ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Mardi 13 mai 2025
Séance de 16 heures 30

Compte rendu n° 3

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

– Audition, ouverte à la presse, de M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN) 2

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures trente-cinq.

La commission spéciale a auditionné M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN).

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons les travaux de notre commission spéciale, qui ont commencé la semaine dernière avec l'audition de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (Anssi). Nous recevons aujourd'hui M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale (SGDSN), que je remercie de s'être rendu disponible.

Monsieur le secrétaire général, vous avez pris vos fonctions en mars dernier, après une carrière diplomatique qui vous a conduit à exercer des responsabilités éminentes, notamment en tant qu'ambassadeur de France en Iran. Le SGDSN s'inscrit dans une histoire ancienne. Né sous la III^{e} République, sous la forme du Conseil supérieur de la défense nationale, il a toujours eu pour vocation de répondre aux besoins de coordination interministérielle en matière de défense.

Depuis 2009, l'ajout du terme « sécurité » à son intitulé, à la suite du Livre blanc sur la défense et la sécurité nationale de 2008, a marqué un élargissement de ses missions à ce domaine essentiel. Aujourd'hui, le SGDSN couvre un champ stratégique étendu, qui concerne la défense, la sécurité, la programmation militaire, la dissuasion et la lutte contre le terrorisme. Dans son périmètre, on retrouve notamment Viginum, créé par le décret du 13 juillet 2021, chargé de la vigilance contre les ingérences numériques étrangères ; l'opérateur des systèmes d'information interministériels classifiés (OSIIC), initié par le décret du 21 avril 2020, et bien sûr l'Anssi, depuis le décret du 7 juillet 2009.

Le premier ministre est chargé de la mise en place du cadre général du dispositif de sécurité des activités d'importance vitale (SAIV), coordonné par le SGDSN. L'institution que vous dirigez depuis le début du printemps est donc particulièrement concernée par le projet de loi que la commission spéciale est chargée d'examiner. Le titre I^{er} du projet de loi vise en effet à transposer la directive 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, dite REC, et ainsi à actualiser et à modifier le dispositif de sécurité des activités d'importance vitale.

La directive REC, qui a été négociée sous la présidence française de l'Union européenne, s'inspire en grande partie du dispositif français existant. Ainsi, le nombre d'opérateurs d'importance vitale (OIV), qui est environ de 300, ainsi que le nombre de points d'importance vitale, de l'ordre de 1 500 ne devraient pas évoluer de manière significative. Pouvez-vous nous le confirmer ?

Toutefois, cette transposition marque un changement important de philosophie. Elle acte le passage d'une logique de protection des infrastructures d'importance vitale à une approche axée sur la résilience. Pourriez-vous nous éclairer par ailleurs sur les modalités de désignation des OIV et l'architecture de planification ? Ont-elles globalement vocation à être conservées par rapport au dispositif actuel ? Enfin, quelle est notre vision de l'article 16 *bis* qui traite du chiffrement ?

M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale. Je vous remercie pour votre invitation à m'exprimer devant votre commission aujourd'hui pour

évoquer ce projet de loi relatif à la résilience des infrastructures et au renforcement de la cybersécurité. Comme vous l'avez rappelé, j'ai pris mes fonctions il y a un mois en arrivant directement depuis Téhéran et suis heureux d'évoquer avec aujourd'hui ce thème de la résilience, thème central pour les deux grandes missions qu'assure le SGDSN au profit du premier ministre, de l'ensemble du gouvernement et du président de la République : d'une part les travaux de coordination interministérielle dans le domaine de la défense et de la sécurité nationale, qui recouvre l'ensemble des questions de résilience nationale ; et d'autre part un certain nombre d'opérateurs d'agences qui dépendent directement du SGDSN.

Comme vous l'avez souligné, ce projet de loi porte sur la transposition de trois textes européens : la directive européenne sur la résilience des entités critiques, la directive *Network and Information Security 2* (NIS 2) et la directive *Digital Operational Resilience Act* (Dora). Ces trois textes forment un tout et constituent un ensemble d'innovations, mais aussi pour nous une certaine forme de continuité.

Je me félicite de la décision que vous avez prise collectivement de mettre en place une commission spéciale aux fins d'examen de ce projet, comme le Sénat l'avait fait avant vous. D'un point de vue technique, ces textes ne constituent pas un ensemble monolithique, mais un ensemble qui conserve toute sa cohérence. La directive REC reprend et développe, comme vous l'avez dit, monsieur le président, des principes bien connus en France : la politique de sécurité des activités d'importance vitale de la planification de défense et de sécurité nationale et la continuité d'activité en cas de crise.

Je ne m'appesantirai pas sur les titres II et III concernant la transposition de la directive NIS 2 ni sur la *lex specialis* qu'est la transposition de la directive Dora, puisque vous avez entendu le directeur général de l'Anssi sur la partie NIS 2 et que vous recevrez certainement le directeur général du Trésor concernant Dora.

La diversité de l'ensemble de ces textes justifie pleinement leur examen au sein d'une commission spéciale qui regroupe les compétences des commissaires de plusieurs commissions permanentes. Néanmoins, pour le gouvernement, pour l'ensemble des administrations et le SGDSN qui a coordonné une partie de ses travaux, ces textes témoignent d'une cohérence d'ensemble. Celle-ci se définit par l'objectif de la construction d'une meilleure résilience de notre pays face à des menaces, y compris hybrides, des chocs et des crises de toute nature qui ne se tarissent pas.

Parmi l'ensemble de ces travaux, deux doivent être mentionnés en particulier : la revue nationale stratégique (RNS) en cours de finalisation, et la mise en œuvre de la stratégie nationale de résilience (SNR) qui, depuis avril 2022, évolue régulièrement et forme pour nous le cadre de la mise en place de ces directives et de la loi, lorsque vous aurez terminé vos travaux et que la loi sera formellement adoptée.

L'objectif consiste pour nous à faire face à des menaces de plus en plus agressives, des crises majeures qui touchent tous les secteurs d'activités de la vie de la nation, quelles qu'en soient les origines. La méthode se trouve en partie dans ce projet de loi qui fixe des cadres au sein desquels notre stratégie globale de résilience a vocation à se renforcer. Les actions seront mises en œuvre par l'ensemble des entités étatiques et publiques, mais aussi par un ensemble d'opérateurs régulés, en application des trois directives ainsi transposées. Au-delà de ces aspects techniques, ce projet de loi participe donc bien d'une entreprise générale collective de renforcement de la résilience de la nation en cas de crise.

Je termine ces quelques mots d'introduction en remarquant que, si en 2022, au sortir de l'épidémie de covid-19, le concept de résilience ne pouvait déjà plus être regardé comme une abstraction, force est de constater qu'il a pris aujourd'hui une nouvelle acuité et une nouvelle force, compte tenu de l'évolution de l'environnement stratégique. D'une certaine façon, nous avons été rattrapés par des réalités de plus en plus sombres et de plus en plus prégnantes pour l'ensemble des services de l'État. Je suis frappé, depuis je suis rentré de Téhéran et que j'ai pris mes fonctions, par l'affaissement des mécanismes internationaux de règlement des conflits, l'affaiblissement de l'idée de régulation, par les doutes qui peuvent naître sur les solidarités les mieux ancrées dans l'histoire, par l'inquiétude qui saisit les pays qui, comme le nôtre, demeurent attachés à l'idée que la paix vaut mieux que la guerre et que la coopération entre États est préférable au chantage. La prochaine actualisation de la RNS, en cours de pilotage interne par le SGDSN, permettra d'établir une synthèse de l'état du monde, de nos analyses de la menace et des risques, et surtout des voies et moyens que la France doit choisir pour y faire face.

Je souhaite tout d'abord évoquer le contexte dans lequel s'inscrit le projet de loi, c'est-à-dire l'actualisation de la RNS que le président de la République nous a commandée dans ses vœux aux armées, le 17 janvier dernier. Ceux qui parmi vous siègent habituellement au sein de la commission de la défense et des forces armées sont bien informés de ce travail en cours.

Je rappelle la manière dont le président de la République a décrit la situation à l'entame de son adresse à nos compatriotes, le 5 mars : *« Vous êtes en effet légitimement inquiets devant les événements historiques en cours qui bouleversent l'ordre mondial. La guerre en Ukraine, qui a entraîné près d'un million de morts et de blessés, continue avec la même intensité. Les États-Unis d'Amérique, notre allié, ont changé leur position sur cette guerre, soutiennent moins l'Ukraine et laissent planer le doute sur la suite. Dans le même temps, les mêmes États-Unis d'Amérique entendent imposer des tarifs douaniers aux produits venant d'Europe. Enfin, le monde continue d'être sans cesse plus brutal, et la menace terroriste ne faiblit pas. Au total, notre prospérité et notre sécurité sont devenues plus incertaines. Il faut bien le dire, nous entrons dans une nouvelle ère. ».*

Le 3 mars, devant vous, lors d'une déclaration du gouvernement sur la situation en Ukraine et la sécurité de l'Europe, le premier ministre a quant à lui évoqué « *une situation historique qui est à nos yeux la plus grave, la plus déstabilisée et la plus dangereuse de toutes celles que notre pays et notre continent ont connues depuis la fin de la seconde guerre mondiale.* ».

Nous faisons donc face à nous à un environnement international profondément dégradé, profondément menaçant. Cette dégradation est liée à une série de facteurs, à une série d'actions d'États. Nous pensons évidemment en premier lieu à la Russie, mais bien au-delà, à l'ensemble des évolutions de l'environnement stratégique. Plus précisément sur notre territoire, les modes d'action que nous disons hybrides sont employés aujourd'hui par un certain nombre de nos adversaires et sont devenus une forme d'agacement sinon quotidien, du moins courant. Je rappelle de quoi nous parlons : les étoiles de David sur les murs du 14e arrondissement ; les mains rouges sur le mémorial des Justes ; les cercueils en carton sous la tour Eiffel ; les réseaux de faux comptes qui bombardent les plates-formes numériques d'histoires inventées et d'informations déformées, des attaques cyber.

Nos partenaires européens comme les pays baltes, la Pologne, l'Allemagne, le Royaume-Uni, la Roumanie font aussi l'objet de manœuvres d'intimidation, d'agression, de

cyberattaques, d'incendies criminels. Chaque échéance électorale est mise à profit pour mobiliser un écosystème de manipulation de l'information et d'ingérence numérique étrangères qui pèse sur le fonctionnement de nos démocraties.

En raison de l'agressivité russe, qui n'a rien de neuf et qui s'inscrit dans une longue durée, et de l'incertitude qui pèse sur un certain nombre de mécanismes de solidarité, nous sommes aujourd'hui collectivement amenés à réviser nos scénarios centraux, en particulier l'hypothèse d'un engagement majeur de nos forces armées. Depuis plusieurs décennies, nous envisagions des opérations de projection de puissance, de projection de forces, loin du territoire métropolitain. Nous sommes désormais obligés d'envisager la mobilisation de nos forces armées dans un conflit de haute intensité, en dehors du territoire national, mais dans la périphérie de l'Europe.

Cela change beaucoup de choses dans l'approche de certaines questions comme les réserves, les stocks stratégiques, les capacités industrielles, la mobilisation des forces morales de la nation. Face à cette hypothèse d'engagement, nous devons aussi durcir notre capacité à agir et notre capacité à faire face aux chocs que nous sommes amenés à subir. Le projet de loi qui vous est soumis concourt directement à cet objectif, qui est au cœur des travaux de la RNS. Les infrastructures critiques qui sont déjà soumises aux risques naturels comme le dérèglement climatique ou les épidémies sont aujourd'hui régulièrement la cible d'attaques physiques et cybernétiques. Je pense ici à des incendies volontaires de pylônes de télécommunications, des sabotages commis contre le réseau ferré, des cyberattaques contre les hôpitaux. Le retour des conflits de haute intensité sur le continent européen et aux frontières de l'Europe a mis en lumière la vulnérabilité des infrastructures critiques, qui constituent aujourd'hui des cibles prioritaires et stratégiques en cas de conflit. Leur destruction peut engendrer de graves conséquences en France et dans les États voisins, du fait de l'interdépendance structurelle de nos sociétés dans les secteurs critiques.

Cette multiplication des risques et menaces a ainsi conforté une ambition politique et normative sur la protection de ces infrastructures critiques, qui se matérialise dans le titre I^{er} du projet de loi. L'ambition qui vous est soumise consiste à améliorer la fourniture, en Europe, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, en renforçant la résilience des opérateurs d'importance vitale nommés « *entités critiques* » dans la directive.

Pour être complet, je veux vous indiquer que le travail d'actualisation en cours traitera d'une forme de réarmement de la défense civile de notre pays – j'ai évoqué les forces morales. Le concept central de ce réarmement est la résilience ; celle, individuelle et collective, de nos concitoyens, mais aussi celle des organisations. Nos orientations stratégiques vis-à-vis des institutions internationales, de nos alliances, de nos partenaires et de nos compétiteurs, sont aujourd'hui organisées autour de ce concept de résilience.

Le deuxième point sur lequel je souhaite revenir concerne précisément l'État actuel de notre stratégie nationale de résilience. En effet, je ne voudrais pas donner l'impression que la question de la résilience ne serait liée qu'à des phénomènes récents, intervenus ces derniers mois. La politique de sécurité des activités d'importance vitale qui vise à assurer la protection et la « continuité d'activité » de l'ensemble des opérateurs indispensables au fonctionnement de nos institutions, de notre économie, et à notre sécurité, date de 2006. On ne parlait pas de résilience à l'époque, mais il s'agit bien de cela.

Plus près de nous, le SGDSN a été mandaté par le premier ministre Jean Castex en mai 2021 pour préparer une stratégie nationale de résilience. Cette consigne visait à faire fructifier un certain nombre d'enseignements tirés de la pandémie de covid-19. La stratégie nationale de résilience a été validée par Matignon en avril 2022. Depuis lors, elle est à la fois en cours de déclinaison par les ministères, mais aussi d'ajustement permanent à l'évolution de notre environnement stratégique et des besoins qui se font jour.

De façon générale, cette SNR repose sur un ensemble de soixante-treize actions qui concourent à trois objectifs stratégiques : la préparation en profondeur de l'État aux crises, le développement des capacités humaines et matérielles pour y faire face et l'adaptation de la communication publique aux enjeux de la résilience. Sur la base de ces soixante-treize actions, un certain nombre d'objectifs et d'indicateurs sont déclinés depuis 2022. Ce triptyque constitue l'une des matérialisations de la stratégie nationale de résilience. Il s'agissait à l'époque à la fois de promouvoir une polyvalence des outils de gestion de crise, mais aussi d'installer le concept de résilience au cœur de nos travaux de planification. À ce titre, une des tâches du SGDSN consiste à préparer la planification nationale de défense et de sécurité nationale.

Nous avons donc complété le dispositif intérieur des grands plans qui visait à répondre à une menace ou un type de menace – vous connaissez d'ailleurs tous le plus célèbre d'entre eux, le plan Vigipirate – avec des fiches mesures universelles, non pas par type de catastrophes, mais par type de conséquences. Ces plans possèdent de grandes qualités, mais, à l'usage de vingt années de gestion de crises diverses, il est apparu, notamment en 2020, qu'ils comportaient également des inconvénients. Ainsi, ils sont bien construits et très complets, mais aussi lourds à mettre en œuvre et complexes à mettre à jour. Le choix effectué en 2021 dans le cadre de la SNR a donc consisté à envisager la planification et la gestion de crise de façon plus générique, en créant une forme de « tronc commun » à l'ensemble des crises et à y associer un ensemble de mesures de mise en œuvre dont le choix permet de s'adapter à la typologie de la crise, qu'elle soit sanitaire, industrielle, climatique, sécuritaire, de manipulation ou de guerre économique.

Autrement dit, nous avons été guidés par un souci de simplification de l'ensemble de travaux de planification nationale de défense et de sécurité nationale. Cette simplification en cours se poursuit puisque nous sommes aujourd'hui rentrés dans sa deuxième phase. De plus, cette SNR se recentre sur deux grands objectifs qui permettent d'offrir plus de clarté et de pilotage à l'ensemble de la stratégie.

Ce recentrage se concentre premièrement sur un objectif très simple : assurer la continuité de la vie économique de la nation. J'entends par là l'impératif d'assurer la résilience des réseaux essentiels (téléphonie d'urgence, eau, gaz, électricité, énergie, communications, communications classifiées) et de remédier aux vulnérabilités critiques d'approvisionnement qui, trop souvent, placent notre pays dans une situation de vulnérabilité, si ce n'est de dépendance.

La deuxième grande priorité consiste à mobiliser les citoyens au service de la résilience et de la défense globale. Cela signifie très concrètement les former, les sensibiliser, les éduquer dès le plus jeune âge et tout au long de la vie. Cela implique également d'harmoniser et de simplifier les dispositifs existants de réserve. Cela nous engage enfin à encourager et faciliter toutes les bonnes volontés, c'est-à-dire tous nos concitoyens et nos compatriotes qui souhaitent aider et favoriser l'engagement, quel qu'il soit, pour constituer un vivier de volontaires mobilisables en cas de crise.

Cette stratégie nationale de la résilience constitue donc la déclinaison opérationnelle de tous les ministères et, au-delà, de toutes les collectivités publiques, de ce que nous caractérisons, dans le cadre de la RNS, comme l'adaptation nécessaire de nos outils et de nos planifications à une évolution drastique de la menace, et notamment des menaces hybrides qui pèsent sur le territoire national.

J'en viens au troisième et dernier point, qui constitue le cœur de vos travaux et en particulier du titre I^{er} de la loi. Le constat de départ, qui a motivé l'adoption de la directive REC, porte précisément sur la multiplication des risques et des menaces pouvant affecter nos infrastructures critiques, c'est-à-dire celles qui sont nécessaires à l'exercice d'une activité d'importance vitale ou dont une perturbation pourrait mettre gravement en cause la santé de la population ou l'environnement.

La directive REC complète donc la démarche engagée par l'adoption de la directive de décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'étendre leur protection, alors limitée aux secteurs des transports et de l'énergie, aux opérateurs de dimension européenne. L'ambition de REC consiste désormais à améliorer la fourniture, dans le marché intérieur européen, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des opérateurs d'importance vitale, désignés comme « entités critiques » dans la directive.

La directive, qui devait être transposée en droit national le 17 octobre 2024 au plus tard, assure un socle minimal commun de résilience à tous les opérateurs de l'Union européenne (UE). Incidemment, elle permet d'atténuer une forme de *dumping* des obligations sécuritaires entre États membres, le cadre français étant déjà relativement complet au regard des dispositions de la directive.

En France, nous avons fait le choix de la simplicité et de la continuité : la transposition révise le dispositif national de sécurité des activités d'importance vitale défini dans le code de la défense (articles L. 1332-1 et suivants), qui a fait ses preuves. Cette politique publique, qui trouve ses origines dans une ordonnance de 1958, instaurée formellement à compter de 2006, a prouvé son efficacité et fait l'objet d'une déclinaison sur l'ensemble du territoire national. Il y a donc lieu de se féliciter de ce que les contours de la directive REC coïncident presqu'exactement avec ceux de la SAIV nationale.

Cette réforme normative et doctrinale représente aussi pour nous l'occasion de moderniser notre dispositif national : révision de la classification du dispositif (statut d'OIV) et renforcement de la mise en œuvre et de la coordination du dispositif, dans une logique de cohérence, d'efficacité et de simplification.

La transposition s'inscrit donc bien dans une politique de résilience globale et cohérente : les OIV seront également soumis aux obligations de cyber-résilience prévues par la directive NIS 2 (négociée en parallèle de la directive REC et de la directive Dora portant sur la résilience du secteur financier). La cohérence d'ensemble que j'évoquais en introduction n'est donc pas une vue de l'esprit.

L'identité de vue entre la directive et le dispositif national constitue évidemment un avantage à plusieurs égards. Le vocabulaire national est conservé, de même que la logique d'identification des sites les plus sensibles – les points d'importance vitale – ainsi que la planification associée.

Le suivi effectué par le SGDSN, les ministères coordonnateurs, les zones de défense et de sécurité et les préfets de département est maintenu et pourra être renforcé. J'y veillerai personnellement. D'ores et déjà, j'ai décidé de poursuivre l'œuvre de sensibilisation des préfets territoriaux à l'ensemble des aspects de la stratégie nationale de résilience. Je suis notamment intervenu lors de la dernière réunion des préfets au ministère de l'intérieur et me déplacerai dans les zones de défense pour poursuivre cette sensibilisation visant à contribuer à l'appropriation par l'ensemble des acteurs territoriaux de ce concept de résilience.

Autre avantage important pour les opérateurs d'importance vitale, nombre des exigences de la directive sont déjà mises en œuvre à travers le dispositif actuel. Ainsi, les entités concernées par la révision du dispositif SAIV sont les opérateurs qui étaient déjà assujettis au dispositif existant.

De nouveaux opérateurs d'importance vitale pourraient le cas échéant être désignés au titre de leurs activités, considérées comme d'importance vitale par l'État si celles-ci devaient évoluer ou émerger, en particulier dans les secteurs de l'assainissement, de l'hydrogène, ainsi que les réseaux de chaleur et de froid, nouvellement identifiés par la directive REC. Toutefois, le nombre d'opérateurs d'importance vitale, autour de 300 aujourd'hui, n'a pas vocation à augmenter significativement.

Concrètement, la mise en œuvre de la directive devrait se traduire par un certain nombre d'améliorations. Il s'agit d'abord d'une meilleure prise en compte des interdépendances entre les secteurs, et entre les États membres, avec l'identification par les opérateurs de leurs interdépendances et de leurs chaînes d'approvisionnement dans une logique de continuité d'activités. Il s'agit ensuite d'une obligation de notification des incidents majeurs, qui existe déjà dans le domaine de la cybersécurité, mais aussi d'une évolution et d'un renforcement du dispositif d'enquêtes administratives de sécurité. Enfin, l'amélioration porte sur une révision du dispositif de sanctions pour les opérateurs qui ne respecteraient pas leurs obligations, avec la création d'un régime de sanctions administratives, en lieu et place des sanctions pénales existantes. Ces quatre mesures nous permettront de mettre en œuvre notre stratégie nationale de résilience de façon beaucoup plus efficace que par le passé.

Pour sa part, la création d'un nouveau statut d'« *entité critique d'importance européenne particulière* » (ECIEP) pour les opérateurs fournissant un service essentiel à au moins six États membres de l'UE, porte des enjeux particuliers, soit une obligation de notification à la Commission et de partage d'information avec les États membres concernés. Néanmoins, il convient de souligner que cette directive a été négociée – le SGDSN a été particulièrement vigilant sur ce point – dans l'objectif de respecter les prérogatives nationales et les enjeux de souveraineté, de sécurité et de protection du secret afférents à la protection des infrastructures critiques, de sorte que seules les données agrégées seront transmises à la Commission européenne.

Dans une optique de modernisation et de cohérence de l'ensemble du dispositif, le choix a été opéré de donner la possibilité à l'autorité administrative d'autoriser les opérateurs à déroger, dans certains cas précis, au droit commun de la commande publique, lorsqu'il pourrait être porté atteinte aux intérêts essentiels de l'État.

Je souhaite enfin évoquer le coût des mesures imposées. Trois points me semblent devoir être précisés. En premier lieu, ces mesures pourront engendrer un coût pour un certain nombre d'opérateurs. Ensuite, nous ne sommes pas en mesure aujourd'hui d'évaluer

exactement le coût afférent à l'évolution de ce dispositif, en raison à la fois de la variété des secteurs et des opérateurs couverts par notre stratégie de résilience. Troisièmement, le coût des mesures de continuité d'activité n'est évidemment en rien comparable au coût d'un arrêt d'activité. Nos opérateurs économiques le savent déjà parfaitement : ils n'ont pas attendu l'État, pour la plupart d'entre eux, pour investir dans la sécurisation de leurs activités. Nous allons donc apprendre en marchant, mais je crois que la question du coût doit être abordée avec sérénité.

J'en termine par les collectivités territoriales, qui dans la directive REC – contrairement à NIS 2 qui s'appliquera directement à un certain nombre de collectivités locales –, ne constituent pas un secteur spécifique. Certaines collectivités sont incluses dans le champ de la directive REC ; il s'agit de celles qui sont déjà désignées OIV, car elles assurent des activités d'importance vitale ou services essentiels au sens de la directive REC – dans les secteurs qui relèvent de leur compétence ; par exemple pour les secteurs de la gestion de l'eau, des transports et de l'énergie.

Dans le cas d'une délégation de service public (DSP) pour des activités d'importance vitale, le projet de loi « Résilience » prévoit l'information de la collectivité territoriale afin que celle-ci soit en mesure de prendre en compte les implications du dispositif sur son délégataire. Ainsi, le délégataire est tenu de mettre en place des mesures pour assurer la résilience de son activité, notamment la sécurisation des sites sans lesquels il ne peut exercer son activité d'importance vitale.

Pour être totalement complet, de nouvelles collectivités territoriales pourraient être désignées à l'avenir au titre de leurs compétences dans les secteurs de l'assainissement, de l'hydrogène, ainsi que des réseaux de chaleur et de froid, car il s'agit de secteurs nouveaux visés par la directive REC et par le projet de loi de transposition.

Tels sont les éléments que je voulais vous transmettre concernant nos travaux dans le cadre de notre analyse des menaces et des risques qui pèsent, de notre travail sur la RNS ; mais aussi de nos actions depuis 2022 en termes de mise en œuvre et de modernisation de la SNR. Les dispositions spécifiques du titre I^{er} du projet de loi viennent parfaitement s'intégrer selon nous dans ce besoin de durcissement et de modernisation d'activités qui sont essentielles à la continuité de la vie de la nation.

M. le président Philippe Latombe. Je cède la parole aux rapporteurs pour une première série de questions.

M. Éric Bothorel, rapporteur général. Monsieur le secrétaire général, puisque vous étiez, il y a encore quelques semaines, notre ambassadeur auprès de la république islamique d'Iran, je ne peux résister à l'envie de vous poser une question qui n'a rien à voir avec le projet de loi, mais qui est également très liée à la thématique de la résilience. J'ai bien conscience que nos auditions sont publiques, que vos réponses sont par nature mesurées, mais je souhaite à titre personnel vous interroger sur la situation des otages Cécile Kohler et Jacques Paris en Iran. Quelle est votre lecture de ce qui semble être une politique qui touche près d'une vingtaine d'Européens et que l'on peut qualifier de politique « d'otages d'État » ?

Je reviens maintenant sur le sujet qui nous réunit aujourd'hui, le projet de loi. D'abord, quelles sont selon vous les nouvelles menaces qui pèsent sur les infrastructures ? Quelles sont les infrastructures qui vous semblent aujourd'hui les plus sensibles ? Je pense

notamment aux gazoducs, aux menaces sous-marines, bactériologiques et celles portant sur les réseaux d'eau.

Nous passons de la notion d'opérateurs de services d'importance vitale, qui étaient parfois uniques et très centralisés, à un élargissement du nombre d'acteurs concernés, avec des entités territoriales nombreuses, des acteurs publics comme privés. Selon vous, l'organisation du SGDSN, par nature très centralisée auprès du premier ministre, devra-t-elle s'adapter à cet élargissement territorial ? Les territoires ultramarins devraient-ils connaître, selon vous, une organisation et une réglementation différenciées ?

Je m'associe également à la question du chiffrement, évoquée par le président Latombe. Ce sujet, qui nous préoccupe tous, est aujourd'hui intégré dans le texte. Vous semble-t-il nécessaire que nous consolidions et que nous sécurisions le chiffrement de bout en bout dans une forme de sacralisation d'une rédaction qui pourrait être plus parfaite ?

Un débat parallèle voit aussi le jour concernant le renseignement d'origine sources ouvertes ou *open source intelligence* (Osint). Selon vous, est-il nécessaire de légiférer sur l'Osint et de profiter de l'opportunité de ce texte pour le faire ? Enfin, nous savons de longue date que les services télécoms ne sont pas au rang des services essentiels dans notre pays. En tant que Breton, je constate que lorsqu'une tempête survient, les priorités portent surtout – de manière légitime – sur le rétablissement de l'eau potable, les hôpitaux, les personnes sous assistance respiratoire, mais les télécoms sont souvent relégués au second plan. Ne faudrait-il pas, dans ce texte, rehausser les infrastructures télécoms au rang des services essentiels, afin que leur remise en route constitue également une priorité ?

Mme Catherine Hervieu, rapporteure. Depuis plusieurs années, les activités françaises représentent une cible pour des États et acteurs étrangers. Nous avons pu évoquer différents points de vigilance, notamment lors de la consultation des parlementaires pour la révision de la RNS 2022. Collectivement, nous demandons la rédaction d'un Livre blanc sur la sécurité et la défense pour une réelle stratégie nationale.

Pour autant, une partie des parlementaires reste encore à convaincre et une majorité des Français à informer. L'information est la clé de voûte pour éclairer, mais également influencer. Notre calendrier est restreint, et soyons réalistes, nous sommes en retard. J'ai d'ailleurs exprimé l'urgence de traiter ce projet de loi en priorité lors des questions au gouvernement, le 30 avril dernier. Dans le rapport de la direction générale de la sécurité intérieure (DGSI) et de la direction générale de la sécurité extérieure (DGSE) qui a fuité, il est indiqué que « *La Russie mène des actions offensives qui peuvent avoir des conséquences directes sur la vie des Français : tentatives d'incendie de centres commerciaux, attaques sur des câbles sous-marins, de télécommunications, cyberattaques sur des terminaux satellitaires (…) visant à faire dysfonctionner des infrastructures critiques, fragiliser l'organisation de la société ou espionner des entités françaises* ». Nos objectifs actuels consistent donc à réduire nos vulnérabilités et à être résilients.

Pourtant, nous sommes tous témoins d'ores et déjà d'ingérences sur nos territoires dans les administrations, les hôpitaux, les communications, les entreprises. Au-delà de la sensibilisation, l'information de l'ensemble des Français, des élus et des opérateurs est nécessaire. Les acteurs de nos territoires disposent néanmoins de moyens différents pour faire face aux menaces dont ils sont les cibles.

Vous avez évoqué les collectivités territoriales et la façon d'organiser les DSP, mais il faudra également tenir compte des différences qui existent entre les territoires. Comment répondre à ces impératifs de protection avec les moyens humains et financiers dont nous disposons actuellement ? Ce projet de loi demande un renforcement et une augmentation des moyens pour sa mise en œuvre.

Il nous faudra développer et cibler les besoins prioritaires à développer, et nous devrons hiérarchiser les différentes étapes du calendrier, compte tenu des situations que vous avez décrites. Concernant le titre Ier, dont je suis rapporteure, pourriez-vous développer l'application du dispositif aux opérateurs régaliens, exclus de la direction en droit européen et intégrés au dispositif français de sécurité des activités d'importance vitale ?

Madame Anne Le Hénanff, rapporteure. Monsieur le secrétaire général, que pensez-vous du critère du nombre d'habitants retenu pour qu'une collectivité soit considérée comme une entité essentielle, et en particulier du seuil arrêté par le Sénat, c'est-à-dire 30 000 habitants ? Que pensez-vous de la classification des collectivités comprenant moins de 30 000 habitants dans la catégorie des entités importantes ?

Par ailleurs, un certain nombre d'administrations sont exclues du périmètre d'application du projet de loi, notamment celles exerçant dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, les missions diplomatiques et consulaires françaises, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), les ministères, le Sénat et l'Assemblée nationale. Dans quelles mesures ces exemptions se justifient-elles ? Quelles garanties pouvez-vous nous apporter quant à leur degré de cybersécurité et de cyber-résilience ?

Ensuite, vous avez parlé de l'implication des préfets. Je fais partie de ces députés qui, depuis des années, demandent que les préfets s'impliquent davantage dans l'accompagnement à la montée en cybersécurité des territoires. Je suis donc particulièrement intéressée par les propos que vous avez tenus à ce propos. Vous avez parlé particulièrement des zones de défense, mais qu'en est-il des autres territoires qui n'en sont pas ? De quels moyens vont-ils disposer ? Quelles seront les marges de manœuvre des collectivités locales, des hôpitaux ?

Enfin, le budget du SGDSN a diminué en 2025. L'Anssi, l'OSIIC et Viginum ont ainsi vu leurs moyens diminuer de 8 millions d'euros. Alors que nous allons entamer l'étude de la loi « Résilience » et la transposition de la directive NIS 2, comment pourrons-nous agir, compte tenu de cette réduction de budget ?

M. Mickaël Bouloux, rapporteur. Je suis, pour ma part, rapporteur thématique en ce qui concerne le titre III du projet de loi, qui porte sur la résilience opérationnelle numérique du secteur financier et qui transpose la directive Dora.

Je souhaite vous poser des questions plutôt générales sur le rôle du SGDSN dans la résilience des entités financières. Tout d'abord, quels sont vos relations et vos leviers d'action avec le secteur bancaire ? J'ai lu qu'il existait un réseau de référents désignés en coordination avec la Fédération bancaire française, afin de favoriser le financement privé de la base industrielle et technologique de défense (BITD), mais aussi de développer une culture de défense chez ces acteurs privés.

Ces référents pourraient-ils jouer un jour un rôle dans la résilience opérationnelle numérique du secteur financier ? Les acteurs bancaires constituent-ils des cibles de choix pour

les tentatives d'ingérence étrangère, dans le but de déstabiliser notre économie ? Enfin, quels types de menaces cyber certains États sont-ils susceptibles de mettre en œuvre contre nos entités financières ?

M. Nicolas Roche. Monsieur le rapporteur général, nos autorités politiques, le président de la République, le premier ministre et le ministre de l'Europe et des affaires étrangères ont été parfaitement clairs depuis des mois – si ce n'est des années – sur le statut d'otages d'État de Cécile Kohler et Jacques Paris. Je suis personnellement allé assister les familles des otages, dont celles de ceux de nos otages qui ont pu rentrer en France ; lesquels sont heureusement nombreux. Nous avons célébré tristement la semaine dernière les trois années de détention arbitraire de ces deux otages aux mains de la république islamique d'Iran. Ils constituaient la priorité de mon action pendant trois ans à l'ambassade de France en Iran. Je reste mobilisé, comme tous les services de l'État et comme le président de la République l'a encore rappelé, pour faire en sorte qu'enfin, nos compatriotes puissent rentrer en France.

Ensuite, s'agissant de la question du chiffrement, nous avons besoin de temps et de sérénité pour mener un travail technique très approfondi, interne aux services de l'État, pour traiter au fond ce sujet, de façon professionnelle, méthodique, propre, détaillée. Nous reviendrons ensuite vers le gouvernement et le président de la République pour signaler si des solutions techniques sont possibles, leurs avantages et inconvénients, afin qu'une décision puisse être prise en toute connaissance de cause. Cette question est évidemment incontournable, puisqu'elle concerne plusieurs politiques publiques essentielles, fondamentales.

S'agissant des éléments plus directement liés au titre I^er^, c'est-à-dire la nature et l'identification des menaces prioritaires, nous n'avons malheureusement pas le luxe du choix. Nous ne définissons pas ces menaces et les risques, qui nous sont souvent imposés par nos adversaires. L'évolution de l'environnement stratégique de ces dernières années montre que, factuellement, les menaces qui ont eu à un moment ou à un autre, en France ou dans des pays amis, un impact direct sur la continuité de la vie de la nation, ont touché tous les secteurs possibles.

Dans le domaine cyber, elles concernent à la fois l'espionnage et les manipulations de l'information, qui sont de plus en plus complexes, de plus en plus élaborées technologiquement, et qui visent de plus en plus le cœur du fonctionnement de nos sociétés. Elles visent aussi le sabotage physique d'un certain nombre d'activités, y compris d'importance vitale. Un certain nombre de secteurs d'activités ont ainsi été touchés en France et en Europe ces dernières années. Elles portent également sur la guerre économique et commerciale, le *lawfare*, c'est-à-dire l'instrumentalisation du droit à des fins de disruption des relations internationales.

Aujourd'hui, nous n'avons pas le luxe de choisir ou prioriser les menaces qui pèsent sur la continuité de la vie de la nation et nous devons toutes les prendre en compte. La RNS réalisera une description précise de l'ensemble de ces menaces sur cette partie du scénario, qui concerne le volet des menaces hybrides, qui pèsent sur le territoire national. Le ciblage très précis qui a été opéré jusqu'à présent sur les secteurs prioritaires pour la continuité de la vie de la nation – et qui ne devrait pas être bouleversé – indique ce que la nation doit protéger, *minimum minimorum*.

Ensuite, je crois que l'existence même du SGDSN, son double rôle d'animation interministérielle et d'opérateur dans un certain nombre de secteurs, de façon centralisée auprès du premier ministre, constitue une immense chance pour notre système administratif et politique. Nous ne sommes pas pour autant inattentifs à la décentralisation, aux collectivités territoriales, aux acteurs privés, aux associations, à nos compatriotes. Cependant, l'environnement stratégique auquel nous sommes soumis impose une forme de centralisation de l'analyse de la menace, de la planification de défense et de l'animation du collectif de la sécurité nationale et de la résilience.

Le SGDSN ne fait pas tout lui-même, très loin de là. Il joue un rôle essentiel dans ce domaine-là d'animation des travaux interministériels et d'animation de l'ensemble des acteurs publics, mais aussi privés. Par ailleurs, dans des domaines très spécifiques qui nous ont été confiés, il endosse un rôle d'opérateur opérationnel dans des secteurs essentiels pour la résilience de la nation, à travers l'Anssi, Viginum et l'OSIIC. En résumé, j'estime que cette organisation et ce pilotage central du SGDSN constituent une des valeurs ajoutées de notre dispositif. Certains pays européens souffrent *a contrario* d'un manque de coordination interministérielle dans la mise en œuvre d'une véritable stratégie de résilience.

Ensuite, il ne me semble pas nécessaire de développer un cadre juridique dédié à l'outre-mer. En revanche, il existe le besoin d'une prise en compte particulière des opérateurs et des situations spécifiques de nos territoires ultramarins, qui sont soumis à des natures et des types de menaces hybrides singulières, dans la mise en œuvre de l'ensemble de nos plans de résilience.

Je me permets de réserver ma réponse sur l'Osint. Je fais partie de ceux qui pensent depuis longtemps que cette question est centrale et que nous avons besoin de capacités d'*open source*. Je reviendrai vers vous plus spécifiquement sur cette question.

Il serait erroné de considérer que les réseaux de télécommunication sont par essence secondaires. En tant que secrétaire général de la défense et de la sécurité nationale, je préside un comité interministériel chargé en partie de la supervision des communications d'urgence. Il existe bien un impératif de rétablissement très rapide des communications d'urgence au minimum pour assurer la continuité de la vie de la nation. Par ailleurs, un certain nombre d'éléments centraux des grands opérateurs de réseaux téléphoniques font partie des systèmes intégrés à notre stratégie nationale de résilience ; nous leur imposons un certain nombre d'obligations.

S'agissant de l'information sur les menaces et de la sensibilisation, je partage entièrement votre évaluation, madame Hervieu. L'un des objectifs de la RNS consiste précisément à contribuer à cette prise de conscience collective et à cet effort pédagogique d'éducation et de sensibilisation de tous nos compatriotes concernant l'ensemble des menaces, notamment hybrides, des risques ou des hypothèses d'engagement majeur de nos forces armées dans une guerre potentielle.

À ce titre, après trois ans passés à l'étranger, je retrouve des compatriotes et des concitoyens dont la prise de conscience est plus mûre que lorsque j'ai quitté la France en 2022, s'agissant de la menace cyber, de la menace de manipulation de l'information, de la menace de guerre commerciale, de sabotage et d'espionnage. Cependant, je vous rejoins entièrement sur le fait que nous ne sommes pas encore aujourd'hui là où nous devrions être et que l'effort de sensibilisation et de renforcement doit être poursuivi. Il s'agit d'ailleurs d'un des objectifs de la RNS, raison pour laquelle j'ai demandé et obtenu de mes autorités

politiques un délai supplémentaire pour permettre la poursuite des consultations, en particulier avec les commissions de la défense de l'Assemblée nationale et du Sénat, dans l'élaboration de cette RNS. La publication et la diffusion de la RNS seront marquées par un effort très vaste d'éducation et de sensibilisation à partir de la synthèse de l'évaluation de la menace et des risques qui pèsent sur le territoire, à l'horizon des années 2030-2040.

Ensuite, toutes les infrastructures sont sensibles en réalité ; je ne peux pas vous répondre différemment : à partir du moment où un opérateur d'importance vitale a été qualifié comme tel, nous ne pouvons pas établir de hiérarchie entre eux. La logique profonde de notre cadre politique, juridique et stratégique consiste précisément à adopter une cohérence d'ensemble de notre stratégie de résilience qui suppose que tous les OIV, toutes les activités d'importance vitale qui ont été identifiés soient protégés, non plus dans une logique de protection de points ponctuels, mais dans une logique de continuité d'activité et de résilience.

À partir du moment où des opérateurs, des activités ou des points entrent dans le champ de la directive REC, du dispositif de la loi « Résilience » et de nos plans de défense, il revient aux opérateurs de se mettre en conformité avec ces obligations qui, encore une fois, sont essentielles pour la continuité de la vie de la nation.

Madame la rapporteure, au-delà des collectivités territoriales et de l'ensemble des acteurs, de nos compatriotes, de nos concitoyens et du tissu associatif, il existe un impératif de mobilisation, qui rejoint d'ailleurs la question de la sensibilisation. Au niveau central, dans les administrations de l'État, en particulier celles qui relèvent directement de la défense et de la sécurité nationale, le niveau de prise de conscience et de connaissance est élevé. J'ai déjà eu l'occasion de vous indiquer qu'il l'est également chez nos compatriotes. Entre les deux, cette prise de conscience est inégale chez un certain nombre d'acteurs pourtant essentiels à la résilience de la nation.

La mobilisation que vous mentionnez est donc bien nécessaire. Elle interviendra en particulier à travers la publication et la mise en œuvre de la RNS. C'est la raison pour laquelle je suis intervenu devant l'ensemble des préfets, pour les sensibiliser sur le scénario central de la RNS, les impératifs de la stratégie nationale de résilience et de mise en œuvre, et la nécessaire mobilisation de l'ensemble des acteurs de l'État et, au premier chef, des préfets et de l'ensemble des acteurs déconcentrés de l'État. Ils jouent un rôle essentiel en tant qu'animateurs de l'ensemble des écosystèmes territoriaux qui contribuent à la défense et à la sécurité nationale, y compris les collectivités territoriales. Il est impératif de multiplier les instances et les enceintes dans lesquelles il nous faut mener cette discussion.

Traditionnellement, tous les Livres blancs et les RNS comportent une dimension nationale d'explication et une déclinaison internationale, afin d'expliquer à nos partenaires étrangers ce que nous réalisons et de construire des coopérations internationales. Le travail est spécifique cette année : nous devrons ajouter à ces deux dimensions une innovation très importante, qui concernera une partie territoriale de la déclinaison de la RNS, à travers la mobilisation des acteurs locaux. Sauf erreur de ma part, la question du seuil démographique pour les entités et des exemptions dans certains secteurs relève très directement de la partie consacrée au cyber et à NIS 2, et non du titre I^{er} sur la résilience.

Concernant les efforts budgétaires, je ne peux que concourir à votre évaluation : la mise en œuvre de la SNR et de la stratégie nationale de cybersécurité nécessitera un certain nombre de décisions. Il reviendra évidemment au gouvernement d'assurer le bouclage de l'ensemble de nos priorités. Interviendra alors, comme dans tout processus budgétaire

classique, une mise en adéquation entre les mesures que nous avons identifiées et les contraintes financières, dans un cadre budgétaire qui me dépasse très largement. Ma responsabilité consiste à porter auprès de mes autorités politiques des choix clairs, et en particulier des priorités en matière de résilience et de sécurité nationale, impliquant des choix budgétaires en termes de ressources humaines. Les choix relèvent ensuite des autorités politiques et du Parlement, en toute connaissance de cause.

Monsieur Bouloux, je suis moins familier de la dimension bancaire. Sur ce sujet, Bertrand Dumont, le directeur général du Trésor constituera un interlocuteur précieux. Je peux néanmoins confirmer l'existence de relations spécifiques entre le SGDSN et les grands acteurs bancaires et assuranciels pour garantir, dans la durée, le financement et l'existence de la BITD. Je ne rentrerai pas davantage dans les détails à l'occasion de cette session publique ; il en sera de même concernant les ingérences étrangères.

Cependant, il est évident que les menaces, en particulier cyber, concernent la totalité des secteurs. Dès lors, il n'y a aucune raison, *a priori*, de considérer que le secteur bancaire n'est pas lui aussi une cible potentielle, compte tenu de son degré de sensibilité aux questions technologiques et digitales.

M. le président Philippe Latombe. Je cède la parole aux orateurs de groupe.

M. Aurélien Saintoul (LFI-NFP). Je souhaite évoquer en premier lieu le rôle des agents assermentés par l'État qui auront pour fonction de mener des contrôles. Disposez-vous d'une forme de cahier des charges à ce titre ? Quel sera le cadre financier ? Qui sera le donneur d'ordre ?

Ma deuxième question concerne la saisine d'une commission des sanctions en cas de manquement ou d'infraction aux obligations contenues dans la directive REC. Quel sera son statut ? Pourquoi devra-t-elle être rattachée directement au premier ministre ? Constitue-t-elle une juridiction de première instance ? Si ces sanctions sont d'ordre administratif, quelle sera la voie de recours ?

Enfin, la commission des sanctions ne peut sanctionner que les personnes privées. Pourtant, la directive n'établit pas de différence entre les OIV, qu'elles soient privées ou publiques. J'aimerais donc connaître la logique qui prévaut pour cette distinction.

M. Sébastien Saint-Pasteur (SOC). Sous la présidence Pompidou, un document pionnier, rédigé à la demande du secrétariat à la défense américain, identifiait déjà les vulnérabilités des systèmes d'information, notamment les risques d'accès non autorisé, de divulgation accidentelle ou d'infiltration délibérée.

Plus de cinquante ans plus tard, l'ombre portée par les menaces cyber a grandi de manière exponentielle. Fort de ce constat que nous partageons tous, je souhaite m'attarder sur plusieurs points. Je pense d'abord à la définition et au respect du périmètre des entités concernées, qui diffère des nomenclatures de l'Anssi auxquelles nous sommes habitués. Ensuite, comment les contrôles pourront-ils être réalisés quand on pense que dans la plus vaste région de France, la région Nouvelle Aquitaine, il existe seulement deux délégués régionaux de l'Anssi pour douze départements ?

Je m'interroge également sur les entités qui ne sont pas concernées. Une commune de moins de 3 000 habitants appartient probablement une intercommunalité à laquelle elle est

reliée par des systèmes informatiques intégrés ou un établissement médico-social, qui traitera des données de santé sensibles. Le flou demeure donc pour les principaux intéressés. Qui plus est, le groupement d'intérêt public « Action contre la cybermalveillance » est aujourd'hui largement sous-doté pour faire face à ces défis. Un récent rapport sénatorial a pointé que les cyberattaques représentaient près de 90 milliards d'euros d'impact pour l'économie française.

Dès lors, comment garantir une transposition lisible pour l'ensemble des acteurs, même les plus petits ? Comment comptez-vous conseiller le gouvernement afin que les moyens d'accompagnement soient bien au rendez-vous, au plus près du terrain ?

Mme Laetitia Saint-Paul (HOR). Au sein du groupe Horizons, nous sommes sensibles à votre volonté d'associer les parlementaires à la RNS. Cependant, sur certains sujets, je suis restée sur ma faim. À titre d'exemple, dans la RNS 2022, l'intelligence artificielle (IA) n'est mentionnée que deux fois.

Je me permets de vous faire part de deux sujets que je souhaiterais voir figurer dans la prochaine RNS. Tout d'abord, la question du *lawfare* ou de la guerre juridique s'applique parfaitement à la confrontation dans les espaces communs, notamment cyber. Ensuite, la configuration du secrétariat général de l'armement nous permet-elle d'être agile sur les enjeux de haute technologie, de start-up, à l'instar du modèle américain de la *Defense Advanced Research Projects Agency* (Darpa) ? De manière générale, notre modèle de travail interministériel est-il suffisamment agile pour faire face à l'hybridité de la conflictualité dans les espaces communs ? Enfin, s'agissant de la loi qui nous concerne, quelles en sont principales lacunes ?

M. Nicolas Roche. Monsieur Saintoul, les agents assermentés seront les mêmes qu'aujourd'hui. Le dispositif d'assermentation ne changera donc pas de manière radicale.

Ensuite, la commission des sanctions ne relève pas d'une autorité juridictionnelle en tant que telle. En revanche, comme toute mesure de police administrative, ces décisions seront susceptibles de faire l'objet de recours en excès de pouvoir devant la juridiction administrative et jusqu'au Conseil d'État.

La distinction entre acteurs privés et publics concerne la non-application des sanctions administratives aux collectivités territoriales. Cet élément tient au fait qu'*in fine*, le délégataire porte l'obligation qui lui est faite de contribuer à la sécurité nationale et à la résilience de la nation.

Les travaux préparatoires au projet de loi n'ont pas convaincu ses auteurs qu'il serait pertinent d'infliger des sanctions à des collectivités territoriales pour des manquements de leurs délégataires de service public, dans les cas d'activités d'OIV et en particulier parce que des sanctions pécuniaires sont ensuite définies en fonction d'un chiffre d'affaires. Le choix a donc été établi à ce stade de ne pas intégrer les collectivités et les acteurs publics des collectivités territoriales dans le champ des mesures qui auparavant relevaient de mesures pénales. À ce titre, le passage d'un régime de sanctions pénales à celui de sanctions administratives m'apparaît constituer une bonne méthode.

Monsieur Saint-Pasteur, il n'existe pas de critère de population pour des opérateurs ou des activités d'importance vitale des collectivités territoriales et des activités d'importance publique dans le titre I^er^.

Le directeur général de l'Anssi vous a exposé la semaine dernière le passage d'une logique de pilotage très précis par l'Anssi des OIV dans le domaine cyber à l'ensemble de la mise en œuvre de la directive NIS 2. Il vaut mieux prévenir que guérir ; en conséquence, l'accompagnement de l'ensemble des collectivités dans la mise en œuvre de la partie cyber de NIS 2 constitue un élément essentiel.

Madame Saint-Paul, j'ai pris bonne note des sujets que vous jugez prioritaires. Je peux vous rassurer en partie : nous conduirons ces travaux avec les parlementaires de la commission de la défense lors des semaines à venir. Les sujets que vous avez évoqués ont été pris en compte dans la RNS, même si j'ignore s'ils le seront à la mesure de ce que vous souhaitez. Ces travaux seront ensuite poursuivis par des consultations avec la représentation nationale, puis des validations par les autorités politiques, qui devraient intervenir d'ici la fin du mois.

M. le président Philippe Latombe. Comment pouvons-nous intégrer ce texte dans le cadre d'une construction d'une autonomie stratégique de cybersécurité, une forme de « BITC », sur le modèle de la BITD ?

M. Nicolas Roche. Ces sujets sont très bien identifiés dans la stratégie nationale cyber et par notre impératif de souveraineté numérique. Dans le cadre des travaux de la RNS, nous avons identifié un certain nombre d'enjeux et de défis pour la BITD. La structuration de la BITD française, son pilotage, son suivi, la relation entre les services de l'État et les acteurs privés me semblent d'une bonne qualité.

L'enjeu consiste aujourd'hui à reproduire ce dispositif pour la base industrielle et technologique de sécurité nationale (BITS), dont les questions cyber et numériques sont parties intégrantes. À ce titre, l'État doit mener un effort de structuration de sa réflexion sur cette BITS, notamment pour identifier des priorités, les sujets technologiques et les acteurs privés essentiels à notre souveraineté. Cette action a commencé dans le cadre de la RNS, mais devra faire l'objet de travaux complémentaires.

M. le président Philippe Latombe. Je vous remercie.

La séance est levée à dix-huit heures dix.

Membres présents ou excusés

Présents. - M. Édouard Bénard, M. Éric Bothorel, M. Mickaël Bouloux, Mme Virginie Duby-Muller, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, Mme Élisabeth de Maistre, Mme Laetitia Saint-Paul, M. Aurélien Saintoul, M. Sébastien Saint-Pasteur, Mme Sabrina Sebaihi, M. Vincent Thiébaut, Mme Sabine Thillaye.

Excusés. - M. Philippe Gosselin, M. Bastien Lachaud, M. Laurent Mazaury.