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

Jeudi 5 juin 2025
Séance de 9 heures 30

Compte rendu n° 8

SESSION ORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 9 heures 30

La commission spéciale a organisé une table ronde réunissant des experts de la cybersécurité : CyberTaskForce : M. Sébastien Garnault, fondateur, M. Philippe Luc, co-fondateur de Anozr Way et Mme Anne-Elise Jolicard, responsable des affaires publiques ; Clusif : Mme Florence Puybareau, directrice, M. Benjamin Leroux, administrateur, Mme Garance Mathias, administratrice, et Mme Eva Aspe, en charge des affaires publiques ; Hexatrust : M. Jean Noël de Galzain, président, Mme Dorothée Decrop, déléguée générale et Mme Sara Durand, consultante ; CyberCercle : Mme Bénédicte Pilliet, présidente, MM. Christian Daviot et François Coupez, senior advisors ; CESIN : Mme Mylène Jarossay, vice-présidente, et M. Arnaud Martin, vice-président ; Alliance pour la confiance numérique (ACN).

M. le président Philippe Latombe. Mes chers collègues, nous poursuivons nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité avec une table ronde rassemblant des spécialistes de la cybersécurité. CyberTaskForce est représenté par son fondateur Sébastien Garnault, Philippe Luc, membre de Cyber Task Force et président d'Anozr Way, ainsi que par Anne-Élise Jolicard, responsable des affaires publiques d'Anozr Way. Nous recevons également les représentants de CyberCercle : Bénédicte Pilliet, sa présidente, ainsi que Christian Daviot, François Coupez, Stéphane Meynet, tous trois *senior advisors*. Le Clusif est représenté par trois administrateurs, Benjamin Leroux, Michel Dubois et Garance Mathias ; Hexatrust par son président Jean-Noël de Galzain et sa déléguée générale Dorothée Decrop. Enfin, nous accueillons Daniel Le Coguic, président de l'Alliance pour la confiance numérique (ACN) accompagné du directeur général Yoann Kassianides ; ainsi que les vice-présidents du club des experts de la sécurité de l'information et du numérique (Cesin), Mme Mylène Jarossay et M. Arnaud Martin.

La France bénéficie d'un écosystème dynamique et structuré dans le domaine de la cybersécurité, à la fois grâce à ses entreprises qui conçoivent et développent des solutions innovantes et à ses associations qui œuvrent activement à la sensibilisation des acteurs économiques face aux risques cyber.

À ce titre, l'Agence nationale de la sécurité des systèmes d'information (Anssi) a par exemple organisé le 17 février dernier au Campus Cyber un exercice grandeur nature de gestion de crise. Cette initiative a permis de renforcer la coordination des différents acteurs et d'enrichir notre culture de réponse face aux menaces émergentes. Le projet de loi que la commission spéciale est chargée d'examiner vise à renforcer notre cadre juridique en matière de cybersécurité, notamment dans le cadre de la transposition de la directive européenne NIS 2, qui fait l'objet du titre II du projet de loi. Il ne faut pas non plus oublier le titre I^{er}, consacré à la résilience des activités d'importance vitale et qui procède à la transposition de la directive sur la résilience des entités critiques (REC) ; et le titre III, consacré à la résilience opérationnelle numérique du secteur financier qui procède à la transposition de la directive sur la résilience opérationnelle numérique du secteur financier (Dora).

Dans ce contexte, nous souhaitons vous entendre sur la manière dont vous percevez le projet de loi et les éventuels angles morts auxquels il faudrait remédier dans le cadre de l'examen du projet de loi par l'Assemblée nationale.

M. Philippe Luc, membre de Cyber Task Force et président d'Anozr Way. Je vous remercie pour cette invitation et pour l'attention que vous voudrez bien porter aux préoccupations que nous vous remontons. Je suis Philippe Luc, président d'Anozr Way, une société spécialisée en cybersécurité, membre du bureau national de l'Alliance pour la confiance numérique. Nous nous exprimons aujourd'hui en tant que témoins d'une évolution préoccupante de la menace cyber, des tactiques des attaquants et de l'adaptation parfois insuffisante des stratégies de défense. Malgré un niveau de maturité croissant des entreprises et de nos institutions, jamais elles n'ont été autant exposées.

Comment expliquer ce paradoxe ? Nous pensons que ceci est d'abord lié à une inadéquation entre nos stratégies de défense et celles des attaquants. Les défenses restent largement pensées selon des logiques techniques, alors que les attaques reposent sur une approche dynamique, opportuniste et surtout humaine. Le directeur général de l'Anssi a évoqué à juste titre la notion de menace systémique capable de fragiliser tout un système par simple effet domino.

Si nous avons progressé sur le terrain des vulnérabilités techniques, la principale faille aujourd'hui est humaine. Prenons un exemple concret : un salarié clique sur un lien d'hameçonnage, un logiciel malveillant s'introduit, se propage via des interconnexions à d'autres entreprises, et finalement, l'ensemble d'un réseau économique est menacé. Le point d'entrée est souvent humain, et cet hameçonnage n'est qu'un point de départ. Aujourd'hui, les vulnérabilités humaines sont devenues multiples et complexes. Un attaquant peut exploiter des informations personnelles, comme une dette de jeu en ligne, pour faire pression sur un salarié dont il pourrait même louer les identifiants, ou les avoir volés déjà au préalable.

Cela devient le modèle économique du cybercrime et le point commun de bon nombre d'attaques qualifiées de techniques. Le facteur humain est désormais le principal vecteur de propagation des menaces systémiques. Les attaques par ingénierie sociale, l'hameçonnage, les *deep fake* utilisent des données personnelles disponibles en source ouverte – on parle de renseignements d'origine source ouverte (Osint). Les attaquants maîtrisent parfaitement ces techniques pour manipuler les individus. Nos stratégies de défense sont inefficaces, car nos dispositifs classiques de sécurité ne prennent pas en compte la réalité du risque humain, et tous les audits de sécurité classique que l'on peut mener ne détectent pas les comportements à risque, les mots de passe réutilisés ou les informations sensibles, nécessaires à la réalisation de ces scénarios d'attaques par ingénierie sociale.

J'en profite également pour préciser qu'on ne résoudra pas le problème du facteur humain uniquement par des sessions de *e-learning* ou des tests d'hameçonnage. Nous devons passer d'une posture statique de sensibilisation à une posture active de gestion du risque humain par un *monitoring* continu du risque d'exposition de ces utilisateurs aux attaques par ingénierie sociale. Cela devra impérativement être intégré dans le référentiel d'application qui accompagnera ce projet de loi.

La France possède déjà un savoir-faire solide en la matière. Dans ce contexte, la directive NIS 2 représente une opportunité cruciale. Elle consacre l'intégration du facteur humain comme un élément central de la résilience cyber. Pourtant, dans sa première version, le projet de loi français ne faisait aucune mention des vulnérabilités humaines. Il a fallu un amendement du Sénat pour les réintroduire, soit une avancée majeure que nous saluons. Cependant, nous devons aller plus loin. Au-delà de l'établissement d'un cadre technique, la directive NIS 2 constitue un véritable changement de paradigme. Elle nous invite à penser la

cybersécurité non plus uniquement en termes de protection, mais en termes de gestion active du risque, en intégrant pleinement les erreurs humaines.

Cela suppose impérativement de travailler sur les définitions. La définition de vulnérabilité a été intégrée, mais la notion de cyber menace ou d'approche « tous risques » reste toujours absente du corpus juridique. De leur côté, nos voisins allemands et italiens les ont intégrées, et l'Allemagne vise explicitement les considérants 78 et 79 de la directive, qui détaillent cette approche globale. Les Italiens en ont même tiré une définition à part entière. De fait, on ne peut pas atteindre un haut niveau de résilience convenable si l'on ne définit pas précisément les termes de risque, de menace et de vulnérabilité. Le sujet n'est pas uniquement français, mais se situe au niveau européen. Il est nécessaire que nous nous accordions sur une même définition en Europe.

En conclusion, si nous voulons sortir de cette spirale d'attaque, nous devons changer de regard. Le cyber criminel moderne n'a pas besoin de forcer la porte ; il sait que quelqu'un lui ouvrira ou qu'une clé traînera sous le paillasson. La directive NIS 2 nous offre l'opportunité d'abandonner une posture purement défensive pour construire une cybersécurité fondée sur l'anticipation, la pédagogie et la gestion proactive du risque humain.

Mme Garance Mathias, administratrice du Clusif. Les propos du Clusif se concentreront particulièrement sur le titre II relatif à la transposition de la directive NIS 2, un enjeu extrêmement important, y compris pour la collectivité du Clusif, peut-être la seule association à être reconnue d'utilité publique depuis la fin de l'année 2024. Dans le cadre de cette transposition de textes très ambitieux, il importe de ne pas se concentrer uniquement sur la France métropolitaine, mais d'appréhender la richesse de l'ensemble de nos territoires. Au sein de l'association que nous représentons aujourd'hui, nous avons également la chance de disposer de clubs de la sécurité de l'information en réseau (Clusir) outre-mer.

Ensuite, il nous semble très important de revenir plus spécifiquement sur le choix des référentiels. Je cède la parole à M. Dubois, qui abordera la question des sanctions, mais aussi la notification des incidents, un aspect opérationnel très important qui concerne l'ensemble des acteurs, collectivités, administrations ou entreprises. Votre projet de loi doit être envisagé comme une opportunité et non uniquement comme une contrainte.

M. Michel Dubois, administrateur du Clusif. Le Clusif appelle à établir un référentiel qui s'appuie sur la famille des normes ISO 27000, à l'instar de la Belgique. En effet, la norme ISO 27002 présente notamment l'avantage d'être opérationnelle dans toute l'Europe et de constituer un élément clé dans la mise en conformité des organisations. La norme ISO 27001 étant certifiante, une approche similaire à la Belgique proposant soit une certification 27001, soit une conformité à un référentiel local, semble constituer une approche intéressante.

M. Benjamin Leroux, administrateur du Clusif. Il est important que ce référentiel soit reconnu dans les autres pays de l'Union européenne. À ce titre, une norme comme ISO peut être intéressante. Si elle n'est pas finalement retenue, il faudra que le référentiel national puisse documenter sa compatibilité avec les autres référentiels locaux.

M. Michel Dubois. Un autre aspect concerne notamment la partie relative aux référents. Nous sommes favorables à une obligation pour les structures éligibles à NIS 2 de disposer d'un référent, que l'on pourrait appeler référent cyber sécurité, référent sécurité numérique ou tout simplement responsable sécurité des systèmes d'information (RSSI). Ce

référent aura un lien direct avec la direction de l'organisme, comme son comité exécutif et disposera de la légitimité et du soutien nécessaires aux travaux de mise en conformité et d'entretien dans le temps de cette conformité. Ce référent sera également le point de contact référent de l'Anssi.

M. Benjamin Leroux. Pour le Clusif, les entités publiques doivent également pouvoir être sanctionnées en cas de manquement, comme les entreprises privées. Il s'agit de la condition *sine qua non* d'une bonne prise de conscience de la part de la sphère publique. Il faut malheureusement parfois en passer par là pour engager une prise de conscience et les travaux de mise en conformité. La responsabilité du dirigeant ne doit pas nécessairement se traduire par des sanctions pénales. La logique consiste à faire prendre conscience de la nécessité de lancer et d'entretenir des travaux de mise en conformité, pour la maîtrise du risque cyber.

Mme Garance Mathias. En matière de sanctions, l'opinion du Clusif se rapproche de l'avis donné il y a déjà quelques mois par le Conseil d'État, notamment sur le point 9 : « *il n'en va pas de même pour les collectivités territoriales et de leurs regroupements et d'établissements, en l'absence des dispositifs d'effet équivalent et qu'en conséquence, cette exemption ne peut être admise* ».

M. Michel Dubois. Un autre point concerne la notification des incidents. Nous appelons à la mise en place d'une plateforme unique et d'un formalisme commun à toutes les entités pouvant être en attente de ces notifications, par exemple la Commission nationale de l'informatique et des libertés (Cnil), l'Anssi ou encore l'Autorité de contrôle prudentiel et de résolution (ACPR) en ce qui concerne le règlement Dora. Ce point est particulièrement structurant pour les entités assujetties à Dora et à NIS 2. Une telle plateforme nous semble être un facteur de simplification et d'accélération des procédures pour les référents.

M. Benjamin Leroux. Enfin, nous savons d'expérience que les organisations présentent des niveaux de maturité très variables par rapport à la problématique cyber. Nous suggérons de nous inspirer de ce qui a été réalisé en Belgique avec Safeonweb, qui propose une très belle plateforme documentée pour la compréhension des mesures et le suivi de leur mise en application.

M. Jean-Noël de Galzain, président d'Hexatrust. Je me concentrerai pour ma part sur un aspect qui me paraît important, dévoilé récemment par le rapport d'Asterès : aujourd'hui, 83 % des achats de produits et services numériques réalisés en Europe sont effectués auprès de fournisseurs extra-européens, particulièrement auprès des Gafam. Nous ne résoudrons pas notre problème de dépendance numérique en continuant avec le modèle actuel. La cybersécurité constitue un moyen clé de reprendre une part de contrôle sur notre vie numérique.

Un aspect clé de cette directive NIS 2 concerne l'accompagnement des utilisateurs. À ce titre, je rejoins les propos tenus précédemment concernant le *monitoring* continu des risques. Il s'agira de s'appuyer sur un certain nombre de dispositifs pour la plupart existants. Ils sont portés par une industrie émergente et bénéficient parfois d'une certification de la part de l'Anssi. Nous pensons qu'il faut insister dans tous les textes relatifs au numérique et à la cybersécurité sur la protection des données et l'usage de solutions certifiées, à chaque fois que cela est possible, pour aligner les recommandations de l'Anssi ou des organismes européens avec les travaux de la filière.

Nous estimons aussi que l'accompagnement doit se concentrer sur l'ensemble du tissu de PME sous-traitantes des grandes organisations, qui constituent aujourd'hui le « maillon faible », car elles manquent de moyens, de compétences et de ressources. Ces dernières sont directement affectées par cette réglementation et devront être accompagnées sur tous nos territoires. De nombreux travaux sont menés par la filière pour y parvenir.

La directive NIS 2 constitue une chance de mettre l'industrie de la cybersécurité et l'industrie du numérique au service des besoins des utilisateurs. Il s'agit d'une opportunité pour alimenter une politique industrielle résolument tournée vers les utilisateurs, autour d'un nouveau standard de la gestion du risque, de la gouvernance de la cybersécurité. Il faut capitaliser sur la directive NIS 2 pour aligner les utilisateurs et leurs besoins, l'État qui veille à la sécurité et à l'accès de tous à la sécurité, et l'industrie qui fabrique des solutions et propose des services pour répondre à ces besoins.

Deux comités stratégiques de filière, le comité stratégique de la filière industrie de sécurité et le comité stratégique de la filière logiciels et solutions numériques de confiance ont instauré des organes de travail permanents entre l'État, l'industrie et les utilisateurs. Ils doivent être utilisés au maximum pour traiter les problèmes concernant les interactions entre les utilisateurs et l'industrie et les aligner avec la volonté de standardisation et de normalisation de la directive NIS 2.

Je souhaite à ce titre mentionner une initiative qui s'est déroulée il y a trois ans, dans le cadre du dispositif France Relance, au service des hôpitaux et des collectivités locales, en portant l'effort sur la demande de ces utilisateurs, en les aidant et en les incitant à s'équiper. Cette initiative a démontré que nous étions en mesure de répondre aux besoins des utilisateurs en matière de cyber lorsque les différentes composantes travaillent de manière coordonnée. Grâce à l'investissement, notamment à travers le crédit d'impôt recherche (CIR) ou d'autres dispositifs d'aide à l'innovation, nous disposons aujourd'hui d'une industrie émergente extrêmement performante, qui pourra se mettre au service des utilisateurs à l'occasion de la mise en place et de la mise en œuvre de cette directive NIS 2.

De nombreux efforts ont été régulièrement produits pour aider à la sensibilisation. Aujourd'hui, l'intelligence artificielle (IA) doit être au maximum utilisée pour rendre l'audit plus accessible au plus grand nombre, de manière systématique. Nous avons nous-mêmes œuvré en réunissant les adhérents pour créer un « HexaDiag », qui permettra aux entreprises de toute taille et de tout niveau d'expertise cyber d'accéder à un premier niveau de diagnostic. Nous sommes allés plus loin dans le cadre de l'« HexaSearch », pour permettre à des organisations de trouver des solutions numériques européennes et souveraines alternatives à celles qui existent par ailleurs et sur lesquelles le contrôle est difficile à opérer.

Mme Bénédicte Pilliet, présidente de CyberCercle. Mon intervention a pour objet d'insister sur les points d'attention qui nous semblent majeurs. Pour CyberCercle, la transposition de ces trois textes européens dans notre droit représente une occasion unique de renforcer la cohérence, la lisibilité, la clarté et l'efficacité de la réglementation en matière de cybersécurité et des politiques publiques qui y sont associées.

À ce titre, j'aborderai six points qui nous semblent particulièrement importants pour renforcer au sein du projet de loi la cohérence entre les différents dispositifs prévus par les trois textes, mais aussi la cohérence avec les textes et dispositifs existants. Le premier point concerne la nécessité d'une stratégie nationale. L'article 5 *bis* introduit par le Sénat, qui

pourrait d'ailleurs être remis en cause par le gouvernement au prétexte que des stratégies plus globales sont en cours de rédaction, nous semble indispensable.

L'élaboration d'une stratégie inscrite dans la loi permettra à l'ensemble des acteurs concernés d'avoir régulièrement un cap et un cadre de référence, mais aussi de mieux comprendre l'organisation et la coordination au sein de l'État et les responsabilités de chacun. Il s'agit ainsi de coordonner dans un même cadre et vers les mêmes objectifs les actions de tous et d'assurer la cohérence des dispositifs. La nécessité d'une stratégie nationale claire de cybersécurité a d'ailleurs été évoquée à plusieurs reprises lors de vos auditions précédentes, notamment celle des collectivités. Cette stratégie permettra également au Parlement de contrôler et d'évaluer l'efficacité des mesures prises et de la dépense publique consacrée à la cybersécurité. Afin d'optimiser sa rédaction, il serait pertinent qu'une commission réunissant les parties prenantes élabore ses stratégies, comme c'est le cas pour le Livre blanc de la défense et de la sécurité nationale.

Le deuxième point concerne la cohérence dans les acteurs impliqués. Ainsi, l'absence des ministères est inexplicable dans la mise en œuvre de NIS 2. Au-delà de notre conviction que pour être efficace envers des secteurs d'activité par nature très différents les uns des autres, une approche par métier est capitale. Il s'agit là de mettre en cohérence les trois textes transposés quant au rôle des ministères coordonnateurs des secteurs d'activité concernés par les directives REC, NIS 2 et Dora. Les quelques centaines d'opérateurs d'importance vitale mentionnés au titre I^{er} du projet de loi sont identifiés et suivis par les ministères coordonnateurs du secteur d'activité auquel ils appartiennent.

Le même principe s'applique pour le titre III du projet de loi : les autorités financières, dont les ministères économiques et financiers, suivent et contrôlent les quelques milliers d'acteurs visés par le règlement Dora. Mais alors que dans le titre II, il s'agit de suivre des dizaines de milliers d'entités visées par la directive NIS 2, seule l'Anssi est en charge de l'ensemble dans le texte, les ministères étant finalement exclus de tout le processus Pourtant, ce sont bien les ministères qui, de fait, connaissent le mieux les métiers, les dépendances et les conséquences d'une défaillance d'un opérateur et les conditions de résilience dans les secteurs d'activité dont ils ont la charge. Ajoutons que dans un objectif d'optimisation de l'action des acteurs et des moyens de l'État, le rôle des ministères relève du bon sens.

Il nous semble donc essentiel d'introduire les ministères coordonnateurs dans le titre II du projet de loi, au moins dans les quatre étapes du processus : la validation et le complément éventuel des listes des entités essentielles et importantes (article 12) ; la définition des objectifs de sécurité et des référentiels d'exigence (articles 14 et 15) ; les contrôles (article 29) et la commission des sanctions (article 36).

Le troisième point est relatif à la cohérence dans les objectifs de sécurité et les référentiels de mesures techniques et organisationnelles. Dans l'article 14, un décret fixe les objectifs de sécurité auxquels doivent se conformer les entités essentielles et les entités importantes. Cependant, il n'est pas précisé qui définit les objectifs, ni comment. Pourtant, un peu plus loin dans le même article, ces éléments sont indiqués pour les référentiels d'exigence technique et organisationnelle.

Dans l'article 15, les entités qui mettent en œuvre tout autre référentiel reconnu équivalent par l'Anssi peuvent s'en prévaloir lors d'un contrôle. Il y a là une incohérence. Ces référentiels équivalents devraient également, comme dans l'article 14, être définis par les

métiers, d'autant plus si ces référentiels sont sectoriels, exigés par les marchés ou issus d'autres réglementations s'imposant à eux.

Enfin, dans son article 25 portant sur la normalisation, la directive NIS 2 précise « *qu'afin de favoriser la mise en œuvre convergente des mesures de gestion des risques en matière de cybersécurité, les États membres encouragent le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information* ». Cet article important de la directive NIS 2 n'a pas été transposé. Pour nous, il y a là une occasion manquée d'une harmonisation au niveau européen ou international, qui aurait soutenu la compétitivité de nos acteurs économiques. Au contraire, le renvoi de l'article 14 du projet de loi examiné par votre commission annonce un énième référentiel franco-français dont le coût de la conformité technique et organisationnelle s'ajoute à celui du coût de la conformité aux normes que les entreprises doivent respecter pour gagner des marchés. En outre, nous pointons les oppositions existantes entre les prescriptions du projet de référentiel Anssi et les obligations des actes d'exécution pris en application de Dora au niveau européen.

Le quatrième point concerne la cohérence et la clarté, voire l'égalité devant la loi en ce qui concerne les contrôles. L'article 29 précise que les contrôles de l'Anssi peuvent prendre plusieurs formes, dont celle d'audits réguliers et ciblés réalisés par un organisme indépendant désigné par l'Anssi. Le coût de cette forme de contrôle est à la charge des personnes contrôlées alors que, pour les autres formes, il relève de l'Anssi. Il nous semblerait pertinent d'encadrer le terme « réguliers » et de préciser à quoi correspond un organisme indépendant désigné par l'Anssi. Pourquoi existe-t-il une telle différence de traitement des entités ? Qui choisira parmi les différentes formes de contrôles celles qu'une entité devra subir et donc si ce contrôle sera ou non à sa charge ?

Le cinquième point est lié à la cohérence dans les sanctions. Deux points sujets à questionnement figurent dans l'article 37 relatif aux sanctions. La commission des sanctions peut prononcer une amende administrative pour les entités essentielles et importantes, à l'exception des administrations et des collectivités territoriales. L'amende ne concerne donc que les entreprises privées. Pourquoi l'interdiction d'exercer des responsabilités pour les dirigeants des entités essentielles ne s'appliquerait-elle pas à l'administration ? De plus, comment appliquer cette interdiction à l'élu d'une collectivité ? Pour plus de transparence et pour éviter d'avoir le sentiment qu'aucune sanction ne sera prononcée contre l'administration, cet article pourrait ainsi préciser les moyens utilisables par l'État, en lien avec l'avis du Conseil d'État du 6 juin 2024.

Enfin, le dernier point sur lequel nous nous permettons d'insister porte sur l'exploitation de l'information relative à la menace, non seulement par les entités visées par NIS 2, mais également par leurs prestataires. Nous n'entrons pas dans le cœur des débats sur le sujet, qui agitent l'écosystème, mais constatons simplement que l'article 45 du règlement Dora donne un cadre à l'échange d'informations entre les acteurs visés par Dora. Ne pas transposer l'article 29 prévu dans la directive NIS 2, portant sur le même sujet, introduit de fait une inégalité et une incohérence pour les entités soumises à Dora et à NIS 2.

Pour conclure, je voudrais citer le rapport d'activité 2024 de l'Anssi relatif au parcours de cybersécurité dans le cadre du programme de France Relance. Même si ce rapport partiel ne permet pas d'évaluer réellement l'efficacité des 100 millions d'euros dépensés pour les 945 entités publiques sélectionnées parmi plus de 1 600 candidatures, il met en évidence deux faits. Initialement, la note cyber moyenne des bénéficiaires de ce programme était de

D+ soit une mauvaise note. Ainsi, treize ans d'empilement de réglementations s'imposant à la plupart de ces entités n'ont pas permis d'élever leur niveau de cybersécurité. Sans réglementation supplémentaire, le niveau de cybersécurité de ces entités est passé de D+ à B, c'est-à-dire de « mauvais » à « bon », grâce à ce programme, pour un montant équivalent voire inférieur à celui annoncé pour NIS 2.

Lors d'une audition de votre commission, les collectivités ont insisté sur la nécessité d'être accompagnées pour ne pas subir de nouvelles réglementations qui, seules, n'apportent pas de maturité. Il en est de même d'ailleurs pour les entreprises. Aussi, si nous comprenons le choix de la France d'inscrire les collectivités dans le cadre de cette loi, devant la croissance de la menace, nous nous interrogeons sur le choix de soumettre autant de collectivités à NIS 2, d'autant plus qu'aucune analyse de l'impact financier n'a été menée.

En conclusion, cette transposition constitue une opportunité de renforcer la cybersécurité de notre pays et sa résilience en élevant le niveau de maturité des acteurs et en les embarquant dans une dynamique vertueuse. Les questions concernent le niveau du curseur et l'accompagnement des acteurs par des politiques publiques adaptées dans un contexte budgétaire restreint. Le Sénat a permis d'améliorer substantiellement le texte initial du gouvernement en introduisant encore plus de cohérence entre les différentes parties du texte. Votre commission spéciale pourrait faire émerger un texte encore plus pragmatique.

M. Daniel Le Coguic, président de l'Alliance pour la confiance numérique. L'Alliance pour la confiance du numérique représente l'industrie française dans le domaine de l'identité numérique, de la cybersécurité, de l'intelligence artificielle et des infrastructures de confiance. Elle a naturellement contribué depuis un an aux différents groupes de travail. Je souhaite d'ailleurs remercier l'Anssi et son directeur général Vincent Strubel d'avoir organisé cette discussion structurée pour préparer la constitution de ce texte.

Nous avons, à de nombreuses reprises, présenté un certain nombre de propositions, notamment d'ajustement. Certaines ont été prises en compte lors de notre audition au Sénat. Nous vivons une période très particulière sur les plans géopolitique, économique, social et de la sécurité, où il est souhaitable de mettre en avant les intérêts de l'industrie française. Les parties prenantes que nous avons consultées nous ont toutes fait part de la nécessité de simplification et de lisibilité : la directive ne doit être ni surtransposée, ni sous-transposée. Les cibles de NIS 2 sont aujourd'hui des entités peu matures dans le domaine de la cybersécurité. Elles doivent pouvoir comprendre le texte auquel elles sont soumises.

Ensuite, la divulgation de vulnérabilités nous semble être un point clé pour accroître la capacité de l'ensemble de ces entités à se défendre. Nous avons également proposé une incitation en direction des PME, un crédit d'impôt à définir, pour financer les investissements.

L'ACN soutient l'objectif général des trois textes, qui concerne l'augmentation de la résilience de la nation. Nous sommes attendus par nos citoyens. Mais il faudra être attentif à la mise en œuvre du texte. Nous soutenons les nombreux dispositifs d'ajustement qui ont été proposés, dans un objectif de simplicité et d'efficacité. Sur un horizon de trois ans, nous devrions atteindre l'objectif des 12 000 à 16 000 cibles à traiter.

Ce programme stratégique offre une opportunité pour l'industrie française de reprendre une place particulière, alors que nous vivons aujourd'hui un puissant déséquilibre entre l'industrie extra-européenne et l'industrie européenne dans le domaine de la

cybersécurité. Si nous n'y prenons pas garde, la mise en œuvre du programme profitera à l'industrie extra-européenne qui possède déjà une part de marché de 80 %.

Il convient donc d'être très attentif aux conditions de mise en œuvre de ce programme. Nous proposons un objectif de transformation des investissements qui seront réalisés autour de NIS 2 et de Dora. Il s'agit ainsi de mettre en place un dispositif de mesures de l'empreinte de l'industrie française en particulier, qui sera la conséquence des investissements des établissements financiers, des institutions de santé, des collectivités locales et des entreprises.

En résumé, nous souhaiterions que le texte mentionne un objectif de 80 % de transformation et la mise en place d'un dispositif de mesure de l'augmentation de cette empreinte dans l'équipement de toutes les cibles. Cela compléterait les dispositifs de France 2030 sur l'innovation. Il s'agit bien de mettre en cohérence les programmes NIS 2 et Dora avec les objectifs économiques de l'industrie française.

En conclusion, il faut faire simple, il faut aller vite, il faut collaborer tous ensemble, qu'il s'agisse des associations d'utilisateurs, mais aussi des associations d'entreprises. Nous formons le vœu que se poursuive cette discussion structurée entre l'industrie et les pouvoirs publics, pour une mise en œuvre efficace au service des citoyens, des entreprises, des organisations publiques, de la cybersécurité et de la sûreté de notre nation.

M. Arnaud Martin, vice-président du Cesin, directeur des risques opérationnels de la Caisse des dépôts. Nous représentons le Cesin, le club des experts de la sécurité de l'information et du numérique, une association loi 1901 créée en 2012 dans un objectif de professionnalisation et de promotion de la cybersécurité. Ce lieu d'échange, de partage de connaissances et d'expériences permet ainsi la collaboration et la coopération entre pairs, mais également entre ses experts et les pouvoirs publics.

Il participe à des démarches nationales et il est force de proposition sur des textes réglementaires, guides et autres référentiels. Le Cesin compte parmi ses membres plusieurs organismes et institutions, ainsi que 1 200 membres qui sont issus de tous secteurs d'activité : industries, ministères et entreprises, dont la plupart des grands acteurs du CAC 40 et du SBF 120. Mylène Jarossay et moi-même en sommes vice-présidents. Mme Jarossay est directrice de la cybersécurité du groupe LVMH et je suis directeur des risques opérationnels du groupe Caisse des dépôts. À ce titre, nous sommes assujettis à NIS 2 d'un côté et à Dora de l'autre.

Nos retours d'expérience dans le cadre de cette audition sont bien évidemment ceux de notre propre expérience, mais également la consignation de l'ensemble des travaux qui ont été menés. Nous souhaitons tout d'abord souligner l'avancée notable que constitue l'ajout de deux articles au niveau du titre II, le 5 *bis* et le 16 *bis*. L'article 5 *bis* réaffirme que la déclinaison des textes de cybersécurité et de résilience se fait désormais dans un cadre faîtier, porté par la stratégie nationale en matière de cybersécurité de la France.

Si ce texte est la déclinaison de la stratégie qui a été travaillée au niveau du secrétariat général de la défense et de la sécurité nationale (SGDSN), nous insistons sur une des recommandations essentielles : la simplification globale du millefeuille réglementaire, à laquelle votre projet de loi participe bien évidemment. Le deuxième point concerne la réaffirmation du principe de non-affaiblissement des algorithmes de chiffrement dans votre texte dédié à la cybersécurité et à la résilience.

Mme Mylène Jarossay, vice-présidente du Cesin, directrice cybersécurité du groupe LVMH. Parmi les sujets propres au texte, je tiens à évoquer un certain nombre de points, en commençant par le lien entre Dora et NIS 2. Actuellement, les organismes assujettis à Dora sont évidemment focalisés sur leur mise en conformité par rapport à ce texte et s'interrogent. Il existe en effet une zone de flou dans leur éventuel assujettissement complémentaire à NIS 2, notamment les rôles et responsabilités que pourraient avoir la Banque centrale européenne (BCE) et l'ACPR vis-à-vis de l'Anssi.

Concernant NIS 2, une interrogation pèse sur les entreprises qui opèrent dans plusieurs pays européens et pour lesquelles le choix du référentiel par le groupe constitue un véritable casse-tête. Dans certains pays, les référentiels insistent plutôt sur l'analyse de risque, dans d'autres sur l'administration des systèmes d'information. Un groupe européen ou international ne s'y retrouve pas ; il est confronté à une complexification et non à une simplification.

La complexité concerne également l'éligibilité, c'est-à-dire le fait de savoir si l'on est assujetti ou non au texte. Il nous semble urgent que la France puisse très vite répondre aux entreprises concernant leur éventuelle éligibilité. Or un grand flou règne aujourd'hui. Les outils actuellement en place ne permettent pas aux entreprises de le déterminer. En conséquence, elles sont en retard, parce qu'elles n'engagent pas réellement leurs démarches.

Ensuite, nous rejoignons les propos qui ont été tenus précédemment sur le sujet de la notification des incidents. Il est important de se demander pourquoi le texte cherche impérativement à établir des délais courts de notification des incidents. Dans la réalité, quantité de signaux arrivent tous les jours dans les entreprises. Il est très difficile de savoir sous vingt-quatre heures si un signal est un « faux positif » ou s'il constituera le début d'une catastrophe. Il est donc très compliqué de produire une notification dans un tel délai, particulièrement s'il n'existe pas de guichet unique, d'autant plus pour une société paneuropéenne, qui devrait reproduire cette notification dans tous les pays dans lesquels elle est implantée. À ce stade, l'effort d'une entreprise ne doit pas être concentré sur la notification, mais sur la mise en place de renforts et la communication avec ses prestataires, d'autant plus qu'un incident sur deux provient de la chaîne d'approvisionnement.

Si finalement une attaque n'en est pas une ou qu'elle a été contenue très vite, donnons-nous la possibilité d'annuler une déclaration d'incident, et de ne pas faire courir le risque que cette déclaration porte éventuellement tort à l'entreprise. Cela nous paraît très important, afin que la notification des incidents demeure vertueuse et serve réellement à protéger.

Un autre point de vigilance concerne la déclinaison des exigences vis-à-vis des sous-traitants, des prestataires. Les entreprises éprouvent des difficultés pour mettre en place ces exigences. Aujourd'hui, il est question de mener des audits sur les fournisseurs, mais rappelons qu'en matière de cybersécurité, un audit ponctuel a peu de valeur : en réalité, la sécurité évolue tous les jours. Il faut peut-être revoir la façon dont on mesure finalement la capacité des tiers à se conformer au texte et le poids contractuel associé. De fait, une réflexion doit être conduite dans ce domaine, dans la mesure où le levier contractuel est très long et très difficile à mettre en place. De plus, la notion d'audit, très coûteuse n'est pas forcément adaptée au monde cyber.

Le dernier point est relatif au référent cyber, qui est naturellement essentiel, dans la mesure où le risque cyber figure parmi les trois principaux risques des entreprises. Quel que

soit le nom qui sera choisi, je préférerais que le terme de RSSI soit abandonné, dans la mesure où le dirigeant de l'entreprise est, *in fine*, le responsable.

M. Éric Bothorel, rapporteur général. Cette transposition de la directive européenne était attendue et même espérée par votre écosystème. Elle conforte les actions que vous avez commencées de façon volontaire il y a plusieurs années, pour nombre d'entre vous. Elle confirme que les craintes que vous exprimiez sont bien réelles. Lors des auditions du Sénat, vous avez rappelé l'évolution majeure de ce texte, qui passe d'une logique des seules infrastructures à celle des organisations et donc des personnes.

Il peut être considéré qu'à ce stade, le projet de loi ne fait pas de place à l'humain. Je souhaite donc vous interroger sur les évolutions – législatives ou autres – afin que les différentes personnes, les salariés, les fonctionnaires et les élus soient mieux associés au projet collectif de résilience.

Lors des dernières auditions, plusieurs acteurs nous invitaient à inscrire dans la loi un certain nombre de définitions, et vous l'avez aussi rappelé ce matin. Ce n'est pas forcément l'usage français, alors que l'Europe procède beaucoup par définition et normalisation. Pourriez-vous nous indiquer quels sont les termes qui nécessiteraient d'être inclus dans la loi ?

Par ailleurs, nombre d'acteurs soulignent tout à la fois l'excellente qualité du travail préparatoire et du dialogue avec l'Anssi. Mais les mêmes acteurs commencent à nous faire part de leurs interrogations sur le trop grand nombre de renvois à des décrets. Ils semblent préférer que les députés soient plus précis dans leur rédaction, allant parfois jusqu'aux détails. Partagez-vous ce point de vue ? Comment envisageriez-vous cette intégration dans la loi, par exemple du référentiel, compte tenu du nombre de détails que vous voulez voir inscrits ? Enfin, j'aimerais que nous parlions de l'Osint, du volet assurantiel.

Mme Anne Le Hénanff, rapporteure. La plupart d'entre vous travaillent sur la sensibilisation et l'accompagnement depuis des années. Mais ces actions de sensibilisation n'engendrent pas forcément une amélioration du niveau de cybersécurité des entités, particulièrement les collectivités locales. Or la directive entraînera un impact élargi sur l'ensemble des territoires. Comment pouvons-nous sensibiliser plus rapidement les collectivités locales ?

Comment comptez-vous sensibiliser et accompagner ce changement, dans le cadre de NIS 2 et au-delà, auprès des prestataires, des sous-traitants et des clients, qui ne sont pas directement dans les 15 000 entités mentionnées, mais qui devront sans doute procéder à des mises à jour ? Comment allez-vous prendre votre part à la cyber-résilience ?

Estimez-vous que la labellisation des entités est pertinente ? Est-il utile pour une entreprise d'indiquer à des clients, des prestataires, des sous-traitants qu'elle est en conformité ou en cours de conformité avec NIS 2 ? À ce sujet, il est souvent question de proportionnalité, mais peut-on également parler de proportionnalité sur la mise en conformité ?

Madame Mathias, vous avez mentionné la nécessité de tenir compte spécifiquement des territoires d'outre-mer. Faut-il en conclure que vous estimez que la rédaction actuelle est insuffisante à ce titre ? Avez-vous en tête des mesures spécifiques ?

Enfin, je souhaiterais connaître l'avis de chacun sur la notification d'incident. Constitue-t-elle le mode d'emploi adapté en termes de mécanismes, de principes et de mesures ?

M. Daniel Le Coguic. Ma réponse se concentrera sur la sensibilisation et l'information pour préparer l'accompagnement. Nous avons identifié deux cibles dont la maturité est insuffisante : les PME et certaines collectivités locales, vers lesquelles des efforts de communication doivent être réalisés. De son côté, l'industrie doit aussi fournir un travail pour mettre en place des solutions très lisibles et compréhensibles pour les cibles.

Si la mise en œuvre de Dora est plus concentrée sur la région parisienne, NIS 2 concernera l'ensemble du territoire français, ce qui nécessitera d'impliquer tous les acteurs. À ce titre, les campus cyber devraient être intégrés dans le dispositif. Les régions seront également intéressées, en raison de leurs compétences en matière de politique économique. Le « retour sur investissement » de NIS 2 doit ainsi concerner les territoires. En résumé, en compagnie de l'Anssi, nous devons travailler à une collaboration globale de tous les acteurs nationaux et régionaux en faveur du programme de sensibilisation et de communication, et ensuite de mesure de la politique industrielle.

M. Yoann Kassianides, délégué général de l'Alliance pour la confiance numérique. L'Osint constitue un enjeu majeur. Les attaquants se servent d'outils essentiellement fondés sur les vulnérabilités humaines. Dans ce cadre, l'Osint représente une réponse efficace et sa pratique est aujourd'hui extrêmement répandue. Néanmoins, l'ensemble des acteurs de ce domaine s'interrogent sur le cadre juridique applicable.

L'ACN mène depuis maintenant deux ans des travaux, en partenariat avec la chaire Cyber de l'Institut des hautes études de défense nationale (IHEDN) rassemblant de nombreux acteurs de la sphère étatique (pouvoirs judiciaires, services du ministère de l'intérieur), la Cnil, des entreprises, des avocats. Le constat est extrêmement clair : le droit actuel ne permet pas aujourd'hui d'appréhender correctement cette pratique de l'Osint.

En conséquence, il est extrêmement difficile de construire des modèles économiques, faute de clarification des zones d'ombre entre ce qui est autorisé et ce qui ne l'est pas. Nous proposons donc de créer un droit commun de l'Osint. À l'heure actuelle, le droit applicable est très morcelé et limité à certains domaines restreints, par exemple le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) ou l'administration fiscale.

Ce cadre préciserait notamment que la pratique de l'Osint est libre tout en étant contrebalancée par l'ensemble des libertés individuelles et publiques et par la protection des secrets. Il permettrait de donner des possibilités d'exercer l'Osint pour des motifs légitimes. L'objectif consiste à définir clairement dans quelles circonstances cette pratique est permise et de distinguer les cas où elle ne l'est pas. Ce cadre juridique aurait également pour but de modifier certains articles du code pénal, afin de simplifier leur interprétation et d'éviter des situations aberrantes.

La situation actuelle, marquée par une divergence entre l'esprit de la loi et sa lettre, conduit à des résultats contre-productifs. Quelques mesures extrêmement simples sur la création d'un droit commun de l'Osint permettraient de remédier à ces problèmes de manière assez claire. Par conséquent, nous souhaitons porter ce sujet au débat.

M. le président Philippe Latombe. Les collectivités nous ont parlé de la fin programmée des financements des centres d'alerte et de réaction aux attaques informatiques (CSIRT). Cet outil vous est-il utile ? Faudrait-il les pérenniser sous une forme ou sous une autre en termes de financement ou de statut ?

Ensuite, comment pourrions-nous modifier le statut des divulgations des vulnérabilités *zero-day* afin de résoudre les problèmes juridiques qu'elles posent aux acteurs qui les identifient et souhaitent en parler à la communauté pour accélérer les correctifs ? Avez-vous des avis sur ce sujet ?

Mme Dorothée Decrop, déléguée générale d'Hexatrust. Je me concentrerai sur l'aspect humain et l'accompagnement des acteurs concernés par les entités importantes, ainsi que sur la chaîne de sous-traitance. Nous collaborons avec la direction générale du travail (DGT) pour intégrer le risque cyber dans le document unique d'évaluation des risques et de prévention (Duerp), afin de sensibiliser les entreprises, à droit et coût constants. Il est crucial d'intégrer ces risques dans la gestion courante, en utilisant des outils existants pour sensibiliser les entreprises de manière homogène au niveau territorial.

L'accompagnement des entreprises est essentiel. Nombre d'entre elles ignorent si elles deviennent des entités importantes selon l'article 12. Un travail sur les codes NAF (nomenclature d'activités française) et NACE (nomenclature d'activités européennes) permettrait de clarifier la situation, offrant une meilleure lisibilité et l'identification rapide des entreprises concernées. Cela garantirait, sous la forme NACE, une interprétation uniforme des entités importantes au niveau européen et permettrait d'homogénéiser les entreprises qui seront cibles ou se saisiront de cette opportunité. Chez Hexatrust, nous sensibilisons les fédérations professionnelles soumises à NIS 2 par un module de sensibilisation de premier niveau. Nous établissons des partenariats pour utiliser l'« HexaDiag », notre démarche de cybersolidarité permettant un autodiagnostic rapide et autonome et des résultats immédiats. Dans un deuxième temps, les entreprises contactent des professionnels pour réaliser des démarches bien plus complètes.

Nous sommes membres du Campus cyber national, nous programmons des interventions et actions communes avec les campus régionaux, et nous sommes partenaires de l'association CoTer. Nous irons également sensibiliser les collectivités territoriales à ces enjeux, au même titre que d'autres associations.

Concernant la labellisation NIS 2, nous manquons encore de documentation précise. La cybersécurité doit rester agile et adaptable, accessible juridiquement, avec des directives claires et dynamiques pour éviter de créer des barrières à l'entrée pour certains professionnels. En résumé, il est difficile de se prononcer à ce stade.

M. Jean-Noël de Galzain. Concernant l'assurance, je pense que la cybersécurité devrait être considérée comme un risque, au même titre que d'autres types de risques. Elle devrait donc faire partie intégrante de l'obligation d'assurance en responsabilité civile des entreprises. Une entreprise qui respecte des normes telles que celles de Dora ou NIS 2 pourrait ainsi obtenir un accès facilité à l'assurance et une couverture en cas d'incident. En effet, comme l'a mentionné le directeur de l'Anssi, les attaques coûtent cher, nécessitent une réaction rapide et des compétences spécialisées pour rétablir la situation rapidement. L'assurance peut donc aider à gérer concrètement les problèmes lorsqu'ils surviennent.

M. Michel Dubois. Le constat est unanime depuis plusieurs années : la sensibilisation ne fonctionne pas ; c'est un échec. Il manque un chef de file. Dans ces conditions, il serait pertinent de mettre en avant cybermalveillance.gouv.fr, qui traite ce sujet. Ensuite, il faut un référentiel des démarches et des supports. L'Anssi a mis en place un « cyber dico » régulièrement mis à jour. Il serait utile de mettre en lumière cet outil pour disposer d'un référentiel unique des définitions en cybersécurité. Des labels ont été établis par l'Anssi pour les formations avec SecNumedu.

Il serait donc intéressant de valoriser ces labellisations dans la loi. Enfin, cybermalveillance.gouv.fr a développé plusieurs fiches thématiques de sensibilisation accessibles à tous. Le module de formation en ligne (Mooc) de l'Anssi constitue également un support disponible.

En réalité, il manque une obligation légale de sensibilisation et de formation. Il pourrait exister une disposition similaire à celle de la sécurité incendie, où l'employeur doit former ses employés au moins une fois par an. La notion du référent en cybersécurité dans l'entreprise pourrait porter cette responsabilité.

Enfin, un maillage local fondé sur les Campus cyber peut être officialisé. Par exemple, le Clusif dispose de représentations régionales en France qui peuvent relayer ces messages, garantissant ainsi un continuum entre un référentiel, un chef de file et des obligations légales.

M. Sébastien Garnault, fondateur de CyberTaskForce. Comment transmettre le message aux collectivités ? Je propose d'utiliser le salon des maires, moment important pour les collectivités, pour communiquer avec les communes. Cependant, elles expriment souvent des besoins financiers. Il faudrait donc accompagner davantage les petites collectivités et réallouer les budgets en conséquence.

Ensuite, les questions soulevées par Bénédicte Pilliet sont pertinentes et méritent des réponses précises. Concernant l'assurance, l'article 5 de la Lopmi avait initié une démarche, mais le problème porte surtout sur le modèle économique. Toutefois, il semble qu'il faille explorer comment des acteurs comme Stoïk réussissent à offrir une assurance cyber à l'échelle française et européenne.

Mme Anne-Elise Jolicard, responsable des affaires publiques d'Anozr Way. La loi de transposition était attendue, notamment en ce qui concerne l'appréhension des vulnérabilités. Nous saluons l'amendement du Sénat incluant le facteur humain parmi les vulnérabilités. Cependant, il est nécessaire d'aller plus loin pour atteindre les objectifs de la directive, en veillant à ce que les termes soient clairs et définis, en suivant l'exemple de nos voisins italiens, belges et allemands, qui ont défini l'approche « tous risques » à partir des considérants 78 et 79.

De fait, le besoin de pédagogie est patent. Il est communément admis que la faille essentielle est la faille humaine. Pour autant, les textes français n'insistent pas assez sur la menace induite sur les entreprises et l'ensemble des citoyens. La définition de ces termes est cruciale pour guider et expliquer le cadre de la cybersécurité. Cette clarification est nécessaire pour mieux appréhender les menaces dans le contexte français.

Le risque de surtransposition a été écarté par le Conseil d'État qui invite au contraire à définir les termes clés de la directive. L'article 14 pourrait ainsi mentionner la notion

d’approche « tous risques » et viser expressément les considérants 78 et 79. Enfin, la notion de cybermenace a aussi été définie par nos voisins. Elle figure dans la directive et pourrait être ajoutée au titre de l’article 6.

M. Philippe Luc. Concernant l’introduction d’une formation obligatoire, il est essentiel de noter que la cybersécurité intéresse principalement les professionnels. Les utilisateurs se concentrent sur l’utilisation des outils numériques sans se préoccuper de leur sécurité, de la même manière qu’ils utilisent leur voiture, sans se soucier du fonctionnement de leur airbag. Il est crucial de fournir des connaissances de base et des bonnes pratiques, surtout pour les jeunes. Pour les adultes, une approche plus légère pourrait éviter de les détourner du sujet. Les efforts actuels de cybermalveillance.gouv.fr sont louables et il faudrait proposer davantage d’outils de protection. Nos salariés sont souvent plus sensibles à se protéger personnellement dans leur vie privée qu’à protéger leur propre entité. En conséquence, ce sujet devrait être travaillé en compagnie de cybermalveillance.gouv.fr.

S’agissant des CSIRT, je ne dispose pas des qualifications pour discuter du sujet du financement. En revanche, il est important de disposer d’un maillage local pour établir des relations de confiance avec les PME. Les structures locales comme les CSIRT jouent un rôle clé en sensibilisant et en répondant aux questions des entreprises, compensant ainsi le manque d’intérêt des acteurs locaux pour les grandes institutions de cybersécurité.

Mme Garance Mathias. La sensibilisation est un aspect extrêmement important, évoqué notamment dans les propositions formulées en octobre 2024 par la commission supérieure du numérique et des postes, notamment les recommandations n° 1 et n° 2. Il s’agit ici d’inclure le grand public, c’est-à-dire tous les acteurs. Par exemple, en matière de sécurité incendie, ces pratiques sont devenues des réflexes bien ancrés alors qu’auparavant, elles n’étaient pas aussi bien prises en compte. Il est donc impératif que cela devienne, dès le début, un automatisme et que toute la population soit sensibilisée via des campagnes d’information. Je tiens également à saluer le travail effectué par cybermalveillance.gouv.fr, le 17Cyber, ainsi que les formations de l’Anssi, qui bénéficient au plus grand nombre. Au sein du Clusif, nos adhérents et salariés formés peuvent offrir des exemples pratiques qui permettent d’ancrer ces solutions grâce à des communications bénéfiques et des retours d’expérience constructifs relatifs au niveau de maturité.

Concernant les territoires d’outre-mer, il est crucial de prendre en compte leur niveau de maturité et leurs besoins spécifiques en rapport avec leur position géographique. Une approche adaptée selon les statuts de chaque territoire et assemblée territoriale, par exemple de Polynésie française, de Wallis-et-Futuna et de Saint-Pierre-et-Miquelon, est essentielle pour utiliser pleinement leur potentiel concernant la résilience opérationnelle.

Fort heureusement, nous avons parmi nos plus de 1 300 adhérents des utilisateurs et des offreurs résidant dans ces territoires. Leur contribution permet de renforcer ce dialogue. La loi, générale et absolue, peut constituer une aide pour impulser ce mouvement déjà initié par cybermalveillance.gouv.fr, l’Anssi et d’autres autorités. Enfin, des définitions claires permettraient une compréhension précise, nécessaire pour se positionner judicieusement.

M. Arnaud Martin. Pour compléter certains propos, je souhaite revenir sur le délai pressenti de trois ans. Dans le cadre de Dora, toutes les banques et assurances sont conformes depuis le 17 janvier 2025. Deux aspects nécessitent du temps : d’une part, les audits et tests, y compris ceux avec des tiers, et, d’autre part, la gestion des clauses contractuelles, dont l’absorption totale par les partenaires pourrait prendre environ trois ans. À titre d’exemple, le

régulateur nous a bien indiqué que les premiers tests de pénétration fondés sur la menace (TLTP) ne seront pas diligentés en 2025, mais plutôt début 2026-2027.

Concernant la déclaration des incidents, il est essentiel que les entreprises se fondent sur des critères factuels pour déterminer leur obligation de déclaration. Ces aspects sont plus structurés sur la partie financière, en termes de nombre de critères impactants. Le principe de proportionnalité est également essentiel. La première déclaration sous quatre heures, qui se substitue d'ailleurs à la directive sur les services de paiement (DSP2), n'oblige qu'à transmettre les informations disponibles à ce moment-là, avant de les enrichir au fur et à mesure.

En matière assurantielle, les rapports annuels de l'Association pour le management des risques et des assurances de l'entreprise (Amrae) montrent une stabilisation par comparaison avec les années 2020-2021. Les assureurs sont désormais prêts à assurer et les conditions de souscription d'assurance se sont améliorées. Cela incite à ne pas réguler un marché en cours de stabilisation sur le haut du marché, augmentant l'appétence des assureurs pour se positionner sur des segments moins matures.

À l'heure actuelle, aucun actuaire ne dispose d'un modèle prédéfini pour évaluer précisément la pérennité de ce marché. Cela ressort d'ailleurs du dernier rapport de l'Amrae, dont la publication est imminente. Cependant, nous observons que ce marché suscite un certain intérêt. En résumé, une régulation excessive dans un domaine en cours d'autorégulation ne constitue sans doute pas la meilleure approche, actuellement.

Enfin, concernant l'acculturation au risque lié à l'impact d'une interruption d'activité, il est crucial que tous les collaborateurs soient sensibilisés, mais une attention particulière doit être portée à la formation des conseils d'administration et des comités exécutifs, conformément aux directives de Dora.

Mme Mylène Jarossay. Monsieur Martin vient de mentionner l'importance pour les dirigeants d'être informés annuellement de l'évolution des menaces cybernétiques. Cette mise à jour n'apparaît pas comme une exigence excessive.

Le facteur humain reste un défi majeur, car malgré les efforts de sensibilisation, l'erreur humaine demeure une vulnérabilité. Le défenseur doit maintenir mille portes fermées, quand il suffit à l'attaquant d'en trouver une seule ouverte. En outre, les scénarios d'ingénierie sociale sont assez redoutables ; ils sont en outre augmentés par de l'IA. Il est essentiel de mettre en place des processus et des solutions techniques pour minimiser les risques engendrés par les erreurs humaines, notamment en distinguant les responsabilités des utilisateurs et des administrateurs des systèmes d'information. L'Anssi souligne le volet administration dans son référentiel de mesures, ce qui est judicieux. Il faut concentrer l'attention sur les informaticiens et trouver des subterfuges techniques de process, pour empêcher qu'un seul humain ne mette à terre une entreprise.

M. Daniel Le Coguic. Concernant la réglementation, il est important de distinguer ce qui relève du décret ou de la loi. Par exemple, le dernier décret pour l'application la loi de programmation militaire (LPM) de 2013 a été publié en 2024, soit onze ans plus tard.

Ensuite, dans une première version du projet de gouvernement, les missions de l'Anssi étaient précisées. Aujourd'hui, elles sont renvoyées à un décret en Conseil d'État. Il est crucial de définir clairement les missions de l'Anssi dans les textes législatifs, plutôt que

de laisser certains aspects à des décrets en Conseil d'État. Il serait bénéfique également de privilégier dans le texte l'accompagnement plutôt que le contrôle strict. Enfin, la question des audits réguliers par des organismes indépendants pourrait être précisée dans la loi.

En conclusion, s'il revient au législateur de définir ce qui relève de la loi et ce qui peut être renvoyé à un règlement, il faudra éviter un certain nombre de pièges.

Mme Bénédicte Pilliet. En matière de sensibilisation, de nombreuses ressources sont produites par l'État, par cybermalveillance.gouv.fr. En revanche, elles demeurent méconnues de nombreuses collectivités. Il existe donc un enjeu d'amélioration de la lisibilité et de l'accessibilité des ressources produites par les différentes administrations auprès des acteurs, afin qu'ils puissent se les approprier.

Mais plus que sensibiliser, il nous faut convaincre les élus et les chefs d'entreprise que la cybersécurité n'est pas qu'un sujet technique, à part. Aujourd'hui, le numérique est présent dans l'ensemble de nos métiers, il est le facteur de développement majeur de nos organisations, il est utilisé pour créer de nouveaux usages au service des citoyens par les collectivités. Dès lors, la cybersécurité doit être envisagée comme un facteur de confiance, de pérennité des projets développés, d'attractivité, de développement ; mais aussi un facteur politique pour les élus. Pour s'en convaincre il n'y a qu'à observer les conséquences d'une cyberattaque réussie sur une collectivité, qui peut l'empêcher de conduire ses missions.

La sécurité du numérique constitue bien un sujet de gouvernance, d'organisation, de formation, de sensibilisation, de droit et de conformité. Mais avant tout, il s'agit d'un sujet de développement pour les entreprises et pour les collectivités. Afin de faire réfléchir les acteurs aux conséquences d'une attaque cyber sur leur organisation, nous avons organisé à Lyon un exercice de gestion de crise d'origine cyber, mais sans spécialistes cyber. À travers cet exercice, les élus ont pris conscience que ce sujet qu'ils voyaient réservé aux spécialistes était en réalité au cœur de la continuité de leurs missions.

À ce propos, le salon des maires offre effectivement une opportunité pour l'acculturation, mais le travail au quotidien est essentiel. Nous le menons sur les territoires, avec les associations des maires. L'enjeu consiste bien à enclencher une dynamique, à trouver un « sponsor », quelqu'un qui soit convaincu. C'est un travail de longue haleine, de proximité, continu, parfois un peu décourageant, mais toujours nécessaire.

M. Éric Bothorel, rapporteur général. Pourriez-vous revenir sur la simplification qui pourrait être apportée à une notification d'incident ? Vous avez formulé un certain nombre de propositions, mais pourrait-on envisager une plateforme commune dans laquelle vous retrouveriez, un plus petit dénominateur commun ?

Ensuite, j'ai le sentiment que l'ensemble des acteurs sont désormais conscients que ce genre d'attaques n'arrivent pas qu'aux autres, que chacun d'entre eux peut en subir.

Mme Mylène Jarossay. En synthèse, nous attendons une clarification sur la situation des entreprises françaises, leur éligibilité et une simplification des notifications d'incidents. Par ailleurs, une entreprise qui est victime d'une cyberattaque est déjà fortement impactée ; elle ne devrait pas subir la double peine de la sanction. Il importe de bien réfléchir à cette question, la sanction doit servir à réparer et encourager une amélioration continue.

M. Arnaud Martin. Concernant la plateforme commune, nous soutenons l'idée de regrouper les propositions existantes. Nous avons déjà travaillé sur ce sujet avec certains de nos collègues, notamment le Clusif. Des graines ont déjà été semées ; nous sommes favorables à cette initiative.

M. Daniel Le Coguic. Deux aspects sont essentiels aux yeux de l'ACN : la collaboration entre acteurs nationaux, régionaux et publics ; et l'organisation de cette collaboration pour renforcer notre autonomie. La collaboration est ainsi essentielle, pour permettre à chacun de trouver sa place. C'est en établissant cette « équipe de France » du cyber que nous atteindrons les objectifs que la loi se donne en matière de résilience de la nation.

Ensuite, si nous ne maîtrisons pas les technologies de cybersécurité dans le numérique de demain, nous serons dépendants et notre résilience sera à géométrie variable. Si les solutions proviennent de France et de l'Union européenne, nous aurons accompli un pas de géant. Naturellement, nous n'atteindrons pas 70 % de parts de marché dans ce domaine, mais si nous parvenons à croître, tout le monde en sortira vainqueur ; les entreprises, le gouvernement, les régions.

Mme Bénédicte Pilliet. Au CyberCercle, nous estimons qu'en matière de cybersécurité, de sécurité numérique, rien ne peut être réalisé seuls. Ensemble, nous allons plus loin et plus vite ; nous avons besoin de collaborer. Les ressources existent en France, mais il est nécessaire de disposer d'objectifs communs et d'une organisation claire, pour offrir aux acteurs concernés par NIS 2 la lisibilité et la cohérence indispensables pour passer à l'action. Cela inclut la prise en compte des besoins et de la montée en compétence des acteurs régionaux et de leurs prestataires informatiques, qui les accompagnent au quotidien, dans le déploiement de NIS 2.

À ce titre, les référentiels et les labels nécessiteraient sans doute de mettre en place une réunion de concertation, qui permette d'inclure tous les acteurs dans une stratégie commune.

M. Jean-Noël de Galzain. De nombreuses initiatives existent déjà, mais il est crucial de poser un cadre général et de s'aligner sur une même direction, la transposition tenant lieu d'une forme de boussole, dans une approche systémique. Une fois le texte transposé, il est prévu de réécrire une stratégie nationale de cybersécurité, qui pourrait utilement intervenir dans le cadre du comité de filière, où nous convions tous les acteurs à participer. Nous aurons à cœur d'aligner la stratégie nationale de cybersécurité, afin de réussir ce passage vers la résilience générale. Il nous semble effectivement essentiel de réunir une « équipe de France » et d'y associer tous les acteurs de l'écosystème, dont le président du Campus cyber, le directeur général de l'Anssi, les représentants de cybermalveillance.gouv.fr.

Je confirme par ailleurs que le sujet de la cybersécurité intéresse désormais tout le monde. J'observe en outre que les jeunes générations sont particulièrement sensibles au sujet de la protection des données. Je compte vraiment sur la représentation nationale pour garder en tête que la souveraineté doit être associée à toutes nos démarches dans le numérique ; il en va de notre autonomie stratégique.

Enfin, une collaboration entre public et privé est incontournable si nous voulons établir un modèle économique durable ; l'État ne peut pas tout faire seul. L'industrie prendra sa part, de manière coordonnée avec les autres parties prenantes. Nous produirons des efforts,

comme nous le faisons tous les jours pour rendre la cybersécurité plus accessible et le numérique plus agréable à utiliser et plus sécurisé, à long terme.

M. Michel Dubois. Tout d'abord, je distingue deux niveaux de notification. Je ne pense pas qu'il soit nécessaire de légiférer sur le sujet des indicateurs de compromission (IOC), car des structures comme InterCERT en France permettent déjà aux CSIRT de partager ces informations. Le deuxième point concerne la notification vis-à-vis du régulateur. Je tiens à souligner l'importance d'avoir suffisamment de temps pour effectuer cette notification. Dans notre groupe, nous consacrons beaucoup de temps à vérifier les revendications de vol de données, car les pirates informatiques cherchent souvent à se vanter en réutilisant des données anciennes ou non pertinentes. Ce processus d'investigation est long et ne peut être accompli en seulement vingt-quatre heures. Enfin, j'insiste sur la nécessité d'harmoniser la procédure de notification, idéalement à travers une plateforme unique, par exemple portée par l'Anssi, qui diffuserait ensuite les informations aux différentes autorités compétentes, comme l'ACPR ou la Cnil.

En ce qui concerne les sanctions, il est crucial que tous les acteurs soient soumis au même régime. Plutôt qu'une simple sanction financière, pourquoi ne pas imposer l'achat de produits et de services de cybersécurité afin de se mettre aux normes ? Cela permettrait de rendre les sanctions à la fois plus constructives et cohérentes au niveau européen. En conclusion, je préconise un cadre législatif pragmatique et cohérent.

Mme Garance Mathias. Les labels peuvent offrir valorisation, attractivité et confiance. Le label, en tant qu'instrument juridique, doit avant tout inspirer confiance. Lors de l'élaboration du RGPD, cette notion n'avait pas été abordée, mais elle mérite d'être explorée aujourd'hui. Il est essentiel de considérer l'attractivité économique que peut générer la confiance. Au sein du Clusif, nous encourageons les échanges d'idées et le retour d'expérience des différents acteurs pour s'assurer que la loi s'aligne avec la réalité du terrain.

M. Sébastien Garnault. Je tiens d'abord à répondre à la demande de simplification administrative émise par M. le rapporteur général. Nos idées sont déjà sur la table, nous n'aurons donc pas besoin de soumettre un nouveau document. Concernant la stratégie nationale, il est crucial de définir clairement nos objectifs. La responsabilité politique et la continuité de l'engagement sont essentielles. Il est également important que les décrets d'application soient bien définis et que la vision ministérielle soit cohérente et continue.

M. le président Philippe Latombe. Je vous remercie pour vos interventions. Nous ne savons pas encore quand ce texte sera étudié dans l'hémicycle, probablement en septembre. Dans l'intervalle, n'hésitez pas à faire parvenir des contributions écrites à nos rapporteurs, afin que nous puissions les intégrer dans notre réflexion, éliminer des zones d'ombre, éviter les effets de bord et produire un texte le plus clair possible.

La séance est levée à 11 heures 35

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 jeudi 5 juin 2025 à 9 h 30

Présents. - M. Éric Bothorel, M. Mickaël Bouloux, M. Philippe Latombe, Mme Anne Le Hénanff

Assistait également à la réunion. - Mme Sylvie Josserand