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

– Audition, ouverte à la presse, de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et de M. Gaëtan Poncelin de Raucourt, sous-directeur « Stratégie » 2

Mercredi 7 mai 2025
Séance de 16 heures 30

Compte rendu n° 2

SESSION ORDINAIRE DE **2024 - 2025**

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures trente.

La commission spéciale a auditionné M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et M. Gaëtan Poncelin de Raucourt, sous-directeur « Stratégie ».

M. le président Philippe Latombe. Nous ouvrons aujourd'hui la première réunion plénière de notre commission spéciale par une audition particulièrement structurante.

Nous avons l'honneur d'accueillir M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Avant d'entrer dans le cœur de nos échanges, je souhaite vous informer d'une évolution importante concernant le calendrier d'examen du projet de loi dont notre commission est saisie. L'examen du texte, initialement prévu en séance publique à la mi-juin, a été reporté. À ce jour, aucune date officielle n'a été communiquée. Il est néanmoins possible que l'examen en séance se tienne lors d'une session extraordinaire en juillet ou en septembre. Par conséquent, l'examen du texte en commission spéciale pourrait avoir lieu dès la semaine du 17 ou du 24 juin, si la séance publique se tenait en juillet ou au début de la session extraordinaire de septembre. Dans l'hypothèse d'un examen en séance à partir de la semaine du 15 septembre, nos travaux pourraient se dérouler début septembre, avec un délai de dépôt des amendements à prévoir pour le dernier week-end d'août. Je m'engage à vous tenir informés le plus rapidement possible.

Monsieur le directeur général, l'Anssi, que vous dirigez depuis janvier 2023, après avoir exercé diverses fonctions pendant près de quinze ans et deux ans à la direction de l'opérateur des systèmes d'information interministériels classifiés (Osiic), est aujourd'hui un pilier incontournable de la sécurité des systèmes d'information en France. Service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Anssi veille à la sécurité des systèmes d'information de l'État, accompagne les opérateurs d'importance vitale et participe à la recherche et à la promotion des technologies de sécurité. Votre rôle va s'intensifier dans le cadre du projet de loi que nous examinons, notamment avec l'article 5, qui vous désigne comme le « chef d'orchestre » de la politique gouvernementale en matière de sécurité des systèmes d'information.

Dans son panorama de la cybermenace 2024, publié en mars dernier, l'Anssi dressait un constat préoccupant : 4 386 événements de sécurité traités en 2023, soit une hausse de 15 % par rapport à l'année précédente. Deux types de menaces dominent : la cybercriminalité systémique et les attaques émanant d'acteurs réputés liés à des États, notamment la Russie et la Chine.

Mes collègues et moi-même avons de nombreuses questions à vous poser afin de mieux cerner les enjeux de la transposition de la directive dite NIS 2, ses implications opérationnelles et ses perspectives stratégiques pour la France et l'Europe.

Premièrement, la transposition belge a fait le choix de s'appuyer sur des normes internationales, apportant visibilité et stabilité aux organisations. Ce n'est pas l'option retenue par le projet de loi français, alors que de nombreux acteurs publics et privés y sont favorables, notamment dans une optique d'harmonisation européenne. Pourriez-vous nous éclairer sur ce

choix et nous indiquer comment nous pourrions construire une convergence européenne sur le sujet ?

Deuxièmement, le sénateur Olivier Cadic évoquait récemment le risque qu'une sous-transposition législative génère une surtransposition administrative. Pensez-vous que le texte issu du Sénat nécessite des modifications, car il serait trop contraignant ou restrictif ? Comment éviter une inflation de référentiels techniques administratifs, parfois contradictoires, source de confusion pour les acteurs concernés ? Je pense notamment aux retours formulés lors du Forum international de la cybersécurité à propos des sondes issues de la dernière loi de programmation militaire (LPM).

Troisièmement, le règlement général sur la protection des données (RGPD) a prévu la création d'un délégué à la protection des données (DPO), fonction assortie de protections spécifiques. De nombreux auteurs universitaires ont proposé la création d'une fonction de type responsable de la sécurité des systèmes d'information (RSSI), munie de protections adéquates par analogie au DPO. Cette idée est également reprise par des organisations matures en protection cyber, entreprises NIS ou collectivités de grande taille. Pensez-vous que le législateur doit s'emparer de cette proposition et, si oui, doit-il l'imposer ou seulement la suggérer pour une partie des entités soumises à NIS 2 ?

Quatrièmement, comment pouvons-nous, selon vous, profiter de ce texte de transposition pour permettre la création d'une base industrielle et technologique de cybersécurité française et européenne (BITC), par analogie à la base industrielle et technologique de défense (BITD), qui participerait à l'autonomie stratégique française et européenne ?

Cinquièmement, quelle interprétation faites-vous de l'avis du Conseil d'État sur la disparité de traitement entre les entités privées soumises à sanctions et les entités publiques dispensées ? Comment envisager de dispenser des entités publiques, par exemple France Travail, de sanctions en cas de manquement avéré en matière de cybersécurité ? Plus largement, quelle exemplarité doivent avoir l'État et les entités publiques en la matière ?

Enfin, sixièmement, que pensez-vous de la rédaction de l'article 16 *bis* sur le chiffrement ?

Monsieur le directeur général, je vous cède la parole.

M. Vincent Strubel, directeur général de l'Anssi. Concernant la genèse du texte, je me concentrerai sur le titre II, qui transpose la directive NIS 2, les titres I^{er} et III transposant la directive sur la résilience des entités critiques (REC) et le Digital Operational Resilience Act (Dora), qui relèvent moins de l'Anssi.

La directive NIS 2 nous a été imposée par l'évolution de la menace. Nous traitons depuis des années une menace étatique d'espionnage et potentiellement de sabotage, mais s'y ajoute, depuis le tournant des années 2020, ce que nous appelons la « menace systémique ». Cette dernière est principalement portée par des acteurs du crime organisé et de l'activisme. Elle se caractérise par son caractère non ciblé, contrairement à la menace étatique, et finit par toucher l'ensemble des acteurs. Les entités les plus vulnérables en termes de cybersécurité, auparavant épargnées, sont désormais concernées : petites et moyennes entreprises (PME), entreprises de taille intermédiaire (ETI), collectivités ou encore associations. Cette tendance,

observée depuis 2020, ne fait que se confirmer année après année. Les chiffres de notre panorama de la menace corroborent ce constat.

Face à cette situation, partagée à l'échelle européenne, nous avons collectivement élaboré la directive NIS 2, avec une forte impulsion française. Cette directive complète un paysage normatif européen préexistant, notamment la directive NIS 1, mais s'inscrit dans une logique différente. NIS 2 représente un changement d'échelle dans le nombre d'entités régulées. En France, nous passerons de quelques centaines à environ 15 000 entités régulées, avec des proportions similaires dans les autres pays européens. Ce texte marque également un changement de paradigme dans le niveau d'exigence. Nous n'appliquerons pas le même niveau d'exigence à une entreprise de taille moyenne qu'à un opérateur d'importance vitale. De plus, la logique de désignation par seuil remplace la désignation individuelle et nous introduisons des sanctions administratives et financières.

Ce texte répond à une nécessité essentielle pour la résilience de notre économie et de notre société face à une menace qui n'épargne plus personne. Cette menace, actuellement opportuniste, pourrait un jour s'avérer coordonnée avec des menaces étatiques dans un contexte géopolitique plus large.

Au-delà de cette nécessité, je suis convaincu que ce texte représente une véritable opportunité. Il permet de sensibiliser à grande échelle l'ensemble des petites structures jusqu'ici éloignées des enjeux de cybersécurité, mais qui ne peuvent plus les ignorer. Il offre également la possibilité de définir simplement et clairement les bonnes pratiques de cybersécurité pour ces entités, tout en délimitant leurs responsabilités. Enfin, il constitue une occasion de mobiliser l'écosystème de cybersécurité national et européen, florissant et riche, qui sera naturellement positionné en proximité pour répondre aux besoins de ces petites structures.

Nous nous sommes efforcés de transposer la genèse de la directive dans le projet qui nous est soumis, en suivant plusieurs grands principes.

Nous appliquons tout d'abord le principe de coconstruction, sans précédent pour l'Anssi. Nous avons consulté près de 80 organisations professionnelles et toutes les associations d'élus. Ces consultations, initiées en septembre 2023, se poursuivent dans la préparation des textes d'application et continueront lors de la mise en œuvre.

Ensuite, un autre principe est l'harmonisation, qui se traduit par l'absence de surtransposition. Nous avons effectué une transposition sèche, sans surtransposition ni sous-transposition. Cette recherche d'harmonisation se poursuit dans nos échanges au sein du groupe de coopération NIS 2, avec la Commission et les autres États membres. Nous cherchons à clarifier certains points de mise en œuvre, notamment l'application aux filiales, sujet qui fait l'objet de nombreux débats partagés par l'ensemble des États membres. Nous avons sollicité un avis consensuel de la Commission pour guider notre interprétation et éviter de créer de la complexité inutile.

Par ailleurs, nous appliquons le principe de proportionnalité, prévu par la directive, qui distingue deux types d'entités : les entités essentielles, plus matures en termes de cybersécurité et plus critiques, et les entités importantes, de taille et de maturité moindres. Nous n'aurons pas le même niveau d'exigence sur ces deux types d'entités. Cette proportionnalité se décline dans le régime de sanctions, différencié selon le type d'entité, et dans le régime de contrôle, *ex ante* pour les entités essentielles et *ex post* pour les entités

importantes. Ce principe s'applique également aux niveaux d'exigence technique que nous porterons.

Cette approche nous différencie de celle adoptée par nos homologues belges. Notre diagnostic actuel suggère que leur approche est potentiellement moins exigeante pour les entités essentielles, mais probablement plus contraignante pour les entités importantes. L'utilisation de la norme ISO 27001 par les Belges impose à ces entités un travail d'analyse et d'expertise significatif que nous ne comptons pas exiger des entités importantes, car elles ne disposent pas nécessairement de cette expertise.

En outre, nous appliquons un principe de simplification et de rationalisation, qui nous conduit à aligner les différents cadres normatifs préexistants, tels que celui des opérateurs d'importance vitale et celui applicable aux administrations via le référentiel général de sécurité, sur un socle commun de mesures. Nous le compléterons d'exigences supplémentaires pour des entités spécifiques, notamment les opérateurs d'importance vitale. Concernant les sondes de détection, après dix ans de mise en œuvre du dispositif applicable aux opérateurs d'importance vitale, nous réexaminerons les dispositions et leur efficacité à l'aune de l'état de l'art du moment.

Le texte a été examiné au Sénat en mars. Je salue le travail des sénateurs, qui a amélioré et clarifié le texte, contribuant à l'effort de pédagogie sur ces enjeux pour sensibiliser les entités qui seront concernées par ce texte. Je ne doute pas que l'Assemblée nationale apportera une contribution similaire, tant sur le texte que sur l'accompagnement et la pédagogie nécessaires.

Parmi les évolutions saillantes apportées par le Sénat, je soulignerai l'inclusion dans la loi de certains éléments en termes de définition, de champ d'application et de délais, qui apportent de la visibilité. Cependant, le bon équilibre a été maintenu en préservant la possibilité pour le pouvoir réglementaire d'apporter certaines précisions, notamment sur la définition des secteurs soumis à la directive NIS 2. Cette flexibilité nous permettra de continuer à adapter le déploiement de ce cadre, notamment en lien avec les travaux que nous poursuivons avec nos homologues européens pour clarifier certaines définitions ou interprétations.

Le Sénat a également introduit la possibilité de créer un label national permettant aux entités d'attester leur conformité à NIS 2. Ce label pourra être valorisé auprès d'autres acteurs, tels que les assureurs, les banques ou les clients pour témoigner d'un niveau de sécurité satisfaisant. Nous pouvons nous réjouir de cette évolution et du bon équilibre trouvé, ce label étant une possibilité, et non une contrainte pour les entités assujetties à NIS 2. Nous aurons peut-être à apporter quelques améliorations, à des fins de sécurité juridique, à cette disposition, mais l'équilibre atteint par le Sénat semble approprié.

J'accueille favorablement la possibilité apportée par le Sénat de créer une reconnaissance de labels délivrés par d'autres États membres. Cette initiative répond notamment à la question de l'articulation avec le dispositif belge, et potentiellement avec d'autres dispositifs équivalents qui pourraient être mis en place par d'autres États membres. L'équilibre trouvé me semble judicieux : il s'agit d'une possibilité, et non d'une automaticité, préservant ainsi une marge d'appréciation quant au niveau d'exigence porté par d'autres labels équivalents. Nous aurons également quelques éléments à proposer en termes de sécurisation juridique de ce dispositif.

Certains points soulèvent des interrogations.

Le Sénat a simplifié l'articulation entre Dora et la directive NIS 2, ce qui est louable dans l'intention. Toutefois, supprimer la notification des incidents cyber qui affecteraient les entités soumises à Dora auprès de l'Anssi, pour ne conserver qu'une notification aux entités de contrôle Dora — à savoir l'autorité de contrôle prudentiel et de résolution (ACPR) et l'autorité des marchés financiers (AMF) —, provoque des effets de bord néfastes. Contrairement à l'Anssi, l'ACPR et l'AMF ne disposent pas d'un service opérationnel 24 heures sur 24 et 7 jours sur 7. Ce passage obligé par les autorités de Dora entraînerait un retard dans la prise en compte des notifications d'incidents par l'Anssi, l'empêchant ainsi de remplir efficacement sa mission d'assistance aux victimes et d'alerte des autres cibles potentielles. Nous proposerons donc de rétablir une forme de double notification, basée sur un formulaire unique pour éviter la duplication du travail, afin de garantir l'efficacité dans le traitement des incidents.

De même, nous nous interrogeons sur les restrictions apportées à la commission des sanctions, indépendante de l'Anssi, mais chargée d'examiner et de prononcer d'éventuelles sanctions à la suite de manquements. Certaines contraintes apportées à sa composition et à ses modalités d'instruction soulèvent potentiellement des risques pratiques quant à sa capacité à disposer de l'expertise nécessaire et à la solidité juridique de ses décisions. Nous sommes à votre disposition pour travailler sur ces enjeux, ainsi que sur des clarifications concernant la responsabilité des organes de direction des entités assujetties.

Parallèlement au processus législatif, nous avons initié des travaux préparatoires pour répondre à deux besoins majeurs exprimés lors de nos consultations : une mise en œuvre progressive et un accompagnement adapté.

Concernant la mise en œuvre progressive, je réaffirme notre souhait de prendre le temps nécessaire à une mise en œuvre adéquate de ces dispositions en distinguant les obligations simples, telles que l'enregistrement auprès de l'Anssi et la notification d'incidents – qui bénéficieront d'un délai de six mois –, des obligations plus complexes pour lesquelles nous accorderons un délai de trois ans après la publication des textes d'application, avec une approche progressive incluant des contrôles à blanc sans sanction durant cette période.

Concernant l'accompagnement, nous travaillerons sur trois axes.

Premièrement, nous développons une offre de services adaptée et clarifiée de la part de l'Anssi, comprenant des dispositifs tels que « Mon Aide Cyber » pour un premier diagnostic, « Mes Services Cyber » pour une meilleure lisibilité du corpus documentaire et « Mon Espace NIS 2 » pour le préenregistrement et le test de la soumission au cadre NIS 2.

Deuxièmement, nous mettons en place un réseau de relais impliquant les services de l'État, les collectivités, les organisations professionnelles et l'écosystème des fournisseurs de produits et services français et européens. La logique de cet accompagnement vise à n'exclure personne et à partager un cadre commun ainsi qu'une offre lisible.

Troisièmement, nous mobilisons tous les dispositifs de soutien et d'accompagnement, publics et privés, y compris à travers la perspective d'un label facilitant la démonstration de conformité et l'appréciation des risques par les secteurs bancaire et assurantiel.

Enfin, un enjeu transverse est celui de la communication. Il est impératif de sensibiliser toutes les futures entités assujetties, qui sont souvent éloignées des préoccupations de cybersécurité et qui ont besoin de s'en préoccuper avant de subir des attaques. Je ne doute pas que vos travaux contribueront à cette sensibilisation. L'Anssi se tient à votre disposition pour vous y aider.

M. le président Philippe Latombe. Je cède la parole aux rapporteurs.

M. Éric Bothorel, rapporteur général. Je me permets de suggérer que nous puissions auditionner une nouvelle fois M. le directeur général à l'issue de nos travaux. En effet, il me semble aussi pertinent de l'auditionner aujourd'hui, en introduction de nos travaux, qu'après avoir entendu un certain nombre d'acteurs qui ne manqueront pas de nous faire part de leurs observations et recommandations.

Concernant le calendrier que vous avez évoqué, monsieur le président, je souhaiterais que nous puissions mener nos travaux de manière continue. C'est un avis personnel, mais s'il était partagé par d'autres, peut-être pourrait-il être pris en considération.

Dans mon mandat de rapporteur général, je serai attentif à rechercher les équilibres concernant un texte qui se veut harmonieux, de par sa nature européenne. Lorsqu'on est attaché à une forme de souveraineté, qui ne doit pas être confondue avec du souverainisme, il est en effet impératif de disposer d'un cadre européen harmonieux plutôt que fragmenté. En tant que rapporteur général, je veillerai à ce que ces équilibres soient respectés.

Monsieur le directeur général, nous entendons parfois qu'il est inutile de s'embarrasser avec ces actions, puisque la norme ISO 27001 est excellente et permet de se passer de nuances technologiques et de spécificités techniques rappelées dans ces trois textes.

Par ailleurs, au-delà de l'articulation de Dora et de NIS 2, comment parvenez-vous à trouver un équilibre avec les autres organisations, notamment la Commission nationale de l'informatique et des libertés (Cnil) ?

Comment pouvons-nous faire en sorte que NIS 2 devienne un sujet de levier et de démultiplication de notre écosystème cyber ?

Enfin, concernant le chiffrement, pourriez-vous apporter une réponse plus précise à la question du président ?

Mme Anne Le Hénanff, rapporteure. Les sénateurs ont directement inscrit dans la loi la liste des secteurs, en distinguant ceux considérés comme hautement critiques de ceux critiques. Un décret en Conseil d'État précisera les sous-secteurs et les types d'entités relevant de ces deux catégories. Quelle est votre opinion sur cette approche des sénateurs ?

Concernant le budget nécessaire pour se mettre en conformité, comment envisagez-vous l'accompagnement des territoires des entités concernées et la mise en œuvre de la directive par ces mêmes entités ? Avez-vous déjà évoqué la question des moyens financiers ou cela reste-t-il à définir dans le cadre d'un projet de loi de finances (PLF) ?

La sénatrice Vanina Paoli-Gagin a évoqué les critères de sélection des contrôleurs, en insistant sur la nécessité qu'ils soient français pour éviter les risques d'ingérence. Pouvez-vous nous en dire davantage à ce sujet ? Pourquoi avez-vous exprimé un avis défavorable au Sénat sur ce point ?

Enfin, pourriez-vous nous éclairer sur le niveau de protection des mesures mises en place dans la transposition de NIS 2, comparativement aux exigences actuelles en vigueur appliquées aux opérateurs d'importance vitale, notamment dans le cadre de la LPM 2013 ?

M. Mickaël Bouloux, rapporteur. En tant que rapporteur thématique sur le titre III du projet de loi, qui est relatif à la résilience opérationnelle numérique du secteur financier et qui ne concerne pas autant l'Anssi que la transposition de la directive NIS 2, je souhaite vous poser quelques questions sur le rôle de votre agence dans la résilience des entités financières.

Tout d'abord, pourriez-vous nous donner des exemples récents de cybermenaces auxquelles sont exposés les acteurs du système financier ? La recapitalisation de la filiale américaine de la banque chinoise ICBC est souvent citée comme exemple. J'ai lu, dans votre dernier panorama, que le logiciel financier Xtrader avait aussi été compromis.

Ensuite, compte tenu des menaces, pensez-vous que le règlement et la directive Dora seront décisifs pour assurer la résilience du secteur financier ?

Enfin, le Sénat a ajouté deux articles additionnels au titre III du projet de loi afin de désigner une seule autorité compétente pour recevoir, de la part des entités financières, les déclarations obligatoires d'incidents majeurs et les notifications volontaires de cybermenaces importantes pour respecter l'article 19 du règlement Dora. Si cet ajout est motivé par le souhait d'éviter le double assujettissement entre NIS 2 et Dora, vous militez pour que l'Anssi puisse également être prévenue. En tant que rapporteur thématique, je suis enclin à soutenir ce point.

Mme Catherine Hervieu, rapporteure. Je suis rapporteure pour le titre I^{er}, relatif à la résilience des activités d'importance vitale pour l'ensemble des thématiques que nous aborderons à travers ce sujet.

La cybersécurité de l'État doit être renforcée pour protéger nos données et nos secteurs critiques. L'objectif stratégique n° 4 de la revue nationale stratégique (RNS) 2022, visant une résilience cyber de premier rang, est plus que jamais d'actualité. Il est impératif de rehausser le niveau de cybersécurité de l'ensemble des entités importantes, face à des besoins qui s'accélèrent quotidiennement. La mise en place d'une stratégie nationale en matière de cybersécurité est donc primordiale, notamment pour une question de défense nationale.

La directive NIS 2 représente une avancée significative pour assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne. Elle participe à une transformation de l'Anssi, modifiant vos méthodes de travail et vos échanges avec vos interlocuteurs. Votre rôle est central pour informer et accompagner des acteurs de notre territoire en matière de cybersécurité des entités importantes.

Quelles sont les conséquences du texte sur les collectivités territoriales, dont les moyens sont très hétéroclites, tant sur le plan humain que financier ? Comment envisagez-vous de déployer l'accompagnement en tenant compte des contextes territoriaux ?

La coopération stratégique et l'échange d'informations entre les États membres, ainsi que le réseau des *Cyber Incident Response Teams* (CIRT) qui favorise une coopération opérationnelle rapide et efficace entre les entités nationales, sont des moyens d'améliorer la cybersécurité à tous les échelons. Pourriez-vous développer vos besoins en matière de coopération avec les États membres de l'Union européenne ?

Enfin, face aux évolutions technologiques exponentielles, notamment l'intelligence artificielle, comment appréhendez-vous notre prise en compte de ces enjeux, en particulier pour les technologies de rupture ?

M. Vincent Strubel, directeur général de l'Anssi. Concernant les exigences ISO 27001, nous n'y sommes pas opposés. La plupart de nos référentiels de prestataires qualifiés déclinent la même architecture que cette norme. Cependant, elle ne constitue pas l'outil adéquat pour répondre aux exigences de NIS 2. Nos homologues belges partagent cette analyse : ils se sont certes inspirés de la norme ISO 27001, mais l'ont complétée par des exigences supplémentaires. Par exemple, ISO 27001 ne traite pas la question des sauvegardes, pourtant cruciale pour les petites entreprises face aux rançongiciels. Nous intégrerons ce type d'exigences, à l'instar des Belges. Nous ne nous contentons donc pas d'une simple déclinaison d'une norme sur étagère.

Une autre réserve concernant l'ISO 27001 tient à sa nature : il s'agit d'une méthode pour élaborer des objectifs de sécurité et se mettre en conformité. Cette norme n'indique pas précisément les actions à entreprendre pour répondre à un niveau de menace précis. Ce travail d'adaptation incombe à l'entité appliquant la norme. Nous estimons donc que cette démarche sera trop complexe pour de petites structures, notamment parmi les entités importantes qui ne disposeront pas toutes d'un RSSI.

Bien que le métier de RSSI soit indispensable, je ne suis pas convaincu de la nécessité de l'encadrer par la loi. De nombreux RSSI exercent aujourd'hui sans ancrage légal et ils ne semblent pas en avoir besoin. En revanche, nous n'envisageons pas d'exiger la présence d'un RSSI ou d'un expert en cybersécurité dans chaque entité importante, ce qui serait déraisonnable au vu de la taille de certaines d'entre elles. Nous procéderons plutôt à une analyse des risques au profit des secteurs d'activité et proposerons des mesures relativement simples à mettre en œuvre.

Concernant le positionnement entre NIS 2 et le cadre applicable aux opérateurs d'importance vitale, nos exigences seront nettement moins strictes pour NIS 2 que pour les opérateurs d'importance vitale. Néanmoins, cela constituera le socle commun. Pour les opérateurs d'importance vitale, dans le cadre de la refonte du dispositif d'activité d'importance vitale portée par le titre I^{er}, nous ajouterons des mesures complémentaires reprenant certaines exigences spécifiques actuellement en vigueur. Ces exigences sont pertinentes compte tenu de leur niveau d'exposition à la menace, y compris stratégique. Les opérateurs d'importance vitale sont concernés non seulement par la menace systémique, mais aussi par des menaces ciblées. Nous maintiendrons donc des exigences en matière de détection, qui figure dans le cadre existant, mais que nous actualiserons au gré de l'évolution de l'état de l'art, tandis que nous appliquerons un niveau d'exigence moindre pour les entités soumises à NIS 2, en raison de leur exposition différente à la menace et de leurs moyens plus limités.

Quant à l'intelligence artificielle, notre analyse, largement partagée lors du sommet pour l'action sur l'intelligence artificielle, ne la considère pas comme une rupture fondamentale en matière de cybersécurité. Elle améliorera certes les capacités des attaquants, mais aussi celles des défenseurs. Il s'agit, pour nous, de nous emparer de ces nouvelles technologies au même rythme que les « méchants » et d'accompagner le déploiement de l'intelligence artificielle par des mesures de cybersécurité appropriées. Toutefois, le rapport d'analyse des risques que nous avons publié, cosigné par deux de nos partenaires étrangers, souligne que le déploiement de l'intelligence artificielle nécessite avant tout le respect des

bonnes pratiques de base applicables à tout logiciel, avant de se préoccuper d'autres risques spécifiques. Le socle de base de bonnes pratiques que nous porterons avec NIS 2 devrait largement résister à l'épreuve du temps et permettre une prise en compte adéquate de ces enjeux, tout en restant ouvert à d'éventuelles révisions.

La nécessité d'une bonne articulation entre les niveaux législatif et réglementaire découle du besoin d'ajuster les mesures en fonction de l'évolution technologique.

Concernant la liste des secteurs inclus dans la loi par le Sénat, elle reprend littéralement ceux prévus par la directive. Initialement, nous avions jugé cette reprise superflue, mais nous respectons la décision du Sénat, qui estime que cela contribue à la lisibilité du texte. Nous ne sommes pas opposés à cette décision tant que nous conservons la possibilité de préciser les sous-secteurs au niveau réglementaire, notamment pour permettre l'articulation avec les définitions retenues dans les périmètres ministériels, susceptibles d'évoluer. Le point d'équilibre trouvé par le Sénat nous semble satisfaisant à ce stade.

Concernant l'articulation avec les entités des cadres Dora et RGPD, parmi lesquels la Cnil, nous suivons le principe de *lex specialis* prévu par les directives. Les entités soumises à Dora et à NIS 2 appliquent les règles de Dora, et non les règles équivalentes de NIS 2. Elles appliquent en outre les règles de NIS 2 lorsqu'il n'en existe pas d'équivalentes dans Dora. Concrètement, elles appliqueront toutes les règles Dora, plus deux règles supplémentaires présentes dans NIS 2 : l'enregistrement auprès de l'Anssi et la notification des incidents de cybersécurité à cette même autorité.

Le Sénat a simplifié la deuxième exigence en prévoyant le principe de simple notification. Si l'intention est louable, l'effet me semble potentiellement problématique. Nous pensons qu'un formulaire commun envoyé aux deux entités de contrôle serait préférable. Nous avons évidemment entamé des discussions avec les autorités de contrôle Dora, à savoir l'ACPR et l'AMF, pour partager notre compréhension des exigences et coordonner nos contrôles. Un principe similaire s'appliquera *a priori* pour l'articulation avec le cadre RGPD, en concertation avec la Cnil.

Le projet de loi établit un principe de *non bis in idem*. Lorsqu'une sanction est envisagée au titre de NIS 2 et du RGPD, le régime de sanctions pécuniaires appliqué sera celui du RGPD, considéré comme plus disant en termes de pourcentage du chiffre d'affaires global.

Nous menons actuellement une concertation avec la Cnil concernant les modalités de contrôle, le partage des retours d'expérience, l'interprétation des exigences et le traitement des incidents. Le projet de loi prévoit un équilibre judicieux : nous avons la possibilité de notifier à la Cnil des manquements évidents à la protection des données personnelles, mais ce n'est pas le principe par défaut. Nous privilégions plutôt l'approche qui est déjà la nôtre dans le traitement des incidents. Quand nous assistons une victime de cyberattaques, nous l'invitons à se préoccuper des enjeux de données personnelles, lui expliquons le cadre applicable et la mettons en relation, le cas échéant, avec la Cnil et lui donnons accès à tous les formulaires applicables, mais nous ne réalisons pas, à sa place, le travail d'estimation des impacts sur les données personnelles. Cet équilibre se dessine et semble faire consensus avec la Cnil.

Concernant les critères de sélection des contrôleurs, le gouvernement a défendu au Sénat la proposition que, pour NIS 2, le contrôle sera effectué par l'Anssi, avec la possibilité

de s’appuyer sur des tiers, y compris des agents de l’ACPR ou de la Cnil, et de faire appel à des acteurs du secteur privé. Il n’est pas nécessaire de rigidifier ce cadre dans la loi.

Par ailleurs, concernant l’articulation avec les collectivités territoriales, le gouvernement a choisi de ne pas imposer de sanctions financières, estimant que priver les collectivités de ressources ne favoriserait pas le développement de leur maturité en matière de cybersécurité. En revanche, d’autres mesures, telles que la publicité des manquements, sont considérées comme des moyens efficaces pour rappeler à l’ordre les collectivités qui ne joueraient pas le jeu. Ce choix du gouvernement est laissé à votre appréciation.

La déclinaison du dispositif pour les collectivités suit une approche comparable à celle d’autres États membres : les régions, départements et grandes agglomérations sont classés comme entités essentielles, les intercommunalités plus petites comme entités importantes, tandis que les communes individuelles ne sont pas directement concernées.

Je ne m’aventurerai pas sur le sujet des moyens budgétaires des collectivités, n’étant pas forcément légitime à porter la position du gouvernement sur ce point. Nous mobiliserons évidemment toutes les possibilités d’accompagnement, ce que nous faisons déjà. Nous avons soutenu, à travers le plan de relance, l’accompagnement méthodologique et l’incubation, ainsi que le développement des CIRT régionaux, complémentaires de l’action de l’Anssi. Il est prévu, dans le cadre de la transposition, que nous travaillerons avec ces CIRT, bien que je n’ai pas moi-même de réponse à la question de leur financement.

Sur le volet industriel, ma conviction est que cette directive représente une opportunité pour tout le tissu industriel, en particulier de proximité. Nous mobiliserons les experts cyber et les prestataires pour les accompagner dans cette transition. Je ne crois pas que cela se fasse en priorité au bénéfice d’acteurs non européens, qui ne sont pas nécessairement positionnés sur ce segment. Par conséquent, je ne juge pas nécessaire d’imposer le recours à des prestataires français.

Enfin, concernant le chiffrement, je comprends la teneur politique de l’article 16 *bis*. L’Anssi est évidemment très attachée, par nature, à la défense d’un chiffrement robuste, l’une de nos premières armes de protection contre les cybermenaces. De ce point de vue, l’article 16 *bis* affirme des principes que nous soutenons. Toutefois, sur le plan juridique, je ne sais pas s’il est nécessaire de le dire dans la loi. Je ne me prononcerai pas sur une éventuelle modification de cet article. Je dirai simplement que la protection du chiffrement et le pouvoir d’enquête des services judiciaires méritent un examen approfondi et ne peuvent être traités trop rapidement. Un travail au niveau technique est donc nécessaire sur ces sujets, avant de revenir au législateur, le cas échéant, afin qu’il arbitre. Ma conviction personnelle est que ce n’est pas dans le cadre du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité que nous résoudrons le problème fondamental porté devant le législateur dans le cadre de l’examen de la proposition de loi visant à sortir la France du piège du narcotrafic.

M. le président Philippe Latombe. Je cède maintenant la parole aux orateurs des groupes parlementaires.

M. Aurélien Lopez-Liguori (RN). Ce texte entraînera notre pays dans un monumental effort de cybersécurité, impliquant plus de 14 500 acteurs, dont des opérateurs d’importance vitale, des hôpitaux, des collectivités et des entreprises. Cet effort s’inscrit dans un contexte de tensions internationales majeures, où les attaques cyber se multiplient, les États

deviennent plus offensifs et l'espionnage se généralise via des règles extraterritoriales qui pullulent. Le numérique est désormais un champ de confrontation directe.

Dans ce contexte, l'effort national demandé doit non seulement servir notre souveraineté, mais aussi stimuler le développement économique de notre filière cyber. La France dispose en effet d'une industrie cyber d'excellence, avec des entreprises innovantes enracinées sur notre territoire, comme Tehtris, Gatewatcher, Ziwit, Wallix et HarfangLab. Ces sociétés ont démontré leur solidité technologique, obtenu des qualifications exigeantes de l'Anssi et contribuent déjà à la protection de nos systèmes vitaux.

Ce texte doit permettre que, pour leur protection cyber, les acteurs cyber concernées se tournent en premier lieu vers des acteurs nationaux et européens. C'est notre rôle, en tant que députés de la nation française, de veiller à ce que les retombées économiques et les externalités positives profitent prioritairement à notre écosystème, plutôt qu'à des sociétés étrangères susceptibles de nous espionner et de menacer nos intérêts via des règles extraterritoriales.

Quelles mesures proposez-vous pour que le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité devienne un levier concret de soutien à notre filière cyber nationale ?

Comment comptez-vous faire en sorte que NIS 2 confère une certaine immunité face aux règles extraterritoriales, à l'espionnage et aux ingérences étrangères ?

Envisagez-vous, dans les textes d'application, la création de labels de certification ou de critères de souveraineté permettant de favoriser les prestataires européens et français plutôt que les acteurs étrangers ?

M. Thomas Gassilloud (EPR). Je tiens à souligner la pertinence de ce texte face aux menaces opportunistes, mais également aux menaces plus structurées pouvant survenir d'États tiers, potentiellement en complément d'autres formes de menaces, y compris de nature cinétique. Je considère ce texte comme une opportunité de consolider notre défense face aux menaces hybrides au sens large, en complément de la démarche nationale entreprise, notamment dans le cadre de la stratégie de résilience.

Quelle articulation est prévue dans ce texte avec le commandement de la cyberdéfense (COMCYBER) ? Comment fonctionnent les interfaces et comment seront traitées les infrastructures critiques duales ?

Concernant la déclinaison territoriale, ce texte offre l'occasion de faire collaborer à froid des acteurs qui ne se connaissent pas nécessairement, autour des services déconcentrés de l'État, des chambres consulaires ou encore des services de l'éducation nationale. Il est crucial de ne pas oublier la chaîne de l'organisation territoriale interarmées de défense (OTIAD) autour des officiers généraux de zone de défense et des délégués militaires départementaux. J'espère que cette démarche permettra aux acteurs de mieux se connaître pour développer des réflexes utiles en temps de crise.

Enfin, je note que le renseignement d'origine sources ouvertes (Osint) n'est pas spécifiquement mentionné dans le texte, bien qu'il s'agisse d'un outil incontournable en matière de cybersécurité, ne serait-ce que pour identifier une exposition dans une base de données piratée. L'État utilise lui-même l'Osint pour ses services de renseignement et ses

questions de sécurité fiscale. Je note que le droit français semble imprécis sur ce point, ce qui incite parfois les acteurs à recourir à des opérateurs étrangers. Pensez-vous qu'il serait nécessaire de renforcer le texte sur cet aspect ?

M. René Pilato (LFI-NFP). Ce projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité place l'Anssi au cœur d'un objectif de résilience, d'où l'importance de cette première audition.

À l'heure où les intelligences artificielles suscitent de nombreuses interrogations et craintes, notamment en raison de leur potentiel de nuisance démultiplié, comment envisagez-vous l'évolution de vos missions face à la multiplication et au changement de nature des attaques liées aux intelligences artificielles, notamment concernant la falsification des données ?

Dans le cadre de votre mission première de protection de la nation, votre agence dispose d'une liste d'organismes d'importance vitale auxquels vous apportez prioritairement votre expertise et vos recommandations en cas de cyberattaque. Pouvez-vous nous indiquer à combien d'entités touchées par semaine ou par mois vous apportez votre expertise et votre soutien face aux attaques suivies ?

Ce projet de loi élabore des listes remaniées, plus larges, en fonction de secteurs hautement critiques pour le fonctionnement de l'économie et de la société, par l'intermédiaire des articles 7 à 10. Pensez-vous disposer des capacités humaines nécessaires pour assurer ces recommandations et protéger efficacement la souveraineté de la nation avec ces nouveaux périmètres ?

Enfin, l'agence que vous représentez est placée au service du premier ministre. Bien que la stratégie nationale en matière de cybersécurité soit une décision politique, je m'étonne de cette mise sous tutelle, alors que c'est votre indépendance qui devrait être notre garantie.

M. Sébastien Saint-Pasteur (SOC). L'Anssi doit être le phare éclairant le chemin de nos travaux, et plus encore celui des très nombreuses nouvelles entités assujetties à cette transposition. Dans le monde réel, la directive NIS 2 est déjà présente sur nos moteurs de recherche, avec des prestataires proposant services et audits moyennant de substantielles rémunérations. L'effet d'aubaine est réel, mais, malheureusement, ces prestations, dont les coûts annuels se chiffrent souvent à cinq chiffres, ne correspondent fréquemment ni aux besoins ni aux attentes dans de nombreuses situations. Il existe un risque de prestations inadaptées, avec des contrats signés dans l'urgence et dans une certaine méconnaissance, ce qui pourrait engendrer une défiance vis-à-vis de cette régulation pourtant nécessaire. La question d'une labellisation des structures, comme dans le domaine militaire, ou d'un référentiel d'exigences en termes de qualification se pose évidemment.

Il est nécessaire de consolider et renforcer les écosystèmes locaux, notamment les cyber campus, ces centres de réponse aux incidents cyber implantés dans de nombreux territoires. J'ai l'honneur d'avoir le siège du cyber campus Nouvelle-Aquitaine dans ma circonscription et vous connaissez probablement le travail remarquable réalisé en leur sein. Ne pensez-vous pas qu'il soit opportun de renforcer leurs moyens d'action et opérationnels ? Il faut certes des « pompiers » intervenant en cas d'urgence, mais aussi une médecine préventive. Les entreprises et collectivités concernées ont besoin, dans le cadre de cette nouvelle donne que constitue NIS 2, de savoir comment prioriser entre l'accompagnement des

utilisateurs, la sensibilisation des directions et des élus dans une collectivité, la sécurité des terminaux ou encore la refonte des systèmes réseaux dans une entreprise.

Ces deux questions visent à éclairer le dernier kilomètre de nos politiques publiques, au plus près des besoins, là où la menace est malheureusement grandissante.

Mme Sabine Thillaye (Dem). Si vous disposez aujourd'hui des ressources humaines et techniques nécessaires à l'exercice de vos missions, il me semble que l'Anssi compte 600 collaborateurs. Des recrutements seraient nécessaires dans votre agence, ainsi que dans les entités dont nous parlons. Or, nous sommes confrontés à un problème de recrutement et de concurrence entre le secteur civil et militaire pour les cyberspécialistes. Comment envisagez-vous de surmonter ce manque de ressources humaines ?

Par ailleurs, l'article 11 de la directive REC prévoit l'obligation, pour les États membres, d'organiser une coopération transfrontalière, notamment via les consultations. Or, contrairement à la directive, le projet de loi ne contient aucune disposition explicite transposant cette obligation. Cette lacune ne risque-t-elle pas de limiter l'efficacité collective de la réponse européenne en matière de protection des infrastructures ?

Enfin, concernant la mise en place du label attestant de la conformité des entités aux exigences de la directive NIS 2, ne craignez-vous pas que le développement de labels nationaux, en l'absence d'une harmonisation européenne, entraîne une fragmentation du marché et des coûts supplémentaires pour les acteurs opérant dans plusieurs États membres ?

M. Vincent Strubel. La coopération transfrontalière est déjà une réalité efficace et extrêmement active. Au niveau technique, elle s'opère via le CSIRTs Network, où la France est représentée par l'Anssi. Sur le plan stratégique, le réseau CyCLONe, regroupant les directeurs d'agences nationales de cybersécurité, joue un rôle crucial. Notre collaboration s'est notamment illustrée lors de la préparation des Jeux olympiques et paralympiques. Il n'est pas nécessaire d'introduire de nouvelles dispositions législatives pour organiser cette coopération. Le projet de loi comporte déjà quelques éléments visant à faciliter et sécuriser juridiquement l'échange d'informations avec la Commission européenne et nos homologues européens, dans le traitement de crises transfrontalières. Nous croyons profondément à cette coopération, qui est déjà une réalité essentielle, car nous sommes conscients que les incidents cyber ne s'arrêtent pas aux frontières. C'est une réalité quotidienne qui ne nécessite pas d'ajout supplémentaire dans la loi.

Je rejoins les observations faites sur l'effort considérable nécessaire pour développer notre résilience. Cet objectif s'inscrit dans l'objectif stratégique de la RNS et, plus généralement, dans un enjeu de souveraineté. Il s'agit de ne pas être une victime facile face aux cyberattaques, qui constituent une pression quotidienne et peuvent être mobilisées de manière plus coordonnée par certains États, où des acteurs étatiques, cybercriminels et activistes coexistent sans être inquiétés par les autorités répressives. Le risque d'une mobilisation massive de ces acteurs pour saboter des pans entiers de notre société et de notre économie est bien réel. Face à cette menace, renforcer notre niveau de résilience devient un défi de souveraineté essentiel. Il s'agit de protéger nos intérêts fondamentaux, d'éviter que des secteurs entiers ne soient facilement compromis et de développer une résilience, même face à des attaques très ciblées.

Bien que la directive NIS 2 ne vise pas principalement à contrer des groupes comme APT28, récemment attribué formellement par la France au renseignement militaire russe, il

est crucial de comprendre que même de petites entités peuvent être des victimes indirectes ou des cibles permettant d'accéder à de plus grands groupes. Élever globalement le niveau de résilience, tout en maintenant des exigences raisonnables par rapport à la maturité des acteurs, est un enjeu de sécurité nationale et de souveraineté. C'est essentiel pour nous préparer à un contexte géopolitique qui ne va pas en s'adoucissant.

Concernant le soutien à la filière française et européenne, je ne crois pas à de mesures contraignantes imposant le recours à des prestataires nationaux ou européens. Ce n'est d'ailleurs pas la base légale que donne la directive. Je crois plutôt à la mobilisation de l'écosystème, qui existe déjà, et au travail que nous menons avec les acteurs bénéficiant de visas de sécurité et de la qualification de l'Anssi. Nous avons travaillé sur nos référentiels de prestataires pour inclure des niveaux d'ambition moindres, afin de prévoir des prestations répondant plutôt aux besoins des ETI ou PME. Nous travaillons également avec des réseaux de prestataires proches de l'Anssi, comme les experts cyber labellisés par le groupement d'intérêt public (GIP) Cybermalveillance.gouv.fr. Notre philosophie est de n'exclure personne et de travailler en proximité avec les acteurs nationaux déjà mobilisés sur ce sujet. Nous veillons à prévenir les effets d'aubaine et la vente de prestations mensongères. Il est important de poser rapidement un cadre clair, applicable et déclinable par tous, même si nous travaillons déjà avec les acteurs de l'écosystème sur ces questions.

Par ailleurs, l'immunité face aux droits extraterritoriaux est évidemment une préoccupation qui se décline dans le référentiel SecNumCloud de l'Anssi, dans la stratégie cloud de l'État, et plus récemment dans la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. Cependant, ce n'est pas le cœur du sujet pour les petites entités concernées par la directive NIS 2. Cette problématique concerne davantage les entreprises stratégiques ou certains secteurs d'activités spécifiques.

En termes d'articulation, nous proposons en revanche de valoriser les prestations disposant d'un visa de sécurité de l'Anssi. Sans l'imposer, nous souhaitons que le recours à un acteur bénéficiant d'un visa de sécurité, d'une recommandation de l'Anssi ou d'un label de confiance apporte une plus-value dans la satisfaction des exigences de la directive NIS 2.

Par ailleurs, en 2024, nous avons traité plus de 4 000 incidents de cybersécurité, concernant non seulement des opérateurs d'importance vitale, mais aussi d'autres entités qui nous sollicitent volontairement.

Il est évident que nous devrons renforcer nos moyens, ce qui fera l'objet de discussions budgétaires ultérieures.

Notre présence territoriale est assurée par un délégué de l'Anssi dans chaque région, coordonnant les acteurs locaux et appliquant notre cadre commun afin d'armer la fonction de contrôle. Nous avons besoin de mobiliser tous les acteurs de proximité, mais je pense qu'un certain nombre d'eux l'est déjà. En outre, la gendarmerie joue un rôle essentiel dans les territoires en utilisant le même outillage que nous, notamment « Mon Aide Cyber », pour établir de premiers diagnostics.

Les campus cyber sont principalement positionnés aux points de rencontre entre des offreurs et des bénéficiaires. Je recommande la prudence quant à l'attribution de missions supplémentaires et je ne juge pas nécessaire de figer leurs missions dans la loi. Chaque campus régional s'inscrit dans un écosystème particulier à l'échelle locale. N'allons pas imposer un modèle unique alors que ce qui existe fonctionne déjà très bien.

Par ailleurs, notre articulation avec le COMCYBER est une réalité quotidienne, notamment au sein du centre de coordination des crises cyber (C4), et nous permet de partager des éléments d'analyse, de compréhension de la menace et d'attribution d'une cyberattaque. Cette coopération nous a récemment permis d'attribuer formellement une cyberattaque marquante à un acteur russe particulièrement présent. Pour les menaces touchant la sphère de la défense, nous travaillons étroitement avec le COMCYBER – qui est autonome sur la sécurité du ministère des armées, mais n'est pas forcément chargé de la sécurité de la BITD – et la direction du renseignement et de la sécurité de la défense (DRSD), sans qu'il soit nécessaire de formaliser davantage cette collaboration dans la loi.

La déclinaison territoriale des bons réflexes de sécurité est un enjeu fondamental, qui ne sera pas seulement porté par la loi. Nous croyons beaucoup aux vertus des entraînements et des exercices, comme nous l'avons fait pour la préparation des Jeux olympiques et paralympiques ou la sécurisation des hôpitaux. À une échelle encore plus grande, dans la perspective du déploiement de NIS 2, nous organiserons l'exercice massif REMPAR25 en octobre 2025, qui mobilisera des collectivités et visera à entraîner les décideurs à la gestion de crises cyber.

Enfin, l'Osint fait partie de la panoplie de la réponse ou de l'anticipation des attaques. L'Anssi pratique Osint comme tout acteur de cybersécurité. Si je suis favorable à l'utilisation de l'Osint, je ne suis néanmoins pas certain qu'une base légale soit nécessaire, car son utilisation ne semble pas illégale dans son état actuel. Je suis ouvert à d'éventuelles propositions d'ajustement, mais, si rien n'empêche le recours à des prestations d'Osint, il ne semble pas nécessaire d'imposer un cadre légal.

M. le président Philippe Latombe. Je cède la parole aux députés pour leurs questions individuelles.

M. Emeric Salmon (RN). Depuis 2013, la loi impose aux opérateurs d'importance vitale d'utiliser des solutions qualifiées par l'Anssi et opérées depuis la France, garantissant ainsi fiabilité et souveraineté. L'article 16 du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité revient sur ce principe. Les opérateurs d'importance vitale utiliseront des produits certifiés, agréés ou qualifiés, la seule qualification, plus exigeante, n'étant plus obligatoire. Le label actuel serait supprimé et remplacé par les exigences issues de cette loi. Pire encore, l'article supprime toute obligation légale de localisation en France pour ces solutions. Cette mesure représente un recul significatif, affaiblissant la protection de nos données les plus sensibles et pénalisant les entreprises françaises ayant investi pour répondre à ces standards.

Pourquoi abandonner un dispositif éprouvé depuis dix ans ?

Les nouvelles règles offriront-elles au moins le même niveau de protection ?

Envisagez-vous d'intégrer un critère de souveraineté pour les prestataires chargés de protéger nos infrastructures vitales ?

M. Vincent Strubel. Je n'ai pas la même lecture de la loi. Le cadre cyber qui s'impose aux opérateurs d'importance vitale est porté par le code de la défense, rénové à travers la transposition de la directive REC. Notre objectif est d'inscrire dans la loi des exigences similaires. Les articles concernés du code de la défense sont relativement succincts et se déclinent ensuite au niveau réglementaire par le décret n° 2015-350 du 27 mars 2015

relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité des systèmes d'information et le décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense, ainsi que par des arrêtés sectoriels définissant des exigences spécifiques. La LPM de 2013 et l'article que cette dernière introduit dans le code de la défense nous permettent d'imposer, dans certains cas, le recours à des solutions qualifiées pour les opérateurs d'importance vitale. La proposition actuelle suit la même logique, en établissant une base légale qui sera ensuite déclinée au niveau réglementaire.

Actuellement, trois obligations s'imposent spécifiquement aux opérateurs d'importance vitale : le recours à des prestataires d'audit de sécurité des systèmes d'information (PASSI), qualifiés par l'Anssi, ainsi que le recours à des prestataires de détection et à des sondes réseaux de détection, également qualifiés par l'Anssi.

L'esprit du travail d'actualisation, en lien avec le titre I^{er}, est de maintenir un niveau d'exigence fort, notamment concernant le recours à des prestations qualifiées.

Concernant les sondes de détection, nous réexaminons actuellement cette question, non pas pour l'affaiblir, ce qui serait contraire à notre mission d'autorité nationale de cybersécurité, mais pour l'actualiser au regard de l'état de l'art.

Le cadre établi en 2013 se concentrait uniquement sur la détection réseau, c'est-à-dire l'analyse des flux entre le système d'information d'importance vitale et internet. Bien que toujours pertinente, cette approche n'est plus suffisante. Aujourd'hui, une stratégie de détection efficace doit combiner plusieurs sources : détection réseau, détection système et analyse de journaux. La France dispose heureusement de solutions dans tous ces domaines. En outre, pour la détection réseau, nous avons des sondes qualifiées par l'Anssi. Pour la détection système, il existe des outils de détection locaux, appelés EDR, comme ceux de la société HarfangLab, également qualifiés par l'Anssi. Ces éléments doivent être remis au goût du jour, et non pas démontés.

Un ajustement en termes de spécifications des exigences pourrait être réalisé. Toutefois, les principes fondamentaux resteront inchangés : le système d'information d'un opérateur d'importance vitale doit être supervisé et capable de détecter des attaques stratégiques émanant de services étatiques. Cela nécessite une détection de grande qualité et de confiance. Nous adapterons ces principes à l'évolution de l'état de l'art, avec potentiellement une obligation de résultat plutôt que de moyens, mais les consultations se poursuivent sur ce sujet.

M. le président Philippe Latombe. Je vous remercie. Nous examinerons la possibilité de répondre à la demande du rapporteur général de vous réentendre ultérieurement. Cependant, vous ne serez pas le dernier intervenant, car nous avons prévu d'auditionner en dernier lieu Mme la ministre chargée de l'intelligence artificielle et du numérique, ce qui servira de base à notre discussion générale. Nous avions le souhait de débuter ce cycle par votre audition, qui sera suivie par celle du SGDSN la semaine prochaine.

La séance est levée à dix-sept heures quarante-cinq.

Membres présents ou excusés

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

Réunion du mercredi 7 mai 2025 à 16 h 30

Présents. - M. Édouard Bénard, M. Éric Bothorel, M. Mickaël Bouloux, Mme Sophie Errante, M. Julien Gabarron, M. Thomas Gassilloud, Mme Catherine Hervieu, M. Philippe Latombe, Mme Anne Le Hénanff, M. Aurélien Lopez-Liguori, M. Laurent Mazaury, M. René Pilato, M. Julien Rancoule, M. Sébastien Saint-Pasteur, M. Emeric Salmon, Mme Sabine Thillaye

Excusés. - M. Pouria Amirshahi, M. Vincent Thiébaut