans l'idée que cet exercice était absolument nécessaire.

Le document de référence interministériel de la SNR précise que l'ensemble des acteurs concernés doit être associé dans le déploiement de celle-ci, l'objectif étant d'élaborer une défense inclusive permettant aux forces vives ancrées dans notre territoire de contribuer à renforcer la résilience de la nation, tout en développant une culture commune de la gestion de crise. Pourriez-vous, à cet effet, nous indiquer comment le SGDSN travaille avec des acteurs aussi variés que les collectivités locales, les entreprises, les chambres consulaires, les associations et les citoyens ? Des conventions partenariales sont-elles ainsi envisagées ou d'ores et déjà mises en place ? Pourriez-vous nous en donner quelques exemples ?

Sur le site internet du SGDSN, il est mentionné que le SNR fera également l'objet d'une large concertation pour la décliner auprès des collectivités et des opérateurs économiques ainsi que l'ensemble de la population. Pouvez-vous nous en dire davantage sur cette concertation ? En avez-vous déterminé les contours, les objectifs ? À cet égard et parce que vous avez aussi occupé différents postes de préfet, pensez-vous utile et nécessaire de voir évoluer les fonctions et le rôle des correspondants défense, qui sont désignés dans les communes et qui ont pour interlocuteurs les délégués militaires départementaux, afin d'en faire également des acteurs et relais à part entière dans nos territoires ? Lors de la crise sanitaire, le binôme préfet-maire a démontré toute son efficacité et il me semble intéressant de s'appuyer sur les collectivités pour agir efficacement.

M. Stéphane Bouillon. Nous travaillons intensivement avec les entreprises, les collectivités locales et les associations de citoyens. Lorsque nous avons commencé à œuvrer sur la transposition des directives, l'Agence nationale de la sécurité des systèmes d'information (Anssi) et la direction de la protection et de la sécurité de l'État du SGDSN ont

pris contact avec les présidents de Régions de France, de Départements de France, de l'Association des maires de France et des présidents d'intercommunalité (AMF) pour leur expliquer ce que nous envisagions de produire. Ce travail est toujours en cours à tous les niveaux, et j'ai d'ailleurs recruté dans chacune des deux directions concernées un spécialiste des relations avec les collectivités locales pour assurer un relais avec les techniciens de l'État et discuter avec les interlocuteurs sur le terrain.

Si cela s'avère nécessaire, nous établirons des conventions. Le travail doit par ailleurs intervenir entre les préfets, les maires et les présidents de conseils départementaux. Mon expérience de préfet m'a permis de cerner l'étendue des actions remarquables des maires sur le terrain, par exemple dans le cadre des comités communaux feux de forêt. Les dispositifs de coordination des différents services fonctionnent bien dans les endroits qui ont l'habitude d'être confrontés au plus grand nombre de risques, qu'il s'agisse des inondations, des feux de forêts, des séismes, des catastrophes techniques ou technologiques. Nous devons donc nous appuyer sur l'expérience déjà existante.

Les correspondants défense que vous avez mentionnés sont effectivement les interlocuteurs du délégué militaire départemental, mais j'ai tendance à penser que l'ensemble du conseil municipal, en particulier les adjoints spécialisés, les directeurs des services techniques et les directeurs généraux des services (DGS) de la collectivité, peuvent accomplir un travail considérable. Dans ce domaine, je crois profondément aux binômes président de conseil départemental-préfet, maire-préfet, président de communautés de communes ou d'agglomération-préfet, pour pouvoir avancer sur ce sujet.

Ensuite, dans un certain nombre de cas, par exemple pour les départements, nous allons demander d'accroître le niveau de résilience aux cyberattaques, dans la mesure où un grand nombre d'entre eux sont actuellement en difficulté sur ce sujet. Au sein du projet de loi qui vous sera également soumis, un certain nombre de dispositifs sont prévus pour conduire les « entités essentielles », les départements, les régions, les communes et intercommunalités de plus de 30 000 habitants à progresser sur ces sujets.

Les communes ou communautés de communes de moins de 30 000 habitants, appelées « entités importantes » ne seront pas soumises aux mêmes exigences. Nous leur demanderons simplement de procéder à des actions « d'hygiène », comme modifier régulièrement leurs mots de passe lors de l'achat de nouveaux logiciels, s'assurer qu'ils ont été certifiés et vérifiés et faire en sorte de disposer de sauvegardes débranchées du réseau informatique. Il existera également un partenariat entre les préfectures, les agences régionales de l'Anssi, les CSIRT (*Computer Security Incident Response Team*) régionaux.

Mme Caroline Colombier (RN). Au nom du groupe Rassemblement national, permettez-moi avant tout de vous remercier pour les riches éléments que vous venez d'exposer à notre commission. Votre intervention est d'autant plus importante que la stratégie de résilience trouve un écho particulier dans le contexte national et international tendu que nous traversons et au regard des échéances que notre pays va connaître prochainement avec les Jeux olympiques 2024.

Aussi, j'aimerais recueillir votre avis sur deux points qui nous paraissent essentiels. Lors de votre audition pour la mission d'information sur la résilience nationale, en décembre 2021, vous avez indiqué que la résilience individuelle de chaque citoyen est clé pour faire face aux crises. Vous aviez cependant conclu que cette implication dans l'action publique ne progressait pas en France. Dans la mesure où nous n'avons pas eu l'occasion de recueillir votre analyse sur les émeutes de l'été 2023, comment jugez-vous la capacité

individuelle et collective à faire bloc face à une telle crise ? Lors de ces quelques jours d'extrême violence, l'impression d'impuissance a surtout dominé. Le fait qu'une extrême minorité de nos concitoyens soit la cause de cette crise vous conduit-il à revoir la stratégie nationale de résilience ?

Enfin, au cours de cette même audition, vous nous aviez indiqué que l'une des leçons à tirer de la pandémie de la Covid était de nous assurer de garantir notre souveraineté dans un certain nombre de domaines dont vous venez de parler. Nous souscrivons totalement à cette recommandation, mais à l'heure où notre pays fait régulièrement face à des pénuries de médicaments, d'énergie, de carburant, de poudre ou de matières premières, êtes-vous inquiet que les constats que vous avez réalisés voilà plus de deux ans ne trouvent que peu d'écho dans la décision publique ?

M. Stéphane Bouillon. Nous sommes évidemment très sensibles à ce qui se déroule aujourd'hui en Ukraine. Les jeux Olympiques et Paralympiques et l'élection européenne constitueront par ailleurs un enjeu et une cible pour certains de nos compétiteurs étrangers. Comme je l'ai fait avant les derniers scrutins nationaux, j'organiserai le 29 mars une réunion pour tous les partis qui se présenteront à l'élection européenne. Seront ainsi présents, outre le ministère de l'intérieur chargé de l'organisation des élections, l'Anssi, Viginum et la direction générale de la sécurité intérieure (DGSI). La première partie sera consacrée à la présentation des risques, l'état de la menace et les dispositifs que nous mettons en œuvre, sous le contrôle du juge de l'élection, pour aider les candidats à y faire face. Dans une seconde partie, le Conseil d'État - compétent en premier et dernier ressort pour connaître des protestations dirigées contre l'élection des représentants au Parlement européen -, la Commission nationale de l'informatique et des libertés (Cnil) et l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) interviendront pour rappeler aux candidats les droits et les obligations auxquels ils peuvent être confrontés dans le cadre de l'action électorale.

Ensuite, la résilience individuelle est effectivement essentielle et me semble progresser. De plus en plus, les gens se sentent intéressés et concernés par leur capacité à jouer un rôle au sein de leur collectivité, de leur commune. J'ai le sentiment que, compte tenu de ce que nous vivons, mais aussi de nos actions informatives et explicatives relayées par les médias, un nombre croissant de personnes commencent à s'y intéresser et sont plus acteurs que consommateurs.

Les troubles de l'été 2023 relèvent de l'ordre public. Ne travaillant plus au ministère de l'intérieur, je ne peux donc vous répondre sur ces sujets. Je souligne néanmoins que les forces de l'ordre ont appliqué scrupuleusement l'ensemble des règles qui peuvent exister, l'ensemble des textes de loi, et ont fait en sorte que l'ordre puisse revenir, très rapidement. Je tiens d'ailleurs à les saluer, rendre hommage à leur savoir-faire, leur efficacité et leur discernement dans des moments qui auraient pu être extrêmement difficiles et dangereux. Pas plus sur ce moment que lors de la crise des gilets jaunes, nous n'avons tiré de conséquences en matière militaire ou de défense, car ces problèmes relèvent de l'ordre public « habituel ».

Enfin, nous travaillons actuellement sur les sujets de souveraineté et notamment les risques de pénurie. Le Gouvernement parle ainsi de relocaliser des usines de microprocesseurs en France, notamment dans le Nord. De même, le ministre de l'agriculture a mentionné la capacité à mettre en place des stocks et à prévoir un certain nombre de productions et d'activités sur le terrain. De la même manière, nous allons bientôt ouvrir une usine de production de paracétamol en France, puisqu'il n'y en avait plus, et nous nous

efforçons de faire en sorte que d'autres usines et d'autres activités de santé puissent se réinstaller, car nous avons tiré les conséquences de la crise sanitaire et de la modification de la mondialisation.

Mais ces efforts nécessitent du temps, des investissements et des investisseurs. De ce point de vue, la capacité renouvelée de la France à pouvoir attirer un nombre croissant d'investisseurs laisse penser que nous pouvons nourrir quelques espoirs de rapidement corriger ces éléments.

Mme Murielle Lepvraud (LFI-NUPES). En janvier 2023 a été publiée la directive générale interministérielle relative à la planification de défense et de sécurité nationale, dans laquelle les plans de continuité d'activité sont définis comme l'élément central de la résilience. Il est écrit que les secteurs fournissant des services vitaux doivent être en mesure de maintenir en permanence leurs activités à un niveau minimum socialement acceptable et de les ramener à un niveau de fonctionnement normal le plus rapidement possible.

Dans les secteurs fournissant les services vitaux, l'hôpital se place en tête de liste. Au-delà de l'état général de l'hôpital public, qui n'est en aucun cas dans une situation de maintien des activités à un niveau acceptable, je souhaiterais me pencher sur l'état du service de santé des armées. En octobre 2023, la Cour des comptes a ainsi publié un rapport qui s'inquiète de l'état de nos hôpitaux militaires. Elle indique que depuis 2015, les investissements réalisés dans ces hôpitaux sont inférieurs aux besoins, rendant le parc hospitalier vétuste. Par exemple, à l'hôpital d'instruction des armées Percy, la vétusté des équipements a atteint en 2021 un taux de 80 %, quand celui-ci était de 76 % à Begin.

Dans ce même rapport, les directeurs d'hôpitaux s'inquiètent profondément de l'impact de ce sous-investissement sur la qualité des soins dispensés. Nous pouvons aussi noter la baisse d'effectifs, avec 1 500 postes en moins entre 2010 et 2017. Il n'y a pas eu non plus de création de postes, malgré les annonces de 2020. Nous ne pouvons décorréler l'état du système de santé des armées de la question stratégique de la résilience. Le principe même de ces notions suggère la capacité pour ces hôpitaux d'absorber des flux importants de patients en cas de crise, ce qui nécessite de pouvoir fonctionner correctement. Pouvez-vous préciser ce qui est prévu pour pallier ces problèmes dans les hôpitaux militaires ? Le service de santé des armées est-il bien pris en compte dans la stratégie nationale de résilience ?

M. Stéphane Bouillon. Madame la députée, je suis au regret de ne pas pouvoir répondre à votre question. Ce sujet est indissociable de l'ensemble des sujets de santé, puisque ces hôpitaux travaillent également en liaison avec l'Assistance Publique - Hôpitaux de Paris (AP-HP), sur l'ensemble des moyens qui peuvent disponibles. Se surajoute un aspect militaire, avec la nécessité de pouvoir s'assurer que les personnels soignants ont fait l'objet d'une habilitation leur permettant d'avoir, le cas échéant, connaissance de secrets défense ou de certaines activités. Pour le reste, je me permets de vous renvoyer vers le ministre des armées, qui saura mieux que moi répondre à votre question.

M. le président Thomas Gassilloud. Monsieur le secrétaire général, vous avez évoqué tout à l'heure la prise de conscience sur le traitement des blessés et les questions logistiques. Pouvez-vous faire un point sur nos capacités civiles à faire face à une crise majeure en matière sanitaire ? À l'occasion de la Covid, nous avons pu constater que nos moyens étaient limités.

M. Stéphane Bouillon. Le dispositif des plans Blancs permet aux hôpitaux, lorsqu'ils se retrouvent en crise sur un territoire, de faire appel d'une part, à l'ensemble des

personnels de cet hôpital et, le cas échéant, de faire appel aux personnels qui travaillent dans d'autres hôpitaux publics. Des conventions peuvent également exister avec le secteur privé afin qu'il puisse assurer le relais et la coordination dans ce domaine. En outre, lorsque des crises surviennent régulièrement en outre-mer, nous sommes en mesure d'envoyer des personnels de métropole en soutien et en renfort.

Les plans Blancs sont régulièrement complétés et amendés, en tenant compte des moyens disponibles et de la crise qui peut exister dans ce domaine. De plus, un dispositif de réserve est aussi prévu, avec l'appel, le cas échéant, à des médecins récemment retraités qui sont prêts à pouvoir intervenir et aider. Enfin, un dispositif vise non seulement à mobiliser le secteur hospitalier, mais aussi le secteur privé, les infirmières du secteur civil, les pharmaciens, pour un certain nombre de tâches.

En résumé, le dispositif existe aujourd'hui sur le papier, de même que la planification. Il reste effectivement à pouvoir trouver les moyens et les équipements qui sont suffisants, mais en tout état de cause, les efforts consentis ont déjà été considérables et ils se poursuivront.

Mme Nathalie Serre (LR). Je vous félicite pour le travail accompli par Viginum et la communication qui en a été faite. Ce matin, vous avez énuméré le très grand nombre de missions qui vous ont été confiées. Quels sont vos effectifs ?

Ensuite, vous avez mentionné les kits de continuité dans les ministères. Or il existe déjà des ressources incroyables au niveau local, c'est-à-dire au niveau des communes et des collectivités. À titre d'exemple, dans ma circonscription, un adjudant du peloton de surveillance et d'intervention de la gendarmerie (PSIG) de Dardilly, a gagné un prix national pour la création d'un jeu à destination des enfants de maternelle, « Stop le loup ! », pour leur expliquer avec un langage adapté, comment se défendre face à une attaque terroriste. La ressource existe sur le terrain et elle est au contact du citoyen, pourquoi ne pas la privilégier ?

M. Stéphane Bouillon. Lorsque le Président du République m'a demandé de créer Viginum, j'ai rencontré le président de l'Assemblée nationale, les présidents de commission à l'Assemblée et au Sénat, les responsables des principaux groupes des deux assemblées pour leur expliquer notre démarche, dont nous vous rendons compte à travers notre rapport, mais aussi celui du comité éthique et scientifique que nous avons mis en place.

Je suis effectivement assez fier du travail que les personnels de Viginum réalisent, parce qu'ils sont capables de signaler que l'information reçue n'est pas de proximité, mais qu'elle émane de personnes installées par exemple à Saint-Pétersbourg, Pékin ou Ankara. Le système semble plutôt bien fonctionner et il nous faut à présent œuvrer avec le monde académique : nous devons davantage travailler avec les chercheurs, les universitaires, l'éducation nationale – et nous avons déjà commencé à l'accomplir – pour pouvoir mener une action d'information et d'éducation des jeunes, pour leur apprendre à se doter d'un regard critique sur les réseaux, et être en mesure de se questionner.

Enfin, il est exact que nos missions sont nombreuses, mais nous sommes un service interministériel placé auprès du Premier ministre. Environ 600 personnes travaillent à l'Anssi ; cinquante-cinq à Viginum, mais ils seront soixante à la fin de l'année ; 300 autres à l'opérateur de la sécurité des systèmes d'information interministériels qui nous fournit notamment les téléphones et les dispositifs sécurisés ; quand le SGDSN « historique » comporte environ 250 personnes.

Dans de nombreuses réunions avec des membres des cabinets des directeurs d'administration centrale ou des sous-directeurs, je passe commande pour des travaux d'anticipation sur tel ou tel sujet, par exemple la préparation des jeux Olympiques et Paralympiques, ou les conditions dans lesquelles dématérialiser les certificats d'enregistrement des personnes qui doivent être habilitées aux différentes notions de secret.

Ensuite, notre rôle consiste à produire des synthèses pour pouvoir donner au Premier ministre ou au Président de la République les éléments dont nous disposons, avec un certain nombre de propositions ou d'actions à mettre en œuvre. La charge de travail la plus importante sur ce sujet consiste à vérifier régulièrement que les dispositifs sont bien mis en œuvre, que les instructions ont été exécutées et que les projets puissent avancer.

Vous avez souligné à juste titre les atouts du terrain : le dynamisme, la volonté et la capacité à agir, essentiels. Je pense que les préfectures, les directions départementales interministérielles (DDI), produisent un important travail en complément des collectivités locales. Cela est peut-être moins aisé avec les administrations centrales, qui sont habituées à fonctionner en silo, mais je dois faire en sorte qu'elles s'intéressent à ce qui se passe à l'extérieur au quotidien, au-delà des situations de crise. Certaines administrations sont assez mobiles sur le sujet, comme celles de l'économie et des finances ; voire des ministères plus spécialisés comme l'agriculture ou l'éducation nationale. Il s'agit de pouvoir s'ouvrir, de regarder la manière dont les problèmes se posent et comment faire en sorte que cette démarche fonctionne à tous les niveaux des ministères, dans les DDI sous la houlette des préfets et dans les directions des services techniques sous la houlette des DGS dans les communes ou les départements.

Il revient aux services du Premier ministre d'impulser l'action dans ce domaine. Le secrétariat général du gouvernement (SGG) y contribue sous l'angle juridique, quand nous l'abordons sous l'angle de la défense et de la sécurité nationale.

Mme Josy Poueyto (Dem). La SNR repose entre autres sur l'anticipation des crises pour en atténuer les effets et faciliter le retour à la normale. En septembre 2021, quelques mois avant l'invasion de l'Ukraine. Un comité interministériel d'anticipation a été créé et se réunit deux fois par an pour proposer des recommandations. Cette action interministérielle est fondamentale et nous la défendons au groupe démocrate depuis la LPM du précédent mandat.

Le risque croissant des ingérences, des influences, des attaques cyber et autres déstabilisations des activités économiques, sociales, voire politiques de notre pays ont été bien identifiés. Aujourd'hui, les armes deviennent invisibles et notre problème concerne le brouillard de la guerre avant la guerre. Les Occidentaux appellent ce phénomène la guerre hybride, quand les militaires chinois ont théorisé dès 1999, leur guerre totale. Dans la même veine, la Fédération de Russie a explicité sa vision d'une guerre « nouvelle génération » dès 2014. Dans ce contexte, notre capacité d'adaptation est mise à l'épreuve.

Les collectivités territoriales et les élus locaux sont-ils correctement impliqués dans l'appréhension des sujets de défense, mais aussi suffisamment informés des risques et des menaces ? Le rôle du préfet est prépondérant à ce niveau. Par ailleurs, pensez-vous qu'il est suffisant de ne réunir que deux fois par an le comité interministériel d'anticipation ? Enfin, quel est votre regard sur la réalité de la guerre totale ou de la guerre « nouvelle génération » et sur sa prise en compte par les ministères, dont les champs de compétences sont parfois bien loin de ces sujets ?

M. Stéphane Bouillon. Le comité ministériel d'anticipation, que j'appelle également de manière imagée le « comité des paranoïaques », à la charge du « *what if ?* ». Nous réfléchissons aux conséquences de la survenue de telle crise, de telle action, à 360 degrés, c'est-à-dire non seulement en matière militaire, mais aussi économique, industrielle, sociale et sociétale. Par exemple, nous pouvons imaginer ce qui pourrait se passer en cas de rupture de satellites ou de l'usage des câbles sous-marins, de la même manière que nous avions réfléchi à un *black-out* d'internet. En résumé, nous essayons de voir les actions qui devraient être mises en œuvre pour faire face à telle ou telle situation, qu'il s'agisse d'une crise géopolitique ou d'une crise technologique. Dans ce cadre, nous sommes conduits à produire très régulièrement des rapports, qui prennent parfois du temps à être rédigés. Nous réfléchissons donc à long terme, mais de manière concrète et applicable. En résumé, cet outil nous semble précieux.

Vous m'avez également interrogé sur l'information des collectivités locales et des élus. Comme je l'ai indiqué précédemment, nous menons un travail avec le Cned pour mettre en place sur un site internet ce travail d'information à destination des élus et leur expliquer à la fois les enjeux, les difficultés et les réactions que nous pouvons apporter. Nous travaillons auprès du congrès des maires, aussi souvent que les collectivités ou les associations de collectivités nous y invitent.

Ensuite, tous les ans, je m'efforce de rendre visite aux préfets de zone de défense et de participer aux réunions avec les préfets de département, pour leur expliquer l'état de la situation, faire un point sur la géopolitique et les enjeux. Il est essentiel que les informations s'échangent et remontent notamment du terrain, à travers des dispositifs sécurisés d'ordinateurs ou de téléphones. Comme je l'ai dit précédemment, cela vaut également pour les administrations centrales habituées au travail en silo.

Deux fois par an, en compagnie de l'Anssi et sous l'égide du directeur de cabinet du Premier ministre, nous dressons un tableau des investissements en sécurité informatique menés par les ministères pour se protéger et renforcer leur surveillance et leur résilience face à différentes attaques. Sur ces sujets, le Premier ministre est également conduit à intervenir auprès des ministres et leur rappeler les dangers. Nous également sommes particulièrement vigilants aux tentatives d'espionnage, face à cette guerre dite hybride sous le seuil de conflictualité.

Mme Mélanie Thomin (SOC). Au nom du groupe socialiste, je vous remercie pour votre propos. Vous avez évoqué les enjeux de résilience de notre nation. Il me semble nécessaire de mieux définir ou de préciser ce terme. Faire face à une tempête ou faire face à une menace étatique n'implique pas le même conditionnement des citoyens, si ce n'est que l'État, dans les deux cas, dispose de marges de manœuvre et du devoir de s'améliorer dans l'accompagnement et la préparation des citoyens et de leurs élus.

Il faut renforcer notre préparation. Nous avons évoqué les plans de sauvegarde ou nos équipements, par exemple l'équipement en termes de lampes, de groupes électrogènes ; les réseaux de télécommunications ou les stocks alimentaires. Mais au-delà, sommes-nous prêts, à hauteur de citoyens ? Le renforcement de la résilience nationale, appelle à associer davantage les collectivités territoriales et les services déconcentrés de l'État. Dans la gestion de crise, le premier maillon inébranlable est la mairie, quand les plus vulnérables sont parfois les représentants de l'État eux-mêmes. J'ai en tête l'exemple de ce qui s'est passé dans ma circonscription au moment de la tempête Ciaran. Les maires ont ainsi assuré la continuité du service public pendant que la sous-préfecture était en grande difficulté, pendant trois jours.

Ensuite, que pensez-vous de l'association, dans vos fonctions, des enjeux de défense globale à ceux des enjeux de sécurité nationale dans le contexte actuel ? N'y a-t-il pas un intérêt à ce que la défense globale soit mieux appréhendée et surtout distinguée dans nos grands enjeux de résilience, en particulier dans nos territoires ? N'est-il pas opportun de donner un sens plus fort à la préparation face aux menaces étatiques par rapport à la gestion courante de notre sécurité intérieure et de notre gestion de crise un peu plus classique ? N'y a-t-il pas un champ plus ambitieux à défricher ?

M. Stéphane Bouillon. À l'origine, la résilience est un terme de physique, qui désigne la capacité d'un matériau à reprendre sa forme initiale après un choc. Ensuite, il a été décliné en psychologie pour caractériser la faculté de supporter un évènement traumatique et de retrouver un état précédent d'équilibre. Le terme s'étend au niveau des sociétés, des institutions et des organismes. Vous avez raison de distinguer la préparation à une tempête de celle à une attaque d'État, car chacune d'entre elles nécessite des actions singulières. Cependant, celles-ci seront toujours mises en œuvre par les mêmes personnes : le maire, le représentant local de l'État, les forces de sécurité.

Lorsque j'ai précédemment mentionné la planification, je vous ai indiqué qu'initialement, nous disposions de plans sur tout et n'importe quoi, mais qui étaient trop détaillés et assez peu applicables dans l'urgence par les principaux intéressés, qui n'avaient pas eu le temps de les lire. Nous nous efforçons donc de mettre en place des dispositifs de réaction de crise et de modification de planification qui, à partir d'un socle commun de dispositifs et d'organisations, permettent de réagir en s'adaptant à la nature des crises, qu'il s'agisse d'une tempête ou d'une attaque cyber.

Nous nous efforçons donc de progresser sur ces sujets et de renforcer notre préparation, sous différents angles. Je pense notamment à l'électricité, en travaillant avec la redondance des lignes électriques ou la redondance des lignes internet, pour établir des dispositifs de secours. Encore une fois, pour y parvenir, nous devons nous appuyer sur la représentation locale de l'État – préfets, sous-préfets – avec les directeurs départementaux, les maires et les présidents de conseils départementaux. Dans ce domaine, l'efficacité est la clef. Ces interlocuteurs connaissent le territoire, ses habitants, sa géographie et son économie, leur permettant de mettre en œuvre les solutions le plus efficacement possible.

Ensuite, nous n'agissons pas uniquement à travers le prisme de la défense globale. En matière de cybersécurité, dans la perspective des jeux Olympiques et Paralympiques, nous avons passé des contrats avec un certain nombre d'opérateurs du secteur privé, en plus d'un contrat avec le ministère des armées, pour venir au soutien de l'Anssi au cas nous subirions de très fortes cyberattaques et intervenir sur tel type ou tel opérateur qui serait mis en difficulté.

Nous allons également apporter notre concours pour les entités les plus importantes en matière de souveraineté nationale, qu'il s'agisse des administrations, des collectivités locales, des hôpitaux, mais également des médias, des transporteurs, c'est-à-dire tout ce qui, à un moment ou un autre, ne peut pas durablement tomber en panne sans entraîner des conséquences considérables sur les plans économiques, sociaux, sociétaux et de sécurité pour les personnes. Nous intervenons donc dans ces domaines, mais en liaison avec l'ensemble des autres acteurs privés et publics qui peuvent agir en la matière. Nous essayons de coordonner la défense de tous les ministères, de la rendre cohérente et de l'agréger pour que les différents intervenants puissent travailler efficacement, ensemble.

Mme Anne Le Hénanff (HOR). Ma question portera sur la cyberdéfense en particulier. En 2018, la France s'est dotée d'une véritable stratégie en matière de

cyberdéfense, dans le cadre de la revue stratégique de cyberdéfense organisée en trois parties. Ce Livre blanc dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la nation et ouvre des perspectives visant à améliorer le niveau de cybersécurité de la société française. Comme tout nouvel espace de souveraineté, il évolue vite et les menaces sont multiformes. C'est pourquoi la défense de notre pays doit s'organiser en conséquence. J'en veux pour preuve l'objectif stratégique numéro quatre, intitulé « Une résilience cyber de premier rang », de la revue nationale stratégique de 2022, ainsi que les 4 milliards d'euros alloués au cyber dans le cadre de la LPM votée en 2023.

Comme nous l'avons évoqué dans le rapport que mon collègue et moi-même avons eu le plaisir de rédiger sur les défis de la cyberdéfense, il est nécessaire de continuer à anticiper les défis de demain et ne pas attendre la prochaine LPM. Je sais qu'à la demande du Président de la République, vous vous y attelez activement, puisque vous travaillez depuis plusieurs mois à l'actualisation de la revue stratégique de cyberdéfense. Quels ont été vos axes de travail ? Comment s'est articulée cette mise à jour de la revue stratégique cyber avec la LPM avec la revue nationale stratégique ? Avez-vous souhaité faire se concerter différents acteurs et pour quelles raisons ? Enfin, pourriez-vous nous partager quelques-unes de vos pistes de travail ?

M. le président Thomas Gassilloud. Il me semble que l'Anssi a presque doublé ses effectifs en dix ans. Vous le confirmez, n'est-ce pas ?

M. Stéphane Bouillon. Je le confirme. Il s'agit là d'une des rares administrations d'État à bénéficier chaque année, sous réserve bien sûr de votre vote favorable, d'une augmentation d'effectifs et de moyens pour lui permettre de faire face à l'ensemble des enjeux auxquels elle est confrontée.

Madame la députée, nous travaillons en effet sur la refonte de la stratégie de cyberdéfense de 2018. D'abord, depuis cinq ans, le monde a complètement changé, et le cyberespace encore plus. Le nombre d'attaques a explosé et chaque jour, se produisent des événements qui nous conduisent à réfléchir à différents aspects. Le travail de révision engagé fonctionne autour des groupes de travail composés d'experts. Une concertation sera réalisée, y compris avec le Parlement. À ce sujet, nous avons d'ailleurs déjà tenu des réunions pour vous préciser l'avancée de nos travaux. Nous tiendrons compte de vos débats lorsque nous vous présenterons la transposition de la directive *NIS2* en droit français et nous serons susceptibles de formuler des propositions pour modifier éventuellement la législation. Soyez convaincus que nous sommes particulièrement attachés à assurer la liaison entre les uns et les autres.

Dans le détail, les groupes de travail portent sur des sujets précis : la gouvernance ; la méthode ; l'action l'internationale ; les investissements nécessaires ; les moyens ; les recrutements et l'attractivité des personnels dans ces installations. En effet, même si l'Anssi n'a pas de difficultés à recruter, compte tenu de son image de marque, la rotation du personnel demeure relativement important. L'enjeu consiste donc à fidéliser les personnels et faire en sorte qu'ils restent au-delà de leurs contrats de trois ans.

Nous devons être plus résistants face à l'agression, envisager la protection des entités les plus critiques, travailler sur les politiques de prévention, de sécurisation et d'accompagnement des victimes. Se pose également la question du partage de l'information, non seulement entre les techniciens, entre les techniciens et la justice, puisque des actions judiciaires peuvent être menées dans ce domaine, mais aussi entre techniciens et non-techniciens.

Enfin, il convient de mentionner l'évaluation de la sécurité des matériels et des logiciels, ainsi que la capacité à concevoir, produire et évaluer les moyens de chiffrement. Nous devons également travailler dans les domaines du quantique et de l'intelligence artificielle (IA). L'IA est un outil puissant, qui peut être utilisé par nos compétiteurs à notre désavantage, mais nous pouvons également nous en servir pour identifier les attaques et y réagir.

Un dernier enjeu concerne l'identité numérique, sur lequel nous travaillons particulièrement avec le ministère de l'intérieur et l'Agence nationale des titres sécurisés, afin d'être dotés de titres d'identités numériques disposant d'un niveau de sécurité élevé, le moins vulnérable possible.

M. le président Thomas Gassilloud. Je cède à présent la parole à mes collègues pour une série de questions complémentaires.

Mme Anne Genetet (RE). Je vous remercie pour vos propos, qui témoignent de l'étendue immense de vos activités et du périmètre de vos fonctions. Il est toujours rassurant de savoir que notre État se prépare à gérer un certain nombre de difficultés, voire de crises. Je voudrais notamment saluer le rôle important de Viginum qui, récemment encore, a mis au jour des menaces quotidiennes importantes et qui ne cessent de grandir. Je pense qu'il est important de révéler ces menaces.

Je partage avec vous l'idée qu'il est parfois difficile d'encourager nos entreprises à mettre en œuvre des plans de continuité d'activité. Je peux en témoigner, ayant moi-même eu la charge de plan continuité d'activité en Asie pour préparer des risques pandémiques de nature respiratoire en 2006, 2007 et 2008. À ce sujet, la stratégie de résilience nationale fait allusion à la ville de Singapour, que je connais bien. Aux pages 9 et 10, vous évoquez ainsi « *l'adoption du concept de défense totale en 1984, qui s'est imposée en raison d'un contexte historique et géopolitique très particulier – une cité-Etat sans profondeur stratégique, une forte dépendance du pays au commerce extérieur, une société plurielle* ». Vous ajoutez que « *l'apparition de nouvelles menaces justifie l'extension des domaines d'application de ce concept. La défense totale est présente dans tous les aspects de la vie des citoyens et réduit les libertés publiques, faisant de Singapour une démocratie hybride* ».

Je souhaite m'arrêter sur cette notion de libertés publiques réduites. Quels sont les moyens financiers dont vous disposez puisque nous, législateurs, pouvons être conduits à agir sur ces derniers ? Dans un contexte où les ressources sont de plus en plus rares, parvenez-vous à les mobiliser quand vous le souhaitez ? En effet, il est beaucoup plus long de former un ingénieur, un technicien spécialisé, que d'autres personnes. Les moyens juridiques dont vous auriez besoin vous manquent-ils aujourd'hui ? Où placer le curseur entre libertés publiques et continuité de l'activité, dans un contexte où nous sommes sous pression de visions politiques très favorables à des moyens autoritaires et de surveillance ?

M. José Gonzalez (RN). Monsieur le secrétaire général, je partage avec mes collègues le plaisir de vous auditionner aujourd'hui. Nous avons appris récemment que des officiers de l'armée allemande avaient été victimes d'espionnage sur des sujets hautement stratégiques. Quelles leçons pouvons-nous en tirer ? L'armée française est-elle suffisamment protégée contre ce genre d'attaque ? Par ailleurs, qu'en est-il de la capacité à empêcher par la suite la diffusion de ces informations ?

Enfin, le lundi 4 mars, un ordinateur contenant des plans confidentiels sur les Jeux olympiques et leur sécurité a été dérobé. Même s'il semble que les informations contenues ne soient pas sensibles, cet événement nous pousse à nous questionner sur la sécurisation de ce

type d'informations, la sensibilisation du personnel et notre capacité de résilience face à ce type d'attaque. Nous aimerions connaître votre point de vue.

Mme Lysiane Métayer (RE). Dans le contexte actuel, dans notre environnement stratégique fortement entravé par une succession d'événements malheureux, de l'extension de la conflictualité aux crises sanitaires et catastrophes naturelles, la stratégie nationale de résilience vise à renforcer la préparation de la France, de ses entreprises et de ses citoyens face à ces chocs, tout en respectant nos engagements internationaux et européens. De quelle manière cette stratégie nationale s'aligne-t-elle avec les engagements internationaux de la France en matière de sécurité et de défense et, en l'occurrence, l'Union européenne ?

M. Jean-Michel Jacques (RE). Ma question porte sur votre action de prévention, notamment les risques informationnels. Je souhaite aller un peu plus loin pour cibler le risque de désinformation à travers nos médias. Sur les plateaux de télévision, d'anciens ambassadeurs, préfets ou généraux interviennent et nous apportent fréquemment leur expertise. Mais leur qualité de retraité n'est pas toujours mentionnée par les médias qui les interrogent, ce qui peut parfois prêter à confusion. Cet exemple témoigne de la nécessité de sensibiliser nos médias en cette période de bulle informationnelle numérique maîtrisée par des compétiteurs extérieurs, où des images pourraient être récupérées pour être détournées. Quelle est votre action de prévention et de sensibilisation auprès de nos médias nationaux, afin d'éviter ce genre de problèmes ?

M. Jean-Charles Larsonneur (NI). Je souhaite revenir sur la question, toujours d'actualité, de nos câbles sous-marins. Quelles sont, selon vous, les principaux points de vulnérabilité que vous identifiez et auxquels vous cherchez à remédier ? Je pense à l'atterrage, aux stations à terre, à l'approche de côte sensibles, par exemple, au large de la Guyane. À quels scénarios vous préparez-vous concernant les déviations de flux de données vers des pays plus ou moins amicaux ? Pourquoi nos principaux opérateurs comme Orange marine ou Alcatel ne sont pas considérés comme des OIV ? Ce débat s'est déjà tenu, mais il mériterait peut-être encore d'être soulevé. Au fond, la résilience des acteurs sur un plan capitalistique constitue aussi un enjeu.

M. le président Thomas Gassilloud. À ma connaissance, la liste des OIV est classifiée, mais le secrétaire général pourra peut-être nous fournir des éléments à ce sujet.

M. Stéphane Bouillon. Madame Genetet, je travaille régulièrement avec mes homologues de Singapour, en particulier pour évoquer les conditions dans lesquelles ils luttent contre la désinformation. Par ailleurs, en tant que fonctionnaire, il ne me revient pas de qualifier le niveau de démocratie d'un pays.

Il est exact que la lutte contre la désinformation est délicate, car elle peut comporter des menaces sur les libertés publiques. C'est la raison pour laquelle les deux décrets qui ont présidé à la création de Viginum ont été soumis à l'avis du Conseil d'État et à celui de la Cnil, pour vérifier que l'ensemble des moyens que nous allions mettre en œuvre n'était pas attentatoire aux libertés individuelles et aux libertés publiques. Une note de l'assemblée générale du Conseil d'État en a conclu que, dans la mesure où Viginum garantissait la sincérité de l'expression des politiques pendant les élections, il correspondait effectivement à un objectif constitutionnel de préservation de la liberté d'expression et d'opinion. Nous sommes d'autant plus vigilants sur ce sujet que notre comité éthique et scientifique est présidé par un conseiller d'État.

J'aurais tendance à considérer que si nous commencions à trop réduire les libertés dans ce domaine, nos adversaires auraient gagné la partie. En conséquence, même si cela n'est

pas aisé, il revient au législateur de fixer le curseur entre les légitimes entraves aux libertés qui peuvent être mises en œuvre et la lutte face aux attaques de nos adversaires contre ces mêmes libertés. À ce titre, il me semble essentiel que le Parlement établisse ces éléments, avec l'appui éventuel du juge constitutionnel et du juge administratif.

Monsieur Gonzales, j'ai lu comme vous dans les journaux que des officiers allemands avaient été espionnés. Je peux vous indiquer que nous nous conformons à des processus de sécurité stricts. Lorsque je me déplace dans certains pays, on me donne un téléphone neuf, sans répertoire ni connexion internet.

De même, pour les conversations sensibles, nous utilisons des réseaux protégés, qui fonctionnent et sont efficaces. Les réunions téléphoniques se tiennent grâce au dispositif Osiris ; le dispositif Horus étant mis en œuvre pour les visioconférences ; ces deux systèmes permettant d'aborder des sujets classifiés. Nous avons également mis en place un téléphone protégé, à disposition des membres du Gouvernement et de certains très hauts fonctionnaires pour leurs conversations confidentielles mais pas classifiées. Un peu encombrant et moins ludique qu'un *smartphone* du commerce, il protège des attaques de sms cherchant à prendre le contrôle du téléphone, comme cela a pu être le cas avec Pegasus. Au-delà des outils existants, la discipline est essentielle et nécessite de bien respecter les consignes. Ceux qui sont coupables de négligence subissent les foudres, parce qu'ils ont commis une faute disciplinaire. Des retraits d'habilitation entraînant des changements de poste peuvent survenir. De fait, nous sommes assez sévères et stricts sur ce sujet, pour éviter le plus possible les compromissions et les fuites. Nos ordinateurs sont sécurisés, chiffrés et le cas échéant, peuvent être bloqués à distance, si des risques ont été identifiés.

Madame Métayer, nous avons travaillé sur les deux directives avec les institutions européennes, non seulement pendant la présidence française, mais aussi par la suite. L'Anssi est ainsi intervenue sur *NIS2* et la direction de la protection et de la sécurité de l'État sur REC. Comme je l'ai indiqué, le dispositif envisagé sur NIS2 s'inspire pour partie des idées et des actions que nous avons pu mener, notamment pour les OIV. Par ailleurs, nous maintenons des contacts réguliers avec nos interlocuteurs et homologues à Bruxelles. Nous avons interagi avec le groupe de travail sur les ingérences du Parlement européen, nous travaillons avec le service européen pour l'action extérieure (SEAE) et les différents commissaires en charge de ces dossiers. L'efficacité dans ce domaine impose évidemment que nous puissions agir au niveau européen, pour renforcer la solidarité européenne.

Monsieur Jacques, vous avez évoqué les actions de prévention et la désinformation à travers les médias. Il revient à l'Arcom de pouvoir réagir dans ce domaine et sur ces sujets. De la même manière, je ne m'occupe pas de la désinformation qui a pour origine et destination la France. J'estime que les médias, les parlementaires et les responsables politiques doivent être en mesure de contrer les déclarations provenant de tel ou tel cercle ou de telle ou telle identité, pour diffuser des fausses informations. De notre côté, nous avons la charge de la défense de notre pays, c'est-à-dire protéger l'intérieur de menaces extérieures.

Monsieur Larsonneur, nous sommes effectivement extrêmement vigilants et parfois inquiets en matière de câbles sous-marins, dont une grande partie de ceux qui assurent la liaison entre les États-Unis, l'Europe et l'Asie, traversent aujourd'hui le canal de Suez et la mer Rouge. À ce titre se pose la question de pouvoir disposer de câbles contournant l'Afrique, tout en la desservant également. N'importe qui peut, en raclant les fonds marins, couper ces câbles et occasionner des dégâts assez considérables.

À ce titre, quelques attaques ont déjà été recensées sur ce sujet dans d'autres mers et dans d'autres circonstances. Nous y sommes évidemment extrêmement sensibles et nous collaborons dans ce domaine avec les deux entreprises que vous avez citées, Alcatel Submarine Networks (ASN) et Orange. Je ne m'étendrai pas sur les mesures de précaution que nous pouvons mettre en œuvre, mais soyez certains que nous sommes extrêmement attentifs. Le SGDSN est très régulièrement en contact avec ces entreprises, pour évaluer les conditions dans lesquelles elles assurent leur propre sécurité et peuvent être amenées à intervenir au profit de leurs clients ou des intérêts fondamentaux de la nation. Des améliorations demeurent à apporter. Je n'en dirai pas plus en public, mais nous y travaillons.

M. le président Thomas Gassilloud. Je vous remercie, Monsieur le secrétaire général.

*

* *

La séance est levée à onze heures trente-trois.

*

* *

Membres présents ou excusés

Présents. - M. Mounir Belhamiti, M. Denis Bernaert, M. Pierrick Berteloot, M. Christophe Blanchet, M. Frédéric Boccaletti, M. Hubert Brigand, M. Vincent Bru, Mme Caroline Colombier, M. François Cormier-Bouligeon, Mme Geneviève Darrieussecq, M. Olivier Dussopt, M. Thomas Gassilloud, Mme Anne Genetet, M. Frank Giletti, M. Christian Girard, M. José Gonzalez, M. Pierre Henriet, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Loïc Kervran, M. Jean-Charles Larsonneur, Mme Anne Le Hénanff, Mme Gisèle Lelouis, Mme Patricia Lemoine, Mme Murielle Lepvraud, Mme Jacqueline Maquet, Mme Michèle Martinez, M. Frédéric Mathieu, Mme Lysiane Métayer, M. Pierre Morel-À-L'Huissier, M. Christophe Naegelen, Mme Josy Poueyto, M. Aurélien Saintoul, Mme Nathalie Serre, M. Philippe Sorez, M. Bruno Studer, M. Nicolas Thierry, Mme Mélanie Thomin, Mme Corinne Vignon

Excusés. - M. Julien Bayou, M. Christophe Bex, Mme Yaël Braun-Pivet, M. Steve Chailloux, M. Jean-Marie Fiévet, M. Sylvain Maillard, M. Olivier Marleix, Mme Pascale Martin, Mme Danièle Obono, Mme Valérie Rabault, M. Fabien Roussel, M. Lionel Royer-Perreaut, Mme Isabelle Santiago, M. Mikaele Seo, Mme Sabine Thillaye