ASSEMBLÉE NATIONALE

XVI^e LÉGISLATURE

Jeudi
6 avril 2023
Séance de 16 heures

Compte rendu n° 57

SESSION ORDINAIRE DE 2022-2023

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 et de M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), sur le projet de loi de programmation militaire pour les années 2024 à 2030.

Présidence de M. Thomas Gassilloud, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures cinq.

M. le président Thomas Gassilloud. Monsieur le Secrétaire général, nous sommes heureux de vous recevoir. Depuis le début du quinquennat, le Gouvernement comme les députés ont témoigné leur attachement à la vision de la défense globale qu'incarne le Secrétariat général de la défense et de la sécurité nationale (SGDSN). En effet, la dimension militaire ne peut plus être notre seule réponse face aux dangers et aux risques auxquels nous sommes exposés – et notamment aux stratégies hybrides. C'est la raison pour laquelle la cybersécurité fait l'objet des articles 32 à 35 de la loi de programmation militaire (LPM).

Vous êtes accompagné du nouveau directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Votre regard sur les grandes tendances du projet de LPM nous est particulièrement important, car il contribue tant au concept de défense globale que de résilience en cas de crise majeure. En effet, vous travaillez l'un et l'autre à une stratégie nationale de résilience.

Par ailleurs, le SGDSN joue un rôle important dans la phase 3 d'Orion. Alors que la LPM prévoit un doublement de la réserve militaire des armées, vous pourrez nous éclairer sur votre vision de la contribution de cette dernière à la résilience de la nation et de son articulation avec les réserves militaires, comme celle de la gendarmerie, ou civiles.

M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale. Le SGDSN, service de la Première ministre, a une spécificité historique : il se situe à la charnière du militaire et du civil, de la défense et de la sécurité, et de l'extérieur et de l'intérieur. Il a pour mission de coordonner – au-delà des périmètres ministériels stricts – les politiques relatives à la défense et la sécurité nationale.

C'est à ce titre que nous avons été chargés de conduire la rédaction de la Revue nationale stratégique (RNS), qui a servi de fondement à la préparation du projet de loi de programmation qui vous est soumis. Les lois de programmation sont généralement précédées d'exercices de revue stratégique, comme en 2007-2008 ou en 2012-2013, ou encore en 2017 à l'échelle du seul ministère des armées.

En 2022, au regard de l'accélération des tensions géostratégiques et de l'amplification des menaces, le Président de la République a demandé au SDGSN de piloter une révision de la stratégie de 2017, dans des délais contraints, et en coopération avec l'ensemble des ministères. Vous avez été consultés dans son état d'achèvement, et dans des délais très serrés. Vos apports ont été intégrés à nos travaux, comme vous avez pu le constater, Monsieur le président, lors du discours de présentation du Président de la République à Toulon le 9 novembre.

Je propose de rappeler les quelques éléments structurants pour la LPM dans lesquels le SGDSN tient un rôle particulier, soit comme partie prenante à l'interministérialité, soit comme opérateur responsable. J'évoquerai donc les articles figurant dans la partie normative du projet, qui ont trait à la cybersécurité, politique publique qui concerne désormais chaque secteur de l'État, et toute la vie de notre pays : à ce titre, c'est une responsabilité de la Première ministre, qu'elle confie au SGDSN et donc à l'Anssi – qui sera ainsi responsable du pilotage de la cybersécurité en préparation des Jeux olympiques de 2024.

L'Agence pourrait en effet bénéficier, si vous le décidez, de nouvelles prérogatives pour répondre à l'objectif stratégique n° 4 de la Revue : « une résilience cyber de premier rang ». L'objectif n° 9 propose « une capacité à se défendre et à agir dans les champs hybrides » : je vous dirai quelques mots sur les menaces dites hybrides, thème sur lequel le projet de LPM prévoit donc d'investir.

Enfin, je reviendrai sur une politique publique qui n'est pas strictement une politique de défense, mais plutôt une politique de sécurité nationale au sens large du terme : c'est le deuxième objectif stratégique affiché dans la RNS : « une France unie et résiliente ». Nous le déclinons dans la stratégie nationale de résilience, adoptée en mars 2021. Elle est contemporaine de la mission que votre Assemblée a conduite à votre initiative, Monsieur le Président, en 2021, sur le même sujet, et qui a nourri largement les travaux de préparation de la LPM. II nous faut donc maintenant concrétiser cette résilience, au sein de l'État et avec l'aide de collectivités territoriales et des entreprises.

Au premier chef, c'est la dissuasion nucléaire qui garantit depuis plus de soixante ans la protection du territoire national et de notre souveraineté. Le SGDSN assurant le secrétariat des conseils des armements nucléaires, il a donc des compétences en la matière. Notre premier objectif stratégique est donc de conserver la crédibilité et la robustesse de la dissuasion, clef de voûte de notre politique de défense et garantie de nos intérêts vitaux – dont la dimension européenne a été soulignée dans la RNS.

Cette crédibilité à la fois politique, opérationnelle et technique suppose une posture exigeante ainsi que des choix et des engagements capacitaires inscrits dans le temps long. La LPM atteste de cette exigence. Dans le contexte de guerre en Ukraine, et, plus largement de montées des tensions entre grandes puissances, avec la modernisation de leurs armements nucléaires qui en découle, le maintien de la crédibilité de notre dissuasion est indispensable.

L'augmentation continue de la cybermenace est l'une de nos préoccupations les plus constantes. Votre Assemblée elle-même l'a encore récemment expérimenté, comme nombre d'hôpitaux, de collectivités locales, d'entreprises et d'administrations. Depuis quelques mois, les cyberattaques – très probablement en provenance de Russie, au vu de leurs modes opératoires – tendent à se multiplier. Elles ciblent des pans entiers de notre société, de plus en plus numérisée et, à ce titre, de plus en plus vulnérable.

Outre la poursuite des efforts de prévention et de protection, une meilleure résilience cyber se caractérise par l'adoption de stratégies de réponses mobilisant l'ensemble des leviers. À travers le centre de coordination des crises cyber (C4), qui rassemble les armées, les services de renseignement, de l'intérieur ou administratifs, l'Anssi joue un rôle de bouclier – que nous nous devons de renforcer : c'est l'objet de plusieurs articles de la LPM, que M. Strubel vous décrira. Nous avons besoin de renforcer les capacités de détection de ces attaques par l'Anssi, et sa capacité à obtenir une coopération plus active des opérateurs : en effet, certains continuent à vendre des logiciels sans alerter les consommateurs des vulnérabilités qu'ils présentent. Pour y réagir, nous vous proposons de nous autoriser à obliger les opérateurs à signaler les vulnérabilités identifiées. L'aménagement de locaux de l'Anssi à proximité de ceux du ComCyber, à Rennes, permettra également de renforcer cette coordination entre l'épée et le bouclier.

J'en viens aux menaces hybrides. Je m'exprime régulièrement devant vous sur cette notion particulièrement plastique et englobante qui comprend à la fois les cyberattaques, les manipulations de l'information, l'instrumentalisation du droit et des normes et les atteintes à la sécurité économique. Il s'agit de « gagner la guerre avant de combattre », selon une expression souvent attribuée au chef d'état-major de l'armée russe, Valeri Guerassimov, et qui traduit en réalité la pensée de Sun Tzu : en effet, les tentatives de nuire à l'efficacité de l'adversaire par tous les moyens – y compris en semant le désordre et la division dans ses rangs – restent des pratiques courantes. Ainsi, la capacité à se défendre et à agir dans les champs hybrides constitue un objectif stratégique – et quelque peu novateur – de la RNS.

La France doit donc renforcer son organisation, pour mieux protéger – notamment – ses infrastructures les plus critiques, et ses entreprises les plus innovantes. Elle doit aussi se mettre en mesure de riposter dans tous les champs – notamment opérationnels – en développant à cette fin la nouvelle fonction stratégique « influence », à laquelle devra s'atteler, en particulier, la ministre de l'Europe et des affaires étrangères. Un groupe de travail interministériel a été créé sous notre égide en 2019. Il réunit la coordination du renseignement, le ministère des armées, celui de l'Europe et des affaires étrangères (MEAE), nos collègues du secrétariat général aux affaires européennes (SGAE), les ministères de l'intérieur, de la justice, de l'écologie, le service de détection et de prévention contre les ingérences numériques étrangères, les services de renseignement et bientôt le ministère de la recherche. Ce groupe de travail interministériel et interservices a rédigé en 2021 un document de référence interministériel sur les stratégies hybrides pour élaborer nos positions à l'international et notre réaction à l'intérieur. Le groupe de travail suit également attentivement les travaux des institutions européennes et internationales sur le sujet. S'il n'a pas vocation à jouer un rôle opérationnel dans la lutte contre les menaces hybrides, il rassemble les renseignements et procède à des évaluations ciblées de la menace hybride dans tous les champs contre la France et l'Europe. Il a par exemple réalisé une étude approfondie de la menace hybride russe dans le cadre du conflit ukrainien contre les intérêts français. Il est en lien avec le centre de renseignement (IntCen) de l'Union européenne.

De surcroît, le SGDSN est au centre de nombreux dispositifs : outre la cybersécurité, le SGDSN œuvre à la lutte contre les manipulations de l'information d'origine étrangère – qui relève des missions de Viginum –, à la sécurité économique – en lien avec le Service de l'information stratégique et de la sécurité économiques (Sisse) – et à la coordination interministérielle dans de nombreux domaines, tels que le *lawfare*, l'anticipation et la planification.

Je souligne à cet égard le rôle du comité de liaison en matière de sécurité économique (Colise), que je préside et qui est animé par le commissaire interministériel à la sécurité stratégique de l'économie : nous veillons à la sécurité économique de nos entreprises stratégiques et concourons à l'objectif de développer une économie de guerre.

Une importante dimension de la lutte contre les menaces hybrides repose sur la coopération internationale. Au sein de l'Union européenne, notre pays siège au sein du Centre d'excellence pour la lutte contre les menaces hybrides d'Helsinki créé en 2017. Son siège au conseil d'administration est occupé par le SGDSN. De même, et en lien avec le MEAE, le ministère des armées et le SGAE, nous participons à l'élaboration des positions de la France au sein du groupe horizontal créé par le Conseil de l'Union européenne en 2019 sur le thème des menaces hybrides. En matière d'évaluation de la menace, nous travaillons avec la cellule de fusion hybride (HFC) en charge du renseignement stratégique au sein du secrétariat aux affaires

étrangères de l'Union européenne. Enfin, le SGDSN a contribué sur cette partie aux travaux d'élaboration de la Boussole stratégique. Le SGDSN joue ainsi un rôle de pilote et de soutien, à la fois avec les grands États déjà organisés dans ce domaine, mais également avec les membres qui ont davantage de demandes à notre égard. Nous échangeons ainsi fréquemment avec les États baltes.

Cette action a vocation à s'amplifier : dans quelques mois, nous vous soumettrons un projet d'intégration dans le droit français des deux directives européennes Résilience des entités critiques (REC) et Network and Information Security 2 (Nis 2) , adoptées sous la présidence française de l'Union européenne. Ces textes, qui pousseront les États à mieux se protéger contre les menaces cyber et hybrides, et à renforcer leur résilience face aux crises, exigeront l'intégration de mesures supplémentaires dans le droit français. Ce travail devrait arriver à son terme en 2024.

Nous coopérons aussi avec l'Otan. La France travaille au sein du comité de la résilience, qui rassemble les directeurs nationaux en charge de la préparation civile. Nous échangeons régulièrement avec l'Otan à ce sujet, tout en veillant à ce que la prééminence de l'Union européenne soit bien respectée sur les questions de résilience. Dans ce domaine, nous contribuons ainsi à plusieurs des objectifs stratégiques de la RNS : « la France, un des moteurs de l'autonomie stratégique européenne », et l'objectif n° 95 : « La France, allié exemplaire dans l'espace euroatlantique ».

Enfin, nous devons renforcer notre résilience face à l'ensemble des risques majeurs auxquels nous pouvons être confrontés, qu'il s'agisse de catastrophes – naturelles, technologiques ou sanitaires –, d'actes militaires ou des conséquences d'attaques hybrides. Cet effort soutenu doit se déployer en métropole et en outre-mer, en associant étroitement les collectivités territoriales, les entreprises, les associations et la population.

Vous connaissez parfaitement cette question : les travaux engagés par l'administration, annoncés en mars 2021, progressent. Le directeur de cabinet de la Première ministre a installé le comité interministériel pour la résilience nationale le 1er février. Il a demandé une mobilisation volontariste des cabinets et des administrations centrales pour anticiper les crises systémiques auxquelles nous pourrions être confrontés. Ce comité sera de nouveau réuni avant l'été pour évaluer la progression des soixante-treize actions engagées : il y a quelques jours, nous avons transmis aux ministères leurs tableaux d'objectifs. En effet, nous devons nous préparer aux échéances de la Coupe du monde de rugby et des Jeux olympiques et paralympiques. Nous attendons donc des résultats de la part des administrations sur les objectifs tels que la consolidation des zones de défense et de sécurité ultramarines, la progression de la logistique interministérielle de crise, le renforcement de la continuité d'activité en temps de crise, la planification des stocks stratégiques, et la communication envers nos concitoyens afin de renforcer leur implication dans la résilience nationale.

De surcroît, le SGDSN poursuit son dialogue avec les associations d'élus afin de déterminer les meilleurs moyens de les associer à la démarche d'ensemble. Lors de la crise du covid, la véritable efficacité de l'action publique s'est déployée dès lors que la coordination entre le maire, le préfet et le président du conseil départemental a été opérationnelle sur le terrain. Dans les communes, nombre de comités communaux de prévention des risques naturels, des feux de forêt et des inondations ont démontré leur efficacité. Nous devons renforcer cette

dernière dans une politique de promotion de l'esprit de défense et de la communauté nationale, indispensable pour faire face à toute crise majeure.

Le développement d'une « économie de guerre » concourant à l'esprit de défense est aussi une condition essentielle de la résilience. Il s'agit de pouvoir mobiliser toutes les ressources de la nation en fonction des crises : les équipements, la logistique, les compétences humaines suffisantes, et désormais, des stocks suffisants et des sources d'approvisionnement sûres et redondantes. Cela implique d'encourager et soutenir des relocalisations de filières de production et de recyclage.

Dans ce cadre, nous avons joué la semaine dernière, avec le chef d'état-major des armées, et sous la direction du directeur de cabinet de la Première ministre, l'exercice Orion 3, qui visait à éprouver les aspects civils d'une grave crise de défense et de sécurité nationale affectant notre territoire. Cet exercice a été très utile : il nous a permis d'avancer sur un grand nombre de sujets relatifs à la contribution que les armées peuvent apporter à la défense civile, et d'évaluer l'apport que les autorités civiles, les entreprises, jusqu'aux réserves dans tous les domaines, peuvent apporter pour l'exécution des missions des armées.

Dans le cadre d'Orion 3, l'objectif du chef d'état-major des armées était de faire travailler les armées dans un scénario de haute intensité intégrant une composante politico-militaire. Celui du SGDSN était de mettre en perspective les travaux de la RNS, notamment en jouant le déploiement de la fonction protection-résilience, en actualisant les plans gouvernementaux pour faire face aux menaces et en assurant une capacité de relève par des réserves.

Nous sommes en train d'en tirer plusieurs enseignements, qui me semblent coïncider avec vos préoccupations concernant les armées. En premier lieu, nous savons que face à une crise importante, les moyens d'un seul ministère peuvent être rapidement dépassés. Dès lors, un effort national plus vaste devient nécessaire. Dans le cadre de l'exercice Orion, l'idée était de mobiliser les ressources du pays pour satisfaire les besoins des armées. Pour y parvenir, il faut d'abord identifier nos lacunes, puis les combler. La première est celle des stocks et des ressources. Nous ne pouvons plus appliquer la même doctrine qu'il y a vingt ans – le « *just in time* » et le « zéro stock ». Or nous manquons de conteneurs, avions et bateaux de transport. Et le recours à nos alliés ou aux réquisitions de moyens civils – envisagé dans plusieurs articles du projet de LPM – est loin de garantir la couverture des besoins.

En matière de transport stratégique, les moyens militaires étant utilisés, il peut être nécessaire de réquisitionner des moyens civils. Le commissariat général aux transports du ministère de l'écologie doit pouvoir les recenser, en développant une coordination efficace au sein de son administration.

Pour faire face à des dommages importants sur des infrastructures civiles, le programme Parades répertorie 12 0000 entreprises mobilisables dans les domaines du BTP, du transport, de la dépollution et des travaux forestiers. Nous devons toutefois veiller à sa constante mise à jour.

Dans le champ des approvisionnements pétroliers, en revanche, notre pays dispose de stocks stratégiques qui appartiennent aux opérateurs pétroliers et à la société anonyme de

gestion des stocks de sécurité, la Sagess. Ils sont utilisables et reconstitués régulièrement. En cas de besoin, une partie de ces stocks peut être prêtée, vendue ou réquisitionnée.

Les enseignements ne sont pas aussi positifs sur les capacités médicales et hospitalières. Il est prévu que le ministère de la santé prenne en charge les combattants blessés, tout en assurant la continuité des soins pour les patients civils. Le défi est de taille. Pour y parvenir, diverses mesures sont à prendre, dont le renforcement des stocks stratégiques de produits de santé – entamé après la crise du covid – et la mise en place d'une cellule logistique pour les approvisionnements. Par ailleurs, il faut organiser une chaine logistique particulière permettant de transporter un grand nombre de blessés, ce que ne permet pas le dispositif militaire actuellement. On doit alors aménager des bus sanitaires, des trains – y compris des TGV, comme durant le pic de la crise sanitaire – voire, envisager l'aménagement de navires-hôpitaux.

Enfin, l'alimentation est au premier plan de la satisfaction des besoins les plus élémentaires de la population. Pendant la crise du covid, les cinq grandes centrales d'approvisionnement ont bien fonctionné. Nous devons pouvoir passer des conventions avec l'ensemble des opérateurs privés, afin de garantir l'approvisionnement de la population et des forces armées.

Nous avons aussi travaillé sur les cadres juridiques, en nous demandant s'ils étaient suffisamment robustes. Vous vous souvenez combien ces questions juridiques sont prégnantes en temps de crise – et combien elles peuvent le rester après la crise. Au-delà de l'article 16 de la Constitution, de l'état de siège, de l'état d'urgence, bien documentés, et dont le cadre d'emploi a été traité par le Conseil constitutionnel, nous avons regardé comment appliquer le droit de la crise en cas d'engagement de haute intensité. Le code de la défense ouvre des possibilités à cet égard, notamment les dispositions qui ont trait à la mise en garde et à la mobilisation, figurant à l'art. L. 2141-1 du code de la défense. Ces régimes accordent d'ores et déjà plusieurs prérogatives au Gouvernement : droit de réquisition des biens, des services et des personnes, droit de contrôle de la répartition des ressources, ou encore pouvoir de rappeler ou maintenir les réservistes opérationnels des armées. Cependant, ces régimes n'ont jamais été activés et une réflexion complémentaire est nécessaire, mais ce sont là des pistes intéressantes qui ont été ouvertes, à droit constant.

Enfin, nous avons constaté que le droit commun ouvre des possibilités d'action et de contrôle, par exemple dans le domaine économique et notamment dans le champ de la BITD, mais des améliorations seraient utiles. Le projet de LPM propose ainsi de constituer des stocks de matière ou de composants stratégiques, et de faire traiter de façon prioritaire les commandes de l'État.

Je souhaite finalement évoquer les réserves, sans lesquelles nous ne pouvons tenir dans la durée : en effet, la pandémie nous a rappelé qu'une crise n'était pas nécessairement un évènement bref, limité dans le temps et dans l'espace. Nous devons donc veiller à pouvoir disposer de réserves dans tous les champs de la crise. Or, nous avons identifié des faiblesses.

D'abord, le cadre législatif et réglementaire actuel nous permet de mobiliser des réserves civiles et militaires, mais il est basé sur le volontariat : le volume et les capacités qu'il garantit ne sont pas toujours adaptés aux besoins. Ainsi, une meilleure lisibilité est nécessaire entre les réserves obligatoires et les réserves contractuelles. Deuxièmement, le processus opérationnel de mobilisation des réserves est perfectible, notamment pour 1'identification des postes à

pourvoir prioritairement, afin d'éviter des effets d'éviction. Un effort de typologie et de description des emplois devant être prioritairement pourvus est à faire. Il faut aussi dépasser la seule approche du « complément individuel » pour y adjoindre une compétence de réserve en unité constituée. Enfin, les lacunes juridiques et opérationnelles imposent une gouvernance structurée, au niveau central comme dans les territoires, qui rassemble chacun des éléments et des professions. Chaque ministère gère ses réserves : mais il faut les coordonner afin de s'assurer que nous disposerons des bons renforts au bon moment.

M. le président Thomas Gassilloud. Je salue votre travail préparatoire à la LPM, qui témoigne à la fois d'une détermination et d'une humilité aussi remarquables qu'indispensables à l'égard de la résilience.

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). L'Anssi, que j'ai l'honneur de diriger depuis près de trois mois, incarne un modèle français de la cybersécurité qui permet à la France de se tenir au premier rang des pays en la matière.

Ce modèle se caractérise d'abord par notre choix de séparer l'épée et le bouclier : l'Anssi n'est pas un service de renseignement, ni de police ; elle est chargée de la cybersécurité. En outre, dans l'organisation de l'État, cette mission relève directement de la Première ministre et revêt une dimension interministérielle qui constitue un atout majeur pour organiser la cohérence d'ensemble du dispositif national de cybersécurité.

L'Anssi doit remplir trois missions. La première est la réponse aux attaques : il ne s'agit pas de contre-attaquer, mais de détecter, comprendre, alerter et remédier, directement ou par le biais de prestataires, aux conséquences des attaques. La deuxième mission de l'Anssi consiste à sécuriser l'État et les activités d'importance vitale. Pour la mener à bien, vous nous avez accordé des pouvoirs réglementaires qui nous permettent de contraindre une administration ou un opérateur d'importance vitale à renforcer sa sécurité. Enfin, l'Anssi est chargée de protéger nos concitoyens, dans un rôle de conseil des politiques publiques en lien avec la cybersécurité, de mobilisation d'un écosystème de prestataires privés, de construction d'une offre de formation pour développer la cybersécurité et l'étendre à toute la société.

Nous exerçons ces missions dans un contexte d'augmentation sensible de la menace. Alors qu'elle restait très concentrée sur quelques acteurs qui se distinguaient par leur taille ou leur visibilité, cette menace touche désormais nos établissements de santé, nos PME ou encore nos collectivités. Elle est de trois ordres : il s'agit d'abord d'une menace stratégique, qui perdure et reste concentrée sur les activités régaliennes. Des États en sont généralement à l'origine. S'y ajoute une menace à vocation lucrative, qui est le fait du crime organisé, et dont le mode opératoire privilégié est le rançongiciel. Enfin, la menace revendicative – dont vous avez récemment été victimes – se contente de saturer des sites internet pour les rendre inaccessibles, sans dégâts pérennes, mais en engendrant une importante visibilité.

Cette menace touche tout le monde – particulièrement la menace criminelle à but lucratif. Son impact est évidemment inacceptable, notamment lorsqu'elle touche des hôpitaux, qu'elle remet en cause la délivrance de services publics de proximité ou qu'elle met en danger la santé de nos entreprises, en particulier les PME.

Cette menace évolue aussi sur le plan technique : une convergence s'est opérée entre les outils utilisés par les attaquants de nature stratégique – les États – et le crime organisé. Elle s'est industrialisée, pour viser massivement un secteur d'activité entier, ou, au contraire, sélectionner très précisément ses cibles. Enfin, nous avons vu se développer son agilité, c'est-à-dire sa capacité tant à s'adapter aux technologies qu'à trouver des parades à nos propres réponses.

Cette menace repose sur des vulnérabilités connues des systèmes d'information, qui font souvent l'objet de correctifs publiés par des éditeurs, mais qui ne sont pas appliqués. En l'absence de telles vulnérabilités, cette menace sait contourner les défenses les plus fortes pour s'attaquer aux maillons faibles, en s'attaquant par exemple aux sous-traitants d'activité critique ou en ciblant de nouveaux usages mal appréhendés en matière de sécurité, comme le cloud.

Une attaque de cybersécurité se déroule en plusieurs phases, qui durent parfois plusieurs semaines ou plusieurs mois. La reconnaissance en est la première étape : l'attaquant – sans action visible – cherche à comprendre sa cible et à déterminer ses vulnérabilités. Il procède ensuite à une intrusion initiale par laquelle il pénètre dans le système d'information. Suit l'escalade des privilèges : l'attaquant essaie d'outrepasser les droits qu'il a pu obtenir lors de la phase d'intrusion initiale et de récupérer des droits d'administration pour prendre le contrôle de l'ensemble du système d'information. Vient enfin la phase d'exploitation, lors de laquelle l'attaquant va exploiter l'accès qu'il a obtenu pour atteindre son objectif.

Il n'y a jamais de lien direct entre un ordinateur à la main d'un attaquant et celui de la victime. En effet, les attaquants passent par des rebonds multiples sur des systèmes intermédiaires afin de masquer leurs traces : il peut s'agir de serveurs qu'ils ont loués eux-mêmes, ou de systèmes de tiers, qui, sous le contrôle de l'attaquant, participent à leur insu à une attaque. Ce chemin de commande et contrôle garantit aux attaquants leur anonymisation et leur persistance. La remontée de ce chemin est l'un des enjeux clés de l'analyse de cette attaque, du déploiement de parades et dans l'alerte de potentielles victimes.

Au défi fondamental de massification des attaques s'ajoute celui de la massification des bénéficiaires. La directive européenne NIS 2 publiée en décembre devrait multiplier par dix ou vingt le nombre d'opérateurs assujettis à des règles de cybersécurité et tombant dans le champ de responsabilité de l'Anssi. Cette massification engendre ainsi un enjeu d'efficacité et de célérité dans les réponses aux attaques. Il nous faut mieux anticiper les vulnérabilités, plus vite identifier les victimes potentielles, comprendre mieux et plus rapidement les attaques et leur évolution, et pouvoir, dans des cas extrêmes, les bloquer au moins temporairement.

Cette finalité de gain d'efficacité est visée par les articles 32 à 35 du projet de loi : ils complètent, en en tirant les bilans, les articles de la LPM de 2018 qui nous avait déjà dotés de certaines capacités en la matière. Elle avait instauré pour la première fois un régime de contrôle de ces activités, reposant sur l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), et distinct de celui assuré par la Commission nationale de contrôle des techniques de renseignement (CNCTR).

Les articles 32 et 33 concernent le système de noms de domaine (DNS). Ce protocole universel et fondateur des réseaux internet consiste à transformer un nom de domaine en adresse IP, c'est-à-dire une suite de chiffres utilisée pour identifier une machine et acheminer les flux au sein des réseaux. Ces services DNS, qui sont opérés par des fournisseurs d'accès ou des acteurs spécialisés, interviennent à leur insu dans les attaques pour accéder au système de leurs

victimes. Les articles 32 et 33 capitalisent sur le rôle du DNS pour augmenter notre efficacité opérationnelle. L'article 32 propose d'étendre le régime de blocage de certains noms de domaine – qui existe dans le cadre de la lutte contre la pédopornographie en ligne ou les appels au terrorisme – au domaine de la cybersécurité. Deux régimes seraient établis : le premier permettrait à l'Anssi de demander aux propriétaires légitimes d'un nom de domaine, attaqués à leur insu, de prendre toute mesure visant à évincer l'attaquant qui se sert de leur serveur, ou de bloquer le nom de domaine s'ils n'y parviennent pas. Le deuxième régime concernerait les noms de domaine détenus par l'attaquant lui-même : il permettrait alors le blocage immédiat des flux. Ces dispositifs auraient une utilisation limitée : ils ne visent en rien à procéder à des blocages massifs. Toutefois, ils seraient très utiles pour jouer un rôle de frein d'arrêt d'urgence en cas d'une vague d'attaques massive, par exemple lors des Jeux olympiques.

L'article 33 vise à nous donner accès à l'historique des serveurs de DNS – c'est-à-dire l'historique de la traduction d'un nom de domaine en adresse IP –, sans inclure les adresses IP des demandeurs qui auraient cherché à accéder directement au site internet. Ces informations, dont disposent de manière générale les fournisseurs de ces services, nous seraient très utiles pour contribuer à la compréhension d'une infrastructure d'attaque, pour contribuer à son suivi dans le temps, pour mieux les entraver, et, surtout, mieux anticiper les prochaines victimes.

Dans un autre domaine, l'article 34 du projet de LPM porte une obligation de notification des vulnérabilités ou des incidents de sécurité connus par les éditeurs de produits numériques qui commercialisent ces derniers sur le marché français, auprès des utilisateurs et de l'Anssi. Cette pratique est bien établie chez les principaux éditeurs tels que Microsoft, qui publie chaque mois une liste de vulnérabilités de ses produits et des correctifs associés. Cependant, elle est moins courante chez les petits éditeurs très spécialisés, par exemple dans le domaine de la santé.

Par ailleurs, cet article vise à répondre à une forme d'incertitude juridique sur les informations qui peuvent être transmises à l'Anssi dans un tel contexte. En effet, au-delà de la notification aux utilisateurs, il est intéressant que l'Anssi soit informée de telles vulnérabilités, car elle peut coordonner elle aussi la réponse, prendre contact avec les utilisateurs, notamment quand ils sont identifiés comme porteurs d'une activité d'importance vitale, et les enjoindre, le cas échéant, à appliquer des correctifs rapidement.

Enfin, cet article évoque les incidents significatifs connus par les éditeurs, comblant un vide juridique : s'il est bien établi dans les pratiques que les éditeurs partagent les vulnérabilités de leurs produits, ils ne communiquent pas aussi volontiers sur les incidents de sécurité qu'ils ont eux-mêmes connus – c'est-à-dire les attaques qui se sont propagées à leur infrastructure. Or, ces attaques sont aujourd'hui des vecteurs majeurs d'infection.

Pour finir, l'article 35 tire le bilan des dispositions introduites par la loi de programmation militaire de 2018. Il clarifie et étend notamment le cadre de détection des attaques par les opérateurs de télécommunication. La LPM de 2018 avait créé un article L. 33-14 dans le code des postes et des communications électroniques, qui permettait aux opérateurs de communications électroniques de se doter de capacités de détection des attaques et précisait les modalités de déploiement de ces capacités. Or, cette possibilité – qui n'était pas une contrainte – a été très inégalement exploitée par les opérateurs. Tirant le bilan de ce constat, l'article 35 propose de créer une obligation de mise en place de capacités de détection, et l'assortit d'un régime de juste rémunération des investissements consentis par les opérateurs en

ce sens, puisque ces actions sont conduites dans l'intérêt commun. Il précise, et étend par ailleurs, le périmètre des données qui peuvent être recueillies au titre de l'article L. 2321-2-1 du code de la défense – également issu de la LPM de 2018 –, qui permet à l'Anssi, dans le cadre de l'identification de victimes et de la compréhension d'attaque, d'accéder à des données traitées par les opérateurs. L'article 35 précise que cette analyse peut porter sur des données de contenu dès lors qu'elles sont liées à la menace observée, ce qui n'est pas l'interprétation retenue actuellement par l'Arcep ; pourtant, nous considérons au regard des débats parlementaires de l'époque que le législateur avait bien l'intention de nous donner accès à ces données, lequel est rendu plus nécessaire encore par le niveau de sophistication des attaques, dont l'analyse ne peut plus uniquement reposer sur l'accès aux métadonnées.

Cet article étend également ces modalités d'accès aux données traitées dans les centres d'hébergement, qui sont très largement utilisés par les attaquants pour louer des serveurs faisant partie de leur infrastructure. Il élargit le motif d'utilisation de ces dispositions – très centré dans le texte existant sur les atteintes aux services essentiels, aux activités de l'État et aux autres activités d'importance vitale – aux sous-traitants de ces opérateurs, puisque ces derniers sont désormais souvent plus ciblés que les opérateurs eux-mêmes.

L'article 35 renforce le contrôle déjà exercé par l'Arcep sur les dispositions de 2018. Les autres articles introduisent également les modalités de contrôle renforcées par l'Arcep pour encadrer ces dispositions nouvelles.

Ces mesures nous paraissent indispensables pour relever le défi de la massification des attaques. Elles sont justement proportionnées aux enjeux, et assorties de limites, de garanties et de modalités de contrôle visant à préserver les droits et libertés de nos concitoyens dans le traitement de ces menaces.

M. le président Thomas Gassilloud. Je vous remercie pour ces explications, et vous félicite pour votre nomination. Votre engagement est plus que jamais nécessaire, car vous êtes chargé de tenir le bouclier numérique de notre nation. Je donne la parole aux représentants des groupes, en commençant par M. Berteloot qui est attendu à l'hémicycle.

M. Pierrick Berteloot (RN). Les menaces cyber sont de plus en plus palpables. De plus, les formes et les cibles des attaques sont en constante évolution, ce qui complique la constitution d'une défense efficace. Ainsi, les collectivités locales, les établissements de santé, et même les petites entreprises sont les cibles privilégiées pour les cybercriminels. Selon l'Anssi, en 2022, 40 % des rançongiciels ciblaient des PME et TPE. Les attaquants étatiques copient les méthodes des cybercriminels à des fins de sabotage informatique, en déstabilisant ces sociétés. Ces évolutions complexifient la caractérisation et l'attribution des responsabilités malveillantes, car les profils des attaquants sont brouillés. En outre, les attaquants se veulent de plus en plus discrets et visent les équipements périphériques comme les pare-feux ou les routeurs. Leur ciblage évolue et ils cherchent désormais à obtenir des accès discrets et pérennes aux réseaux de leurs victimes.

En outre, dans le contexte de guerre en Europe, les actes malveillants tendent à se multiplier, en particulier contre la France et les pays affichant leur soutien à l'Ukraine.

Dès lors, une multiplication des acteurs de la défense cyber risque de complexifier l'élaboration d'une stratégie de défense coordonnée et efficace. Monsieur Strubel, vous avez déclaré que, compte tenu des grands événements sportifs que la France se prépare à accueillir,

nous devons renforcer la vigilance et la responsabilité de chacun. Aussi, comment coordonner efficacement les différents acteurs du SGDSN dans la lutte contre les cybermenaces ?

M. Vincent Strubel. Ma tâche n'est pas de coordonner les acteurs du SGDSN, mais vous évoquez en effet l'enjeu important de la coordination des différents acteurs dans la réponse aux cyberattaques.

Cette coordination existe aujourd'hui dans la réponse aux attaques, grâce au C4. Cette instance assure une coordination étroite entre les acteurs ayant une forte expertise technique – l'Anssi, le commandement de la cyberdéfense, le ministère des armées, et les services de renseignement – qui peuvent mettre en commun leurs connaissances pour mieux caractériser une attaque, et s'efforcer de l'imputer à un acteur identifié. Ces acteurs peuvent se répartir la tâche d'analyse des codes malveillants, par exemple, en cas d'attaque massive ou présentant un caractère d'urgence.

Cette coordination s'étend plus largement aux forces de sécurité intérieure – la police et la gendarmerie. La coordination avec la justice fonctionne également bien, grâce aux dispositions législatives que vous avez votées et qui facilitent la transmission d'informations.

Plus largement, la coopération avec le secteur privé doit faire l'objet de nos efforts. Nous gagnerons certainement à poursuivre la clarification de la qualification des différents prestataires et du cadre doctrinal dans lequel s'inscrit leur action. À ce titre, nous avons engagé un travail sur le cadre doctrinal de la remédiation, qui facilitera les actions communes dans la matière. Nous le publierons dans les jours à venir sous forme d'appel à commentaires.

M. Jean-Michel Jacques, rapporteur. Il est essentiel d'investir dans la cyberdéfense. À ce titre, nous pouvons nous réjouir que le projet de LPM consacre 4 milliards de besoins programmés à ce domaine.

J'aurais souhaité évoquer la lutte informatique d'influence. Nous avons toutes et tous été témoins du rôle qu'ont joué les fausses informations dans l'évolution de la situation au Sahel, dans le cadre de l'opération Barkhane. La multiplication des stratégies hybrides que vous avez évoquées, Monsieur le Secrétaire général, confèrera davantage d'ampleur encore au champ informationnel à l'avenir. Or, pour que la réponse globale de l'État soit efficace, pertinente et crédible dans ce domaine, il est nécessaire de coordonner l'ensemble des entités en charge de la lutte informatique d'influence, comme le ComCyber, la direction du renseignement militaire, la direction générale des services extérieurs de sécurité extérieure, la direction du renseignement et de la sécurité de défense, ou encore l'Agence Viginum rattachée au SGDSN.

Quel rôle joue le SGDSN dans la coordination de la doctrine de lutte informatique d'influence à l'échelle interministérielle ?

M. Stéphane Bouillon. Lorsque nous avons travaillé sur la lutte contre les ingérences numériques étrangères, je vous ai présenté le projet de création d'un service à compétence nationale, Viginum. Après avoir été actif pendant les campagnes électorales ainsi que le referendum en Nouvelle-Calédonie, ce service se concentre désormais sur une série d'acteurs qui pourraient nous nuire. À ces champs d'action s'ajoutent les menaces contre nos entreprises,

en raison des nombreuses attaques informationnelles menées dans le cadre de la guerre en Ukraine.

La coordination de ces acteurs est importante : nous avons fait le choix de distinguer, là encore, l'épée et le bouclier. Dans ce cadre, le ministère des affaires étrangères a pour rôle d'expliquer la position de la France, notamment dans les pays africains où nous sommes très attaqués, en mettant à profit son réseau de diplomates. Ses effectifs ont été renforcés par le Président de la République et la Première ministre à cette fin. S'agissant du bouclier, nous avons décidé de nous appuyer sur un dispositif inspiré du C4. Je dirige un comité opérationnel de lutte contre les manipulations de l'information, qui réunit l'ensemble des ministères et des services de renseignement, ainsi que le Service d'information du gouvernement (SIG) afin de surveiller ces attaques, dans le cadre des textes qui régissent Viginum. L'ensemble de ces services détecte, le plus tôt possible, les attaques, tente de les caractériser, et transmet les informations aux autres pour leur permettre de les analyser et proposer un moyen de réaction.

L'exemple de Gossi est particulièrement éclairant : il nous a fallu démontrer que des troupes avaient remplacé nos soldats à Gossi, et que ces nouveaux venus avaient récupéré et enterré sur place des cadavres pour faire croire à un massacre perpétré antérieurement à leur arrivée. Ces fausses informations avaient été propagées par des *bots* et des trolls, dont les adresses IP ont pu être retracées aussi bien en Russie qu'aux États-Unis. Sans cette analyse, notre parole aurait manqué de crédibilité : nous ne prétendons pas détenir la vérité, mais nous expliquons comment la fausse information a été créée.

Ainsi, les contre-réactions que nous pouvons employer incluent le contre-discours, l'explication, l'utilisation du droit – la loi de 2018 relative à la lutte contre la manipulation de l'*information* ou la loi de 1881 sur la liberté de la presse – ou encore la possibilité de représentation diplomatique : lorsque nous démontrons qu'une information a été manipulée par un État, c'est toute sa politique, sa réputation internationale et sa capacité à convaincre et à agir qui peuvent être remises en cause.

Compte tenu des tensions actuelles, nous avons accéléré le dispositif. Ainsi, le comité opérationnel de lutte contre les manipulations de l'information se réunit à la fois en séance plénière et restreinte pour échanger quasiment jour par jour les informations qui nous parviennent afin de les signaler et d'y réagir le plus tôt possible.

M. Lionel Royer-Perreaut (RE). J'aimerais vous interroger sur l'espionnage industriel. Notre pays peut s'enorgueillir de détenir plusieurs fleurons industriels dans des domaines éminemment stratégiques. Notre expertise en matière d'énergie nucléaire et d'aéronautique est particulièrement reconnue – et donc prisée. En effet, dès les années 2010, le gouvernement de l'époque s'est alarmé des cyberattaques touchant nos entreprises françaises. Fin 2013, Airbus a été ainsi victime de pirates informatiques qui ont dérobé des documents sur l'avion de transport militaire A400M. De même, l'un de vos rapports de 2018 pointait les nombreuses cyberattaques ayant touché le Commissariat à l'énergie atomique (CEA) ainsi que les grands groupes comme Airbus, Safran, Dassault, Thales ou Sanofi. Enfin, la même année était révélée une action de services de renseignements chinois ciblant les cadres des grandes entreprises françaises : approchées sur les réseaux sociaux, plusieurs centaines de cibles seraient alors entrées dans un processus de compromission assez abouti, au détriment de notre sécurité nationale.

Pourriez-vous nous détailler la contribution de cette LPM à la lutte contre l'espionnage industriel ?

M. Stéphane Bouillon. Les articles de la LPM que nous avons mentionnés doivent nous permettre de recenser beaucoup plus rapidement les sources et les auteurs des actions d'espionnage industriel par cyberattaque.

En matière de soutien à l'économie de guerre, la LPM offre aux entreprises les moyens de faire face à des attaques qui ne sont pas d'ordre cyber : leur vulnérabilité tient aussi à des aspects de prédation boursière ou de mise en cause de leurs activités, y compris sous l'angle judiciaire, en tirant parti d'une application extraterritoriale d'un droit national.

Les menaces à l'encontre de la sécurité économique pour nos entreprises sont de natures très variées : outre les cyberattaques, l'espionnage peut simplement être le fait de stagiaires ou de visiteurs présents dans les entreprises. Dans ce domaine, il est très difficile d'agir : d'ailleurs, je suis moins inquiet pour le CEA, Thalès, Safran ou Airbus – qui se montrent vigilants – que pour les TPE ou les PME. En effet, certaines d'entre elles produisent des pièces spécifiques qui sont utilisées par de grandes entreprises pour fabriquer nos matériels militaires ou de dissuasion nucléaire. Or, ces entreprises n'ont pas suffisamment conscience de la nécessité de se protéger et nous peinons à les convaincre de procéder aux investissements nécessaires. La première étape est de les doter de vrais informaticiens, de les inciter à procéder à des sauvegardes et d'inviter le personnel à opter pour des mots de passe réellement sécurisés. Nous réalisons un immense travail sur ce sujet, à la fois à travers France Relance pour aider des entreprises et en liaison avec les collectivités territoriales par le biais des Computer Security Incident Response Teams (Csirt) régionaux.

La LPM est orientée sur les aspects militaires. Nous travaillons sur les crédits Lopmi du ministère de l'intérieur, qui proposent des dispositifs au sein de la gendarmerie ou de la police nationale pour aider, protéger et renforcer les services d'enquête. Notre travail consiste aussi, par le biais du Colise, à éviter le rachat de ces pépites françaises par des entreprises étrangères.

Enfin, nous travaillons avec le ministère de l'enseignement supérieur et de la recherche, avec son haut fonctionnaire de défense, pour convaincre les chercheurs que la science n'est plus universelle : leurs travaux de recherche doivent bénéficier à la France plutôt qu'à une puissance étrangère qui tenterait de s'emparer de leurs travaux.

Nous nous sommes d'ailleurs demandé si les textes en matière de sécurité économique ou de soutien à l'économie de guerre ne devraient pas intégrer des mesures plus coercitives vis-à-vis de certaines entreprises ou certains laboratoires de recherche. Nous ne l'avons pas fait, car nous pensons que nous pouvons les convaincre de mieux se protéger : mais chacun doit rester attentif.

M. Vincent Strubel. Au-delà de ces mesures de prévention, nous savons que ces entreprises sensibles sont des cibles privilégiées pour les attaquants de nature étatique qui cherchent à voler de l'information. Il s'agit des cyberattaques les plus discrètes : elles s'inscrivent dans le temps long, captant parfois des informations durant plusieurs années. Nous devons les détecter et les caractériser, afin de limiter leurs effets. En effet, les services de renseignement ne se limitent généralement pas à une seule cible au sein d'un secteur. Les articles 32 à 35 du projet de LPM permettront d'améliorer nos capacités en la matière.

M. Aurélien Saintoul (LFI-NUPES). Dans quelle mesure la LPM permet-elle d'améliorer notre préparation au risque global de réchauffement climatique et d'épuisement des ressources, qui pèse aussi à un niveau très élevé sur l'économie ?

Quel est l'avis de la Commission nationale de l'informatique et des libertés (Cnil) sur les articles concernant la conservation d'identification personnelle ou le recueil de données ? A-t-elle été saisie ? Quel sera le cadre légal applicable ?

Quels éléments du retour d'expérience du covid et de la guerre en Ukraine, concernant la sécurisation des approvisionnements et la lutte cyber figurent-ils dans le projet de LPM ?

Pouvez-vous préciser le fléchage des ressources humaines en matière cyber ?

Quel est le montant alloué à la défense cyber dans le cadre des Jeux olympiques ?

M. Stéphane Bouillon. S'agissant du réchauffement climatique, le mode d'organisation des équipements prévus par le ministère des armées prend en compte la contrainte écologique. Je me souviens avoir participé l'année dernière à un forum sur les possibilités de limiter les impacts climatiques des activités menées par les armées.

Je ne peux pas vous préciser le fléchage des ressources humaines sur le cyber en ce qui concerne les armées.

La crise du covid était une crise civile. Les armées sont intervenues pour nous soutenir. En matière de service de santé des armées, des leçons ont été tirées sur les aménagements et les recrutements pour faire face à une crise militaire et apporter leur concours à une crise civile.

Je vous invite à interroger le chef d'état-major des armées quant aux leçons qu'il a tirées du retour d'expérience de la guerre en Ukraine. L'utilisation et les effets d'armes rustiques nous ont invités, outre les investissements dans les hautes technologies, à recompléter nos stocks de matériels certes moins coûteux, mais qui présentent toutefois une forme d'efficacité.

M. Vincent Strubel. La loi relative aux Jeux olympiques et paralympiques prévoit une enveloppe de 10,1 millions d'euros pour la cybersécurité : elle nous permettra de mener un travail spécifique d'audit et d'accompagnement des acteurs numériques essentiels liés à l'organisation des Jeux. Après avoir mené un travail d'inventaire des systèmes d'information qui joueront un rôle critique , nous avons lancé l'opération « *Fosbury »*, qui vise à les auditer et à leur proposer des plans d'action pour améliorer leur cybersécurité. Nous en mènerons à bien une partie, et nous en sous-traiterons le reste à des prestataires privés, qualifiés par l'Anssi.

Par ailleurs, la LPM proposée vise à éviter autant que possible l'accès à des données personnelles. L'article 33 spécifie ainsi que les données sont anonymisées. L'Arcep devra vérifier que les collectes organisées respectent ce principe. Les enjeux de données personnelles soulevés par l'article 35 sont encadrés : nous ne devons conserver que les données relatives à l'attaque, sous contrôle de l'Arcep. Une saisine formelle de la Cnil n'a pas été jugée nécessaire à ce stade.

Mme Valérie Bazin-Malgras (LR). La menace cyber se développe de plus en plus dans notre pays, dans les services de l'État, à l'Assemblée nationale, et sur les réseaux des élus de la nation. Les attaquants sont créatifs et n'ont aucune limite : leurs actions sont source de discrédit, et le développement de *fake news* devient monnaie courante.

Monsieur Strubel, comment mettre à profit la LPM pour créer un cadre efficace pour lutter contre ces menaces qui mettent en danger notre démocratie ?

M. Vincent Strubel. Ce travail relève essentiellement de Viginum, bien qu'une concertation s'opère, le cas échéant, face à un continuum entre des cyberattaques et des *fake news*. Ainsi, des cyberattaquants publient parfois des informations volées, en y ajoutant des fausses. Thales avait subi une attaque de ce type : le cyberattaquant avait prétendu avoir mené une attaque d'ampleur, alors que seul un sous-traitant avait été touché et qu'aucune information sensible n'avait été dérobée.

La LPM doit nous apporter une partie de la réponse, en complétant nos capacités opérationnelles de réaction, qui relèvent du champ de la défense et de la préservation des intérêts fondamentaux de la nation. Par ailleurs, il nous faut apporter des solutions de prévention, qui peuvent s'inscrire dans un cadre réglementaire : outre la directive Nis 2, d'autres pans de ce cadre sont en cours de construction, principalement au niveau européen – le marché unique se prêtant à une réglementation aussi homogène que possible. La plupart des acteurs numériques agissant de manière transfrontalière, l'échelle européenne nous paraît cohérente pour éviter tout angle mort.

Nous devons enfin travailler à la bonne compréhension de ces attaques et de leurs conséquences : j'ai eu l'occasion d'aborder cette dimension pédagogique auprès de journalistes qui m'interrogeaient sur la cyberattaque opérée contre l'Assemblée nationale. En effet, le titrage de leurs articles contribuait selon moi à donner de la visibilité à ce qui n'était en réalité qu'un « déni de service », dont la portée s'est révélée limitée et sans conséquences durables. Or, c'est précisément à cette visibilité qu'aspirent les attaquants.

M. Stéphane Bouillon. Le cadre d'action de Viginum est fixé par décret, en accord avec le Conseil d'État et la Cnil : il vise à s'attaquer aux menaces et aux ingérences numériques d'origine étrangère remettant en cause les intérêts fondamentaux de la nation. Pour élargir ce cadre, qui découle des lois existantes, de nouveaux textes seraient nécessaires, sous le contrôle du Conseil constitutionnel. Lorsque le Conseil d'État a rendu son avis en assemblée générale sur la création de Viginum et l'accès à des données personnelles, il a reconnu une stricte proportionnalité et une conformité à la Constitution des travaux que nous menons, parce que nous nous attachions uniquement à ceux qui mettaient en cause la sincérité du scrutin ou les intérêts fondamentaux de la nation, et parce que nous prenions en compte des ingérences numériques étrangères destinées à nuire à ces derniers. Ainsi, s'agissant des attaques dont les élus peuvent faire l'objet, notre champ d'action est limité : nous pouvons appeler les médias à renforcer leur travail de *fact checking*, tandis que la justice a son rôle à jouer. Cependant, nous ne pouvons pas intervenir de notre côté dans ce domaine, et cela me paraît sain. Si une loi devait nous permettre de franchir ce seuil, il faudrait l'examiner très précautionneusement afin que le SGDSN reste dans le strict cadre de ce que la constitution protège en matière de liberté d'opinion et d'expression.

Mme Delphine Lingemann (Dem). La guerre en Ukraine nous montre la manière dont le réseau internet s'intègre directement dans des dynamiques de transfert de souveraineté, pour en prolonger le contrôle territorial. Je ne parle pas uniquement de cyberattaques classiques, visant à détruire des infrastructures, mais aussi de manœuvres cybernétiques plus larges. Ainsi, fin avril 2022, l'organisation NetBlocks, qui suit au jour le jour la liberté d'accès à internet dans le monde entier, a fait état d'une interruption brutale de la connectivité de la ville de Kherson. Elle a été restaurée quelques heures plus tard, mais le chemin emprunté par le réseau internet passait par la société russe Rostelecom, au lieu de l'infrastructure de réseau ukrainien. Les connexions de la zone étaient ainsi soumises à la réglementation, à la surveillance et à la censure de l'internet russe. Or, la Russie dispose d'un vaste système de censure et de surveillance de l'internet qui s'est développé ces dernières années, alors que le pays tente de mettre en œuvre un projet d'internet souverain qui le coupe du reste du monde. Le système d'activité opérationnelle d'investigation du pays peut être utilisé pour surveiller la plupart des flux de communication. Début mai, dans la ville de Kherson reconquise le pouvoir ukrainien a rétabli les connexions.

Cet exemple de guerre des réseaux pose la question du rôle d'internet dans les conflits hybrides. À l'inverse, dans l'internet dématérialisé, l'évolution du réseau et des acteurs politiques concernés indique un tournant vers le rôle fondamental des infrastructures et sur l'importance de leur protection.

Pourriez-vous nous indiquer quels sont les moyens mis en œuvre pour protéger nos infrastructures nationales de réseau, qu'elles soient terrestres ou sous-marines ? Qu'est-il prévu à ce titre dans la prochaine LPM ?

Par ailleurs, nous adoptons désormais une posture défensive, pour laquelle nous cherchons les meilleurs moyens techniques et législatifs de développer ce que la RNS appelle « un bouclier cyber ». Cependant, il me semble que l'Anssi est aussi parfois dans la position de l'attaquant. Aussi, je souhaiterais vous interroger sur cette doctrine d'attaque : la France doit elle se montrer plus offensive ? En avons-nous les moyens techniques ? Quels sont les freins légaux ?

M. le président Thomas Gassilloud. J'en profite pour vous interroger sur le projet de bouclier cyber européen récemment annoncé par Thierry Breton.

M. Vincent Strubel. L'Anssi n'attaque pas. En revanche, nous pouvons procéder à des simulations d'attaques, dans le cadre des audits que nous conduisons pour identifier des vulnérabilités d'un système d'information.

La France s'est dotée de capacités en matière offensive. La dualité entre des capacités défensives et offensives crédibles fonde notre rang de grande nation cyber. Le choix de les séparer clairement, tout en permettant leur coordination sous l'égide du SGDSN, notamment *via* le C4, me paraît éminemment pertinent. Il contribue à la clarté des missions de l'Anssi, que nombre de nos partenaires nous envient. C'est en effet ce qui justifie la confiance profonde que l'on nous témoigne partout dans le monde : ainsi, lorsque TV5 Monde a subi une attaque d'ampleur en 2015, ce média a accepté que l'Anssi prenne la main sur ses systèmes informatiques.

M. Stéphane Bouillon. En effet, Monsieur Saintoul, jusqu'à présent, aucun des médias ni aucune collectivité locale au profit desquels l'Anssi est intervenue ne s'est plaint qu'une seule de ses données ait été indûment utilisée, exploitée ou extraite par l'Anssi.

S'agissant de la protection des infrastructures terrestres, de nombreux câbles ne sont pas protégés. Bien que leurs chambres d'accès soient peu connues, elles peuvent être décelées et détruites, comme un opérateur français l'a expérimenté en région parisienne il y a quelques mois. En revanche, la capacité du réseau internet à pouvoir fonctionner très largement, grâce à la redondance et à la multiplicité des câbles, est un gage d'efficacité.

Il en va de même pour les câbles sous-marins, même si les actions de sabotage existent. Les câbles entre la France et les États-Unis ou la Grande-Bretagne sont nombreux et le flux peut toujours emprunter un autre chemin. Nous demeurons toutefois très sensibles à la vulnérabilité de ces câbles. Dans la LPM, il est prévu des investissements pour les grands fonds marins, qui ont notamment pour objectif d'assurer la protection de nos câbles à grande profondeur, et leur réparation en cas d'attaque.

Nous travaillons en coopération avec nos alliés, qui ont tout autant intérêt que nous à la préservation de ces câbles.

A l'inverse du très fort contrôle de certains États autoritaires sur les réseaux, certains réseaux sociaux ne maîtrisent pas suffisamment leur contenu. La directive européenne DSA vise ainsi à garantir une régulation ; c'était d'ailleurs aussi l'un des objectifs de la loi de 1881 sur la presse, qui avait permis de moraliser l'activité des journaux sans remettre en cause leur liberté. En matière de réseaux sociaux, il faut aussi que les opérateurs abandonnent une partie de leur objectif – faire du profit à tout prix – et acceptent de respecter des règles, au regard de leur rôle particulier dans la formation de l'opinion des populations.

M. Vincent Strubel. Le bouclier cyber européen désigne le travail en cours sur le « *Cyber Solidarity Act* ». Cette démarche reflète la construction d'une solidarité européenne, y compris dans la réponse aux attaques : il ne s'agit pas de contre-attaquer collectivement, mais de s'entraider efficacement face à une attaque. Or, pendant longtemps, cette solidarité constituait une forme de tabou, car elle apparaissait comme contraire aux prérogatives des États membres en matière de sécurité nationale. Elle est désormais perçue comme une nécessité. En effet, nous nous tromperions si nous considérions que les cyberattaques qui se produisent chez nos voisins ne peuvent avoir d'effets dans notre pays ; et il faut, à l'inverse, ne pas faire l'hypothèse que nous n'aurons jamais besoin d'aide.

Les réserves évoquées dans ce cadre existent déjà. Elles seront concrétisées par le biais de prestataires privés, qui seront engagés au profit d'un État partenaire. La coopération existe aussi : je participe ainsi au réseau *Cyber* Crisis Liaison Organisation Network (*CyCLONe*), qui rassemble les directeurs des agences en charge de la gestion de crise cyber des États membres. L'ANSSI est également très active dans le réseau des CSIRT européens (*CSIRT network*).

M. Jean-Marie Fiévet (RE). Le domaine cyber est un champ de conflictualité à part entière. Dans le même temps, l'intelligence artificielle est entrée dans une nouvelle dimension en démontrant des capacités qui se sont largement démocratisées alors qu'elles paraissaient jusqu'à présent à peine imaginables. Je pense par exemple au logiciel ChatGPT, capable de répondre à plus de 1000 milliards de questions en quelques millisecondes.

Ainsi, alors qu'il faut aujourd'hui de nombreux hackeurs armés de puissants ordinateurs pour bloquer des administrations entières ou des entreprises, il semblerait que ces mêmes attaquants pourraient très prochainement bloquer l'entièreté d'un pays avec l'aide de l'intelligence artificielle. Si tel était le cas, l'intelligence artificielle pourrait devenir une arme à part entière, avec un niveau de puissance supérieur à l'arme nucléaire, dans la mesure où elle pourrait entièrement immobiliser un pays qui administration ses armées, ses transports, ses banques – et sans générer aucune perte humaine.

Quelle position devons-nous nous adopter face à ces futures opportunités et éventuelles menaces envers notre sécurité nationale ?

M. Vincent Strubel. L'intelligence artificielle n'est pas un concept nouveau : le terme date en effet de 1956. Il est désormais employé pour désigner les modèles apprenants, entraînés sur des masses de données qui n'étaient autrefois pas disponibles. Leur évolution transforme profondément certains pans du numérique, soulevant des enjeux de sécurisation importants. Cependant, malgré l'apport qu'elle peut offrir à des États membres qui souhaiteraient mener des cyberattaques – en matière d'ingénierie sociale ou de recherche de vulnérabilité, notamment –, l'intelligence artificielle ne modifie pas réellement les capacités d'un attaquant. D'ailleurs, les attaquants n'ont pas attendu l'intelligence artificielle pour paralyser un pays et déployer des capacités de cyberattaque industrielles – comme on l'a vu en Albanie, au Costa Rica ou au Monténégro.

Notons enfin que l'intelligence artificielle peut aussi contribuer à l'amélioration de nos capacités de détection.

Mme Caroline Colombier (RN). En octobre dernier, le Président de la République s'est engagé à ouvrir une quatrième unité d'instruction et d'intervention de la sécurité civile (UIISC). Ces unités, bien que parties intégrantes de l'armée de terre, ont une organisation hybride : tandis que le recrutement et la formation sont assurés par l'armée de terre, les équipements et la logistique de la sécurité civile sont sous la responsabilité du ministère de l'intérieur.

Ce caractère hybride semble ralentir la création de la nouvelle unité. En effet, l'armée de terre et le ministère de l'intérieur ne semblent pas parvenir à s'accorder sur son développement. Ce projet, s'il est justifié et qu'il suscite l'adhésion de l'ensemble des partenaires locaux, soulève de nombreuses préoccupations. Tout d'abord se pose la question des financements qui conditionnent la création même de cette quatrième unité : si une grande partie des crédits relève du ministère de l'intérieur, les unités d'instruction et d'intervention de la sécurité civile font partie de l'armée de terre. À l'aune de cette nouvelle LPM, j'aimerais vous entendre sur les crédits alloués à la création de cette quatrième unité, ainsi que sur la déchéance.

Beaucoup d'interrogations font aussi surface à l'égard du recrutement. Face au manque d'informations et de budget, une crainte prend de l'ampleur : celle de voir cette nouvelle unité être encadrée et composée par les membres des unités déjà existantes, les unités en place étant déjà pleinement mobilisées.

Pouvez-vous, Monsieur le préfet, en votre qualité de Secrétaire général de la défense et de la sécurité nationale, nous informer sur l'état d'avancement de la création de cette unité ? Plus encore, êtes-vous en mesure de nous apporter les garanties de son bon développement afin d'éviter l'affaiblissement des trois unités déjà en place, et la création d'une nouvelle unité en demi-teinte ?

M. Stéphane Bouillon. Ce sujet relève d'un arbitrage entre le ministère des armées et le ministère de l'intérieur. Cependant, en tant que préfet, je peux vous assurer que les UIISC sont des unités très efficaces, dévouées et organisées. Je ne peux que me réjouir de la création d'une quatrième unité.

M. Jean-Louis Thiériot (LR). Dans le cadre de l'économie de guerre et du soutien à notre BITD, comment s'articulent les activités du SGDSN, de la direction générale de l'armement (DGA) et de l'Anssi s'agissant de la cybersécurité ? La LPM prévoit-elle un renforcement de la coordination dans ce secteur ?

M. Stéphane Bouillon. La LPM n'accorde pas crédits à l'Anssi, car le SGDSN est un service de la Première ministre. Nos crédits et nos effectifs sont inscrits en loi de finances, au programme 129 « Coordination de l'action du Gouvernement ». Leur augmentation est régulière : outre les 10 millions d'euros supplémentaires dans le cadre des Jeux olympiques et paralympiques, nous avons reçu 176 millions d'euros du plan d'investissement France Relance pour soutenir des établissements publics hospitaliers et des collectivités territoriales dans leur démarche cybersécurité.

En revanche, au-delà des 4 milliards d'euros prévus par la LPM pour soutenir le cyber, l'Anssi et le SGDSN coopèrent avec la DGA et l'état-major des armées.

L'audition passe à huis clos

Mme Natalia Pouzyreff (RE). L'hôpital André Mignot de Versailles a subi une cyberattaque très importante. Les services ont mis plusieurs mois à s'en remettre. L'attribution de cette attaque est fondamentale : pouvez-vous me confirmer qu'il s'agissait de hackeurs russes ?

Par ailleurs, c'est la gendarmerie qui est intervenue en premier lieu, au titre des compétences cyber dont elle dispose. N'y a-t-il pas une dispersion des compétences entre la gendarmerie et d'autres antennes en matière cyber ?

M. Vincent Strubel. Cette attaque est le fait du rançongiciel *LockBit* qui appartient à un groupe criminel considéré comme russophone. Ce type d'outils peut facilement être récupéré par d'autres acteurs : il est donc difficile d'attribuer précisément l'attaque – et cette tâche relève du rôle de la justice.

La situation de l'hôpital reste délicate, puisqu'il fonctionne encore à 70 % de ses capacités. Cette attaque a en effet causé beaucoup de dégâts, car elle a été identifiée tardivement, et il est très complexe de reconstruire l'ensemble du système numérique d'une telle structure.

La Première ministre et le ministre de la santé prêtent une attention toute particulière au rétablissement de la situation.

L'intervention de la gendarmerie n'est pas redondante de l'action de l'Anssi. Le contact entre l'Anssi et l'hôpital s'est établi dans les premières minutes qui ont suivi le constat de l'attaque, et nous avons assisté l'hôpital la nuit même. Notre rôle a consisté en une action de conseil et de coordination des plans de réponse, essentiellement assurés par des prestataires privés, chargés d'une partie des investigations et de la reconstruction. La gendarmerie intervient plutôt dans un rôle d'enquête, de prise de plainte, et de travail au profit de la justice pour poursuivre les auteurs des faits. La coordination des acteurs se fait dans le cadre élargi du C4.

Enfin, la vulnérabilité des hôpitaux a bien été prise en compte dans les plans du ministère de la santé. Elle fait l'objet d'une partie importante des mesures engagées dans le cadre du plan de relance. Ces actions portent leurs fruits : les attaques qu'ont subies le CHRU de Brest ou d'autres hôpitaux depuis le début de l'année ont été détectées très rapidement grâce à des solutions qui avaient été déployées et en partie financées par le plan de relance. Associée à la préparation des équipes dirigeantes et des directeurs d'hôpitaux et à des plans de réaction, cette détection précoce fait toute la différence. Ainsi, l'attaque contre le CHRU de Brest n'a pas eu d'incidence sur l'offre de soins et ses conséquences ont été traitées en trois semaines.

M. Jean-Louis Thiériot (LR). Je souhaitais à vous témoigner ma gratitude pour le rôle que l'Anssi a joué dans la réponse à l'attaque massive qu'a subie le département de Seine et Marne, dont je suis conseiller départemental et président du groupe majoritaire.

M. le président Thomas Gassilloud. Merci à tous.

*

* *

La séance est levée à dix-huit heures quinze.

*

* *

Membres présents ou excusés

Présents. - M. Xavier Batut, Mme Valérie Bazin-Malgras, M. Pierrick Berteloot, Mme Caroline Colombier, M. Jean-Marie Fiévet, M. Thomas Gassilloud, M. Frank Giletti, M. Christian Girard, M. José Gonzalez, M. Jean-Michel Jacques, M. Loïc Kervran,

Mme Delphine Lingemann, Mme Josy Poueyto, Mme Natalia Pouzyreff, Mme Valérie Rabault, M. Lionel Royer-Perreaut, M. Aurélien Saintoul, M. Michaël Taverne, M. Jean-Louis Thiériot, Mme Sabine Thillaye

Excusés. - M. Christophe Blanchet, Mme Yaël Braun-Pivet, M. Steve Chailloux, Mme Cyrielle Chatelain, M. Yannick Favennec-Bécot, Mme Anne Genetet, M. Olivier Marleix, Mme Lysiane Métayer, M. Pierre Morel-À-L'Huissier, M. Fabien Roussel, Mme Isabelle Santiago, M. Mikaele Seo, Mme Nathalie Serre, M. Olivier Serva