ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
13 mai 2026
Séance de 11 heures

Compte rendu n° 67

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

Présidence de Mme Sabine Thillaye, *Vice-présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures dix.

Mme Sabine Thillaye, présidente. Mes chers collègues, je vous prie tout d'abord de bien vouloir excuser le président Jean-Michel Jacques, retenu par un engagement impondérable lié à sa fonction, qui m'a chargée de présider cette audition. Dans le cadre de notre nouveau cycle « Guerre hybride et continuum de conflictualités », nous avons le plaisir d'accueillir M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information, plus brièvement (Anssi). Cette agence, parfois surnommée le « cyber pompier de la France », a été créée en 2009 sous l'autorité du secrétariat général de la défense et de la sécurité nationale (SGDSN), pour développer notre cyber résilience.

L'Anssi figure au cœur de la gouvernance de la cyberdéfense. Détecter et répondre aux cyberattaques, sécuriser les activités d'importance vitale de l'État, contribuer au quotidien à la stabilité du cyberespace, telles sont les missions, monsieur le directeur général, que vous menez chaque jour. Vous le dites depuis des années : la France doit se préparer à un scénario d'attaque informatique toujours plus massif.

La menace évolue constamment ; elle provient à la fois d'États étrangers et d'acteurs du crime organisé, agissant à des fins lucratives. Elle compromet la continuité des services publics essentiels et, surtout, met en péril nos entreprises. Vous nous qualifierez la réalité et l'importance de cette menace, vous nous direz quels sont vos moyens d'action, comment vous préparez notre pays et ses acteurs à être à la hauteur des cyberattaques.

Que pouvons-nous faire ? En premier lieu, il faudrait enfin transposer la directive NIS 2 en droit national. Elle représente une opportunité unique : sa mise en application permettra à des milliers d'entités appartenant à dix-huit secteurs de mieux se protéger. J'espère que nous y parviendrons avant l'été.

Quel est votre regard sur ce retard ? Quels sont les défis induits par la directive pour l'Anssi ? Par ailleurs, l'Anssi a aussi renforcé ses partenariats public-privé depuis des années, tout en assurant un maillage sur le territoire avec ses centres de réponse aux incidents de sécurité informatique (CSIRT) déployés dans les régions. Cette trajectoire opérationnelle dans les territoires permet-elle de passer à l'échelle ?

Une stratégie nationale de cybersécurité 2026-2030 a été dévoilée en janvier dernier, dans le prolongement de la revue nationale stratégique (RNS). Quels en sont les principaux axes ?

Enfin, le Premier ministre a annoncé le 30 avril dernier une série de mesures de lutte contre la menace cyber pesant sur les infrastructures de l'État. Il a notamment annoncé la création d'une Autorité nationale du numérique et de l'intelligence artificielle placée sous son autorité et chargée d'imposer des règles de sécurité à l'ensemble des ministères. L'Anssi est-elle concernée par ces restructurations ? Pourriez-vous nous expliquer ce qui en est attendu ? Comment chacun d'entre nous, parlementaires, peut-il agir ?

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information. Je suis particulièrement honoré de m'exprimer à nouveau devant vous sur ce sujet du *continuum* de menaces pesant sur nos intérêts les plus fondamentaux, dont je m'attacherai à détailler le volet cyber.

Dans ce propos liminaire, je souhaite d'abord revenir sur la menace telle que nous la percevons aujourd'hui dans ses évolutions récentes. Nous nous y préparons, car la situation est d'ores et déjà grave, mais elle est surtout susceptible de se dégrader sensiblement. Enfin, j'aborderai la manière dont nous nous préparons à ce contexte, qui constitue sans doute le point le plus déterminant.

Pour caractériser la menace, j'ai coutume de m'appuyer sur un triptyque fondé sur la nature des attaquants. Ceux qui portent atteinte à nos systèmes d'information, qu'il s'agisse de ceux de l'État, des entreprises, des collectivités ou des particuliers, relèvent de trois catégories principales. Il y a tout d'abord les États, qui mènent des opérations d'espionnage depuis l'origine du numérique. Cette réalité n'est pas nouvelle, même si son intensité s'est accrue. Viennent ensuite les acteurs du registre criminel, qu'ils soient structurés ou non, motivés par une finalité lucrative. Ces acteurs ont considérablement évolué au tournant des années 2020, adoptant une organisation quasi industrielle qui fait que, désormais, la menace n'épargne plus personne. Enfin, il faut mentionner les acteurs « hacktivistes », beaucoup plus protéiformes, qui recherchent avant tout des effets de réputation, des coups d'éclat ou des effets de sidération.

Ces trois catégories coexistent et se superposent. Elles demeurent identifiables, même si leurs frontières tendent à s'estomper. On observe en effet des mutualisations d'outils, des circulations de compétences et des collaborations ponctuelles entre acteurs criminels et étatiques. La conjonction de ces trois types d'acteurs explique le niveau de menace particulièrement élevé. Comme je le rappelle souvent, chacun peut en être victime, même sans être directement visé.

Toutefois, ce phénomène ne témoigne pas d'une explosion récente du risque, mais plutôt d'un plateau haut. Les données issues de l'Anssi, bien qu'elles comportent des biais de sélection, montrent un niveau d'incidents stable entre 2024 et 2025, avec environ 1 360 incidents traités par an. L'année 2024, marquée notamment par les Jeux olympiques, constituait déjà un niveau record.

Concrètement, les équipes de l'Anssi, mobilisées en permanence, traitent quotidiennement une dizaine de signalements, dont environ quatre sont confirmés comme des incidents et nécessitent une intervention approfondie. Ces interventions peuvent être lourdes et prolongées ou, selon les cas, faire l'objet d'un traitement plus léger, éventuellement confié à des acteurs du secteur privé, sous supervision.

Afin de mieux caractériser la menace, il importe de distinguer les éléments nouveaux, les constantes et les éléments moins visibles préoccupants. Les vols de données apparaissent aujourd'hui comme la forme la plus visible de cette menace. Sans être totalement nouveaux, ils connaissent une augmentation très significative, de l'ordre de 50 % entre 2024 et 2025, et s'accompagnent d'incidents marquants tant par leur ampleur que par la nature des cibles.

Cette évolution s'explique en partie par un changement de stratégie des acteurs criminels. Ceux-ci privilégient désormais les vols de données, parfois en substitution des attaques par rançongiciel, car ces opérations sont plus simples à mener et plus complexes à contrer. Elles restent rentables, d'où leur persistance. On observe également l'émergence

d’acteurs isolés ou « loups solitaires », y compris très jeunes, qui agissent seuls ou en petits groupes, motivés à la fois par l’appât du gain et par la recherche de reconnaissance.

Ces dynamiques s’inscrivent aussi dans un contexte de recomposition de l’écosystème criminel, liée notamment aux opérations judiciaires ayant conduit à des arrestations. Les vols de données produisent des effets particulièrement préoccupants et inacceptables, touchant directement les individus dans leur intimité, notamment lorsque sont en cause des données de santé ou des informations bancaires. Ces atteintes, si elles ne relèvent pas directement de la sécurité nationale au sens strict, n’en demeurent pas moins graves.

Elles mettent en lumière des vulnérabilités souvent basiques, récurrentes, observées tant dans le secteur public que dans le secteur privé. Ces failles ne sont pas propres à la France ; elles sont universelles et exploitées depuis des années par les attaquants. Toutefois, l’asymétrie inhérente à ces attaques suscite une inquiétude particulière.

La cybersécurité repose par nature sur une asymétrie : il est toujours plus difficile et plus coûteux de défendre, d’analyser et de corriger que d’attaquer. Cette asymétrie est encore accentuée dans le cas des vols de données. Ces attaques se prêtent en outre au bluff, les attaquants pouvant prétendre détenir des données sans que cela puisse être immédiatement vérifié. Cette incertitude constitue en elle-même un levier de pression particulièrement efficace, renforçant encore la complexité de la réponse à apporter.

Globalement, parmi les cas traités par l’ANSSI en 2025, 60 % des attaques relevaient du bluff ; elles ont toutefois engendré une surcharge de travail, chaque revendication nécessitant une vérification. Elles entraînent un effet d’érosion des capacités de cyberdéfense de l’Anssi, des équipes ministérielles, des entreprises et de leurs partenaires privés, mobilisés en continu depuis plusieurs mois. Qu’il s’agisse d’invalider une revendication ou d’analyser une attaque avérée, l’effort requis reste le même. Dans ce dernier cas, la tâche est d’autant plus délicate que les données volées sont irrécupérables : il faut alors comprendre les faits et éviter qu’ils ne se reproduisent. Cette dynamique engendre une fatigue réelle à l’échelle de tout l’écosystème.

De plus, ces attaques entraînent une érosion de la confiance générale tout aussi préoccupante. Celle-ci conduit à douter de nos capacités, de nos institutions et parfois à intégrer les éléments de langage des attaquants eux-mêmes. Ces derniers sont très actifs en matière de communication. Ils interviennent le plus souvent en premier à la suite d’une attaque et parviennent ainsi à imposer, dans les phases initiales, leur propre cadre narratif. Il en découle un déséquilibre informationnel susceptible d’altérer la perception collective.

Ce phénomène s’inscrit dans un *continuum* plus large. Les attaques de ce type ne représentent qu’environ 15 % de ce que traite l’Anssi. Elles constituent la partie visible de l’iceberg. Le reste comprend des menaces plus anciennes toujours présentes, à l’instar des rançongiciels, dont la fréquence a légèrement diminué, mais qui continuent d’affecter les collectivités et les entreprises. Des exemples récents montrent qu’ils peuvent encore paralyser des infrastructures locales.

Il existe également des actes de sabotage visant des installations de petite taille, comme des éoliennes ou des micro-barrages. Ces actions, souvent menées par des acteurs hacktivistes, notamment pro-russes, n’ont pas entraîné de conséquences majeures, mais elles

témoignent d'une désinhibition croissante. L'intention est manifeste et doit, à ce titre, être prise en considération.

Enfin, il existe des menaces plus discrètes, mais potentiellement plus graves, qui correspondent aux actions menées par des États. L'espionnage constitue une réalité quotidienne, affectant des administrations sensibles, nos réseaux diplomatiques, des entreprises stratégiques, notre base industrielle et technologique de défense (BITD) ou des opérateurs de télécommunications. Ces attaques mobilisent des moyens importants sur le long terme et peuvent nécessiter des équipes entières pendant plusieurs mois. La plus grande mobilisation a ainsi concerné 2 500 jours personne, soit une équipe de vingt personnes intervenant à temps plein pendant six mois.

Le point de vigilance majeur réside dans la possible évolution de ces actions d'espionnage vers des formes de sabotage. De fait, la différence entre espionnage et sabotage ne tient pas à la technique, mais à l'intention. Les capacités nécessaires sont identiques. Dès lors qu'un acteur est en mesure d'infiltrer un système, il peut, en théorie, en perturber le fonctionnement.

Des exemples récents à l'étranger montrent que ces scénarios ne sont pas théoriques. Ainsi, la Pologne a rendu compte d'une attaque contre son réseau électrique le 29 décembre, qu'elle a attribuée à la Russie. Cette attaque visait de manière synchronisée une trentaine de points d'interconnexion du réseau électrique avec des énergies renouvelables, une centrale thermique. Plus récemment, le même pays a fait état d'une attaque contre ses installations de production et de distribution d'eau potable.

Ces événements doivent nous alerter, d'autant plus que certaines dynamiques pourraient traduire un pré-positionnement stratégique d'acteurs étatiques sur nos infrastructures critiques, susceptible de déboucher sur des actions de sabotage. Ils doivent nous conduire à anticiper et à renforcer nos dispositifs. La situation actuelle est déjà préoccupante, mais elle pourrait s'aggraver pour plusieurs raisons.

La première tient à l'intelligence artificielle (IA). Celle-ci n'introduit pas une rupture totale, mais accélère des tendances déjà à l'œuvre. Elle facilite la découverte et l'exploitation de vulnérabilités, ce qui accroît le volume et la rapidité des attaques. On peut donc s'attendre à une augmentation significative des incidents dans les années à venir.

L'intelligence artificielle peut également constituer un facteur de vulnérabilité en tant que tel. Lorsqu'on la déploie à grande échelle, de manière très accélérée, il faut garder à l'esprit que nous ne disposons pas aujourd'hui des mêmes garanties de sécurité que pour un logiciel classique. Il existe donc un risque réel de créer, par une diffusion massive et homogène de modèles, une forme de monoculture susceptible d'engendrer des vulnérabilités systémiques ou structurelles dans le numérique, lesquelles pourraient se manifester plus tard de manière critique.

La seconde raison qui nous conduit à anticiper une aggravation de la situation réside dans le scénario central de la revue nationale stratégique de 2025. Ce scénario prévoit une mobilisation coordonnée de l'ensemble des composantes de la menace. Il inclut des services étatiques concentrés sur les infrastructures les plus critiques et les attaques les plus sophistiquées, mais aussi une partie de l'écosystème cybercriminel susceptible de mener des actions de paralysie ciblant des hôpitaux, des collectivités ou d'autres infrastructures

essentielles au fonctionnement quotidien de la nation. À cela s'ajoute un ensemble d'acteurs plus diffus, qui viendraient amplifier le phénomène et saturer les capacités de réponse.

Ce scénario correspond à une forme d'attaque coordonnée, pouvant se traduire par une montée en puissance rapide, avec un effet d'embolie et de déstabilisation généralisée. Nous nous y préparons à travers la RNS, pierre fondatrice de ce travail de préparation, à travers sa déclinaison dans la stratégie nationale de cybersécurité, qui priorise nos actions, à travers cet objectif de résilience cyber de premier rang.

Toutefois, un constat s'impose : l'État ne peut pas, à lui seul, faire face à une telle situation. La réponse doit être collective, articulée autour d'une mobilisation de l'ensemble des acteurs. Cela implique le développement de capacités de cyberdéfense complémentaires et distribuées, notamment à travers les réseaux CSIRT, les acteurs régionaux, sectoriels ou ministériels, mais aussi les partenaires privés. Je pense notamment au 17 Cyber, ainsi qu'au travail remarquable du groupement d'intérêt public Action contre la cybermalveillance (GIP Acyma).

Cette organisation vise à éviter les points de défaillance uniques et à faciliter une priorisation efficace des actions. Elle concentre les efforts sur les incidents les plus graves, tout en assurant une prise en charge globale. Elle conforte un modèle français de cybersécurité qui a démontré son efficacité en séparant clairement les fonctions offensives et défensives, tout en assurant leur coordination. Elle réaffirme notre volonté d'imposer un coût aux attaquants. Ce dispositif repose sur un modèle de gouvernance éprouvé, incarné par le C4, qui réunit, sous l'autorité du SGDSN, l'Anssi, la direction générale de la sécurité extérieure (DGSE), la direction générale de la sécurité intérieure (DGSI), le commandement de la cyberdéfense (Comcyber) du ministère des Armées, la direction générale de l'armement (DGA) et le Quai d'Orsay dans sa dimension stratégique.

Cette enceinte constitue le cadre approprié pour assurer la coordination, la mise en commun des expertises et la confrontation des analyses. Les coopérations se sont également renforcées avec le volet judiciaire, permettant des résultats significatifs. L'action conjointe des services de police, de gendarmerie et du parquet, notamment sa section J3, mérite d'être soulignée. Par ailleurs, la coordination s'étend à la lutte contre la manipulation de l'information. Sous l'égide du SGDSN, l'Anssi et Viginum agissent ainsi de manière complémentaire face à des attaques hybrides.

Néanmoins, le cœur de la stratégie demeure la prévention, la protection et la résilience, en premier lieu la sécurisation des systèmes de l'État. C'est l'objet de la feuille de route validée par le premier ministre, ainsi que de la réforme du pilotage du numérique de l'État, destinée à répondre à la complexité et à l'hétérogénéité des systèmes d'information publics, condition indispensable à une cybersécurité solide. Cette réforme visera notamment à renforcer l'action de la direction interministérielle du numérique (Dinum), lui donner des leviers d'action et un périmètre de mission renforcé, afin d'établir un numérique plus solide, base d'un travail de cybersécurité.

L'accent mis sur la prévention excède largement le seul périmètre de l'État. Il s'inscrit dans une logique d'ensemble qui vise à généraliser les bonnes pratiques à l'échelle de la société. Leur diffusion passe tout d'abord par le droit, à travers la directive NIS 2, qu'il nous faudra transposer dans les meilleurs délais en droit national, car elle constitue un levier

structurant. Cette logique se prolonge par le règlement européen sur la cyber-résilience, qui constitue un second pilier essentiel, en imposant des responsabilités accrues aux fournisseurs du numérique, notamment aux éditeurs de logiciels. Ces acteurs doivent désormais intégrer pleinement les exigences de sécurité dans leurs produits et leurs processus.

Au-delà du seul cadre normatif, notre ambition nécessite également un accompagnement adapté. Il s'agit de construire une logique économique cohérente autour de ces exigences de sécurité, afin qu'elles soient soutenables et effectivement mises en œuvre. La prévention passe aussi par l'entraînement et la préparation à la gestion de crise. À cet égard, l'exercice de crise REMPAR25 conduit en septembre 2025 constitue une illustration particulièrement significative. Il s'agissait d'un exercice massif, sans précédent à ma connaissance, qui a permis d'entraîner simultanément près de 1 300 entités de toutes natures, publiques et privées, grandes et petites, à des scénarios de gestion de crise cyber. L'effet en a été remarquable, et il importe désormais de généraliser ce type d'initiatives, au-delà de la seule impulsion de l'Anssi.

À cette dynamique s'ajoutent des enjeux de compétences qui sont absolument essentiels. Ils concernent à la fois la formation de spécialistes et la sensibilisation des non-spécialistes. La création d'un portail national grand public, prévue dans le cadre de la stratégie nationale, répond précisément à cet objectif. Ce portail mobilisera notamment le GIP Acyma et contribuera à diffuser une culture de cybersécurité accessible au plus grand nombre. Parallèlement, un travail est engagé avec l'éducation nationale afin d'introduire davantage ces thématiques au collège et au lycée. Il s'agit de former les citoyens de demain à ces enjeux numériques et de développer une forme de résilience collective face à des menaces encore trop mal comprises.

Je souhaite également insister sur un enjeu fondamental, réaffirmé dans la stratégie, celui de la maîtrise des technologies et de nos dépendances numériques. Comme j'ai déjà eu l'occasion de l'exposer, le numérique qui irrigue aujourd'hui notre quotidien s'est construit dans un contexte historique particulier, celui des « dividendes de la paix ». Nous atteignons désormais un moment où il est nécessaire de prendre du recul sur cet héritage. Certains choix ont pu être biaisés, certaines trajectoires ont été prises sans pleine conscience de leurs implications, et nous ne disposons pas toujours d'une vision claire de nos dépendances.

Aujourd'hui, nous sommes confrontés à une difficulté majeure : nous ne savons pas toujours précisément de quoi est constitué notre numérique, ni comment se structurent nos chaînes de dépendance. Cette opacité complique l'anticipation des ruptures et des évolutions. Elle impose un travail approfondi, notamment dans des domaines émergents comme l'intelligence artificielle ou l'ordinateur quantique. Il est impératif de se préparer dès à présent à ces transformations, car les urgences immédiates ne doivent pas occulter des enjeux de fond susceptibles de limiter nos marges de manœuvre dans les années à venir. Il nous faut donc agir simultanément sur ces deux plans.

Dans ce contexte, se pose également la question des risques d'ingérence étrangère. Ces risques ne sont pas uniquement d'ordre technique et ne peuvent se réduire à des réponses purement techniques. Ils sont également liés à la provenance des technologies, même s'il convient de se garder d'une approche simpliste ou binaire. À cet égard, la France se distingue en Europe par certaines initiatives, notamment dans le domaine du cloud et des réseaux 5G,

où des dispositifs spécifiques, comme le cadre SecNumCloud, ont été mis en place. Toutefois, ces efforts gagneraient à être portés à l'échelle européenne, car le marché intérieur constitue l'échelon pertinent pour traiter ces questions de manière efficace.

Cette démarche suppose un effort de conviction important et appelle à éviter certains écueils. Il ne s'agit pas de céder à des logiques d'exclusion systématique de certains fournisseurs, ni de poursuivre une illusion d'autarcie numérique, qui serait à la fois irréaliste et contre-productive. L'enjeu est de trouver un équilibre, pour renforcer notre capacité d'action collective au niveau européen, tout en préservant les prérogatives de souveraineté qui relèvent du niveau national. Ce fil directeur guide l'ensemble de nos travaux, et il continuera de le faire dans les débats à venir, notamment dans le cadre des évolutions du Cybersecurity Act.

Mme Sabine Thillaye, présidente. Je vous remercie pour ces propos introductifs particulièrement lucides. À certains moments, nous constatons un déficit de réactivité. Si des structures ont effectivement été instaurées, leur périmètre d'action ainsi que leurs responsabilités demeurent insuffisamment définis. Il apparaît dès lors nécessaire d'améliorer la lisibilité du dispositif, tant à l'échelle nationale qu'européenne. En effet, des actions peuvent être conduites de manière coordonnée, tout en préservant une souveraineté partagée entre les acteurs, dans la mesure où les menaces — notamment les ingérences — présentent un caractère commun. Comment rendre cet écosystème plus lisible, et permettre aux citoyens d'agir au lieu de subir ?

Mme Florence Goulet (RN). Nous avons bien compris que la menace est devenue multiforme, que la conflictualité s'exerce aujourd'hui sur l'ensemble de notre vie économique, politique et sociale, et surtout qu'elle est devenue permanente. La nouveauté repose sur l'émergence d'acteurs technologiques capables d'agir hors du champ étatique, soit à bas coût par l'influence, notamment via les réseaux sociaux, soit parce qu'ils ont des moyens financiers très supérieurs à ceux de l'État, comme les grandes entreprises technologiques américaines ou chinoises.

L'objectif stratégique numéro 9 de la RNS, complété par la Stratégie nationale de cybersécurité 2026-2030, organise une montée en puissance des capacités de l'État pour répondre à la menace. L'Anssi figure au cœur de cette réponse, mais relève d'une logique centrée sur l'action des administrations. Or, la guerre hybride exige également une réponse sociétale.

Le ciblage de l'arrière n'est pas une stratégie nouvelle. Lors des deux guerres mondiales et pendant la guerre froide, l'adversaire cherchait déjà à ébranler la cohésion nationale pour réduire tout désir de résistance ou de combat. Mais l'hyperconnexion généralisée a ouvert la possibilité d'un contrôle direct des populations. Pour contrer cette vulnérabilité majeure, les pays baltes et la Scandinavie s'appuient sur le renforcement de la cohésion nationale et de l'esprit de défense, que le chef d'état-major de l'armée de terre nomme « les profondeurs de la nation ».

Le bilan 2025 de votre agence souligne la hausse significative des fuites de données, l'érosion des frontières entre acteurs cybercriminels ainsi que le ciblage d'infrastructures critiques comme les télécommunications ou l'énergie, au risque d'un grand *black-out*. Vous ne l'excluez pas, évoquant une série d'attaques informatiques coordonnées à

visées destructives contre les infrastructures électriques polonaises fin 2025. S'agissant des scrutins électoraux, nous avons la chance, selon vous, de disposer d'un système de vote essentiellement fondé sur le papier.

À ce titre, la solution n'est-elle pas dans le retour du papier ou au moins dans un système moins numérique et, partant, moins vulnérable ? La France peut-elle assurer sa souveraineté en la matière ? En a-t-elle les moyens technologiques et financiers ?

M. Vincent Strubel. Je commencerai par rappeler que l'action centrée sur l'administration s'inscrit dans un cadre plus large, tel que le définit la revue nationale stratégique. Le constat qui y est posé est clair : il est indispensable de traiter l'ensemble des pans de notre société et de notre économie susceptibles d'être ciblés de manière coordonnée. En effet, les menaces auxquelles nous faisons face ne relèvent pas uniquement du champ cyber au sens strict, mais d'un *continuum* de menaces hybrides. Dans le scénario que j'évoquais précédemment, je me limitais au volet cyber, mais il est évident que celui-ci pourrait être accompagné de manipulations de l'information, de sabotages, de la mobilisation d'acteurs criminels au sens traditionnel du terme, et plus largement, de tout un ensemble d'actions qui demeurent sous le seuil de conflictualité ouverte, tout en visant à déstabiliser le front intérieur.

Dans ce cadre, l'Anssi dispose d'un atout majeur : sa capacité à travailler avec l'ensemble des acteurs concernés et au bénéfice de tous. Depuis toujours, en matière de cybersécurité, l'Anssi agit en coopération étroite avec ses partenaires. Cela inclut les acteurs du secteur privé, les collectivités territoriales, de plus en plus impliquées, les relais locaux, le monde associatif, ainsi que, de manière évidente, les autres services de l'État. Cette coopération s'exprime également dans des cadres particuliers, notamment celui du C4.

Toutefois, cette action globale s'inscrit nécessairement dans une logique de priorisation. Il ne s'agit pas de considérer toutes les cibles de manière indistincte, mais d'adapter l'engagement des ressources en fonction des enjeux. Ainsi, certaines fonctions stratégiques occupent une place centrale, comme nos capacités de dissuasion, qui constituent le cœur de notre sécurité, ou encore le noyau régalien de l'État, incluant les réseaux diplomatiques, les systèmes classifiés et les fonctions militaires.

À ces priorités s'ajoutent les infrastructures critiques, telles que les réseaux électriques, qui jouent un rôle essentiel dans le fonctionnement du pays. Au-delà de ces catégories, nous devons prendre en compte l'ensemble du tissu économique et social sans pour autant disperser l'action. Cette démarche repose sur un principe fondamental : ne laisser personne de côté. Il ne s'agit pas de traiter tous les enjeux avec la même intensité, mais de s'assurer qu'aucune zone de vulnérabilité n'est ignorée.

Dans cette gradation des priorités, le cadre électoral occupe une place particulière. Les scrutins constituent l'un des fondements de notre modèle démocratique, et leur intégrité revêt une importance critique. Depuis plusieurs années, l'Anssi porte une attention soutenue à la protection des processus électoraux. Les cyberattaques visant les scrutins sont une réalité avérée depuis au moins une décennie. La France bénéficie toutefois d'un atout significatif puisque l'organisation de ses élections repose majoritairement sur des procédures papier, ce qui limite la dépendance au numérique et réduit certaines vulnérabilités. Néanmoins, les

systèmes numériques qui interviennent dans ce processus font l'objet d'une vigilance particulière.

Par ailleurs, l'Anssi propose depuis longtemps une offre de services destinée aux équipes de campagne et aux partis politiques. Cette offre, non contraignante, vise à les accompagner face aux risques cyber auxquels ils sont exposés. En effet, les partis politiques et les élus constituent des cibles potentielles, parfois plus vulnérables que les infrastructures étatiques les plus sensibles, en raison de leurs moyens plus limités. Une attaque visant ces acteurs peut contribuer à déstabiliser le fonctionnement démocratique dans son ensemble.

Cette action s'inscrit également en lien avec les autorités compétentes en matière électorale, notamment le juge de l'élection, afin d'assurer une réponse adaptée en cas d'incident.

Mme Patricia Lemoine (EPR). La France est aujourd'hui fortement exposée à la menace cyber, le début de l'année 2026 ayant été marqué par des violations de données majeures touchant des systèmes publics sensibles. Face à cette vulnérabilité, vous avez identifié trois priorités : réduire les dépendances numériques, reprendre la maîtrise des technologies critiques et accélérer le cadre réglementaire. Aujourd'hui, la menace cyber s'est installée au cœur des conflictualités hybrides, la souveraineté française est fragilisée par ses dépendances techniques profondes, et le passage à une cybersécurité de masse tarde à s'opérer.

Lors de votre récente audition au sein d'une commission d'enquête, vous avez alerté sur l'absence de cartographie de l'environnement logiciel et sur la dépendance aux mises à jour de sécurité d'éditeurs étrangers. Dans ce contexte, comment l'Anssi articule-t-elle sa mission de conseil et d'appui en l'absence de pouvoirs coercitifs ?

Par ailleurs, le piratage de l'Agence nationale des titres sécurisés (ANTS) en avril 2026 illustre un scénario qui dépasse la simple négligence technique. Un expert en cybersécurité affirme avoir signalé deux failles critiques à l'ANTS bien avant l'attaque, l'une étant encore active une semaine après l'intrusion. Le problème ne semble plus se situer au seuil de connaissance de la menace, mais au niveau de la chaîne de traitement. L'Anssi dispose-t-elle aujourd'hui des leviers pour s'assurer que les signalements de vulnérabilité sur les systèmes d'information (SI) de l'État aboutissent à des corrections dans des délais contraignants ?

Enfin, la RNS identifie la massification et la coordination des cyberattaques comme le scénario central d'escalade géopolitique. La France a maintenu une doctrine de cyber défense défensive et une retenue affichée sur les capacités offensives, alors que d'autres pays comme les Pays-Bas ou le Royaume-Uni ont opté pour le développement de capacités cyber-offensives. Pensez-vous que la France devrait revoir sa doctrine et, dans l'affirmative, de quelle manière ?

M. Vincent Strubel. L'attaque subie par l'ANTS révèle en premier lieu la complexité du système d'information de l'État. C'est ici que réside aujourd'hui la principale difficulté. Nous sommes face à un ensemble extrêmement vaste, composé de milliers d'applications, dont le pilotage n'est pas uniformisé et dont les choix technologiques sont marqués par une très grande hétérogénéité. C'est sur ce point qu'il faut agir prioritairement pour renforcer la sécurité.

La réforme annoncée par le premier ministre porte précisément sur ce besoin de renforcer le pilotage du numérique. Il ne s'agit en aucun cas d'une remise en cause du rôle de l'Anssi ou de la Dinum, qui accomplit un travail essentiel. Au contraire, il s'agit de donner à la Dinum des moyens et des capacités renforcés pour rationaliser le système d'information de l'État, notamment par la mutualisation. L'exemple du réseau interministériel de l'État (RIE) illustre bien cette approche, puisqu'il a permis de regrouper des infrastructures auparavant dispersées, d'améliorer la souveraineté, de concentrer l'expertise et de renforcer la cybersécurité.

Par ailleurs, le traitement des signalements de vulnérabilité constitue un élément structurant. L'Anssi compte déjà plusieurs dispositifs destinés à recevoir et protéger les signalements, y compris anonymes. La difficulté, en réalité, ne réside pas tant dans l'identification des failles que dans leur correction, qui suppose une maîtrise accrue des systèmes.

S'agissant des dépendances, le rôle de l'Anssi consiste à définir des cadres de gestion des risques, à identifier ces dépendances et à proposer des mesures de protection. Le dispositif SecNumCloud en est une illustration ; il vise à garantir la sécurité technique des infrastructures, mais aussi à prévenir les risques liés à des législations extraterritoriales ou à des mécanismes de prise de contrôle. Toutefois, ces dispositifs ne suffisent pas à eux seuls. Ils doivent être accompagnés d'une politique industrielle visant à soutenir des solutions européennes et à développer des alternatives. Il est essentiel de mener les démarches de manière concomitante, qu'il s'agisse de la gestion des risques d'un côté ou du développement industriel de l'autre.

La France dispose de capacités offensives, mais elles ne relèvent pas de l'Anssi. Ce choix structurel, opéré dès la création de l'agence, permet selon moi de maintenir une distinction claire des rôles et de préserver un climat de confiance. Le fait que l'Anssi soit une agence défensive et non un service de renseignement a contribué, à mon sens, au succès du modèle français, qui continue d'être une pierre angulaire de nos capacités. De fait, il ne s'agit pas d'opposer les approches défensives et offensives, car la réponse aux cyberattaques ne peut se limiter à une logique de riposte.

Encore une fois, les cyberattaques posent des enjeux d'asymétrie : il est plus facile de reconstruire une infrastructure d'attaque que de réparer les dégâts causés sur un hôpital ou une station d'épuration.

M. Emmanuel Fernandes (LFI-NFP). En 2025, vos services ont eu connaissance de 1 366 cyberattaques réussies par des agents malveillants. Selon vous, combien de cyberattaques n'ont pas été recensées ? Quelle est la part des attaques qui aboutissent réellement ?

Plus largement, face à ces menaces croissantes, estimez-vous que le rythme du changement de paradigme collectif, qui doit être partagé à tout niveau, est suffisamment rapide et que les moyens mis à disposition, notamment par l'État, sont suffisants ? On peut se poser sérieusement la question quand on voit que la direction générale de la sécurité intérieure (DGSI) a, en décembre dernier, renouvelé un contrat avec Palantir. Le Premier ministre a initié une réorganisation des instances chargées de la protection des ministères contre les cyberattaques. Mais n'y a-t-il pas là un paradoxe ?

Plus spécifiquement, comme l'a rappelé mon collègue Aurélien Saintoul dans une proposition de résolution de création d'une commission d'enquête, les cyberattaques touchent particulièrement des publics déjà exposés à des situations de précarité économique, des personnes privées d'emploi, des allocataires de prestations sociales ou des patients. La dimension sociale des cyberattaques est-elle prise en compte dans les analyses de l'Anssi ?

Ces analyses mettent-elles en évidence des inégalités devant le risque de cyberattaques ? Enfin, s'agissant des infrastructures physiques, la guerre déclenchée par Israël et les États-Unis avec l'Iran a vu des data centers commerciaux notamment à Bahreïn et aux Émirats arabes unis être délibérément ciblés dans le cadre d'opérations militaires. Ces actions soulignent que ces infrastructures sont exposées à des menaces croissantes. Avez-vous intégré ces éléments dans votre stratégie de protection ? Les centres de données sont-ils suffisamment préparés face à ce type de menaces, qu'elles soient cyber ou matérielles ? Enfin ne pourrait-on pas envisager des solutions de plus grande décentralisation de la collecte et surtout du stockage des données, afin de réduire les risques de pertes massives ou de fuites ?

M. Vincent Strubel. Je commencerai par clarifier la question relative aux instances chargées de la protection cyber au sein des ministères, afin d'éviter toute ambiguïté. Il existe en effet une chaîne fonctionnelle cyber clairement établie. L'Anssi en constitue le chef d'orchestre, en tant qu'autorité nationale de cybersécurité et de cyberdéfense. Ce rôle est stable et n'est en aucun cas remis en cause par la réforme en cours, qui prévoit la création de l'entité dénommée Ariane, autorité du numérique et de l'IA.

La réforme concerne en réalité le pilotage du numérique, et non celui de la cybersécurité au sens strict. Cette distinction est essentielle, car les difficultés actuelles, telles qu'elles apparaissent dans la feuille de route des ministères, relèvent en grande partie de problématiques structurelles du numérique. Il s'agit notamment du déploiement de l'authentification à double facteur, du suivi de l'identité numérique ou encore de la gestion des obsolescences. La cause profonde de ces défis réside dans la complexité et l'hétérogénéité considérables du système d'information de l'État. Une telle situation existe également dans le secteur privé, mais elle est amplifiée à l'échelle d'une organisation aussi vaste que l'État.

La réforme vise précisément à agir sur ce point, sans modifier la répartition des rôles. L'Anssi continuera à définir les exigences de cybersécurité, à fixer des priorités et à en contrôler l'application, rôle qui sera encore renforcé dans le cadre de la directive NIS 2, laquelle étendra ses pouvoirs de contrôle. Toutefois, une cybersécurité efficace suppose également un numérique performant. C'est à ce niveau que la réforme intervient, en améliorant les capacités de pilotage, les leviers d'action et la clarté des missions, afin de favoriser la mutualisation et l'harmonisation des choix techniques.

Demain, l'Anssi et l'autorité issue de la réforme travailleront de manière étroite pour élaborer conjointement la feuille de route numérique et cybersécurité de l'État, en veillant à la cohérence des efforts engagés. L'objectif est d'éviter la dispersion des ressources et la mobilisation des efforts dans la sécurisation d'un nombre excessif d'applications. À cet égard, la rationalisation des ressources apparaît comme une nécessité absolue.

Cette exigence est renforcée par l'accélération du rythme des menaces, en particulier en matière de vulnérabilités logicielles. Nous sommes susceptibles d'atteindre un volume mondial de 50 000 vulnérabilités identifiées en une année, dont une part significative,

environ 30 %, est exploitée dans les vingt-quatre heures suivant leur publication. Dans ces conditions, il est illusoire de vouloir corriger instantanément chaque faille. En revanche, il est impératif de concevoir des architectures plus robustes, résilientes et capables de tolérer temporairement l'existence de vulnérabilités.

S'agissant de la dimension sociale des cyberattaques, je reconnais la difficulté à en proposer une analyse exhaustive. Néanmoins, la stratégie engagée repose sur la constitution d'un maillage dense d'acteurs capables de répondre aux incidents. Ce maillage est assuré notamment par les CSIRT, ainsi que par les dispositifs accessibles au public comme le 17 Cyber. L'objectif fondamental consiste à garantir à toute victime, qu'il s'agisse d'un particulier, d'une entreprise ou d'une collectivité, la possibilité de trouver un interlocuteur et un accompagnement adaptés.

Ce dispositif accepte, au besoin, certaines redondances. Elles ne constituent pas un défaut, dès lors qu'elles contribuent à éviter toute lacune dans la prise en charge des victimes. L'essentiel est que chacun sache vers qui se tourner en cas de cyberattaque ou de cyber-malveillance. À cet égard, le rôle du GIP Acyma est central, notamment à travers la plateforme cybermalveillance.gouv.fr, le 17 Cyber et le futur portail de sensibilisation et de prévention destiné au grand public. Ce modèle, fondé sur la coopération, s'impose comme une référence.

Enfin, la question des infrastructures physiques dépasse le seul cadre de la cybersécurité, mais elle en constitue un complément indissociable. Elle est pleinement intégrée dans la revue nationale stratégique. Parallèlement à la transposition de la directive NIS 2, la directive REC vise à renforcer la protection physique des infrastructures critiques. Il s'agit de mener de front ces deux dimensions, numérique et physique.

M. Thierry Sother (SOC). L'actualisation de la loi de programmation militaire (LPM) 2024-2030 intervient dans un contexte profondément transformé depuis 2023. Ce dernier est marqué par la guerre en Ukraine, la multiplication des attaques contre les hôpitaux, collectivités et opérateurs critiques, une hausse des ingérences informationnelles visant à défaire le lien social ou faire basculer nos élections, une intensification des opérations hybrides. Nombreux sont les événements qui ont montré l'importance d'une agence comme l'Anssi pour détecter les menaces, les analyser, organiser la mise en sécurité de nos systèmes et développer la cybersécurité dans la société.

Ensuite, un article de presse paru ce matin fait état de grande tension entre l'agence et le Premier ministre. Il y est indiqué « en off » que l'Anssi ne remplirait plus ses missions et serait devenu un outil trop administratif. Ce jugement comporte-t-il une part de vérité à vos yeux ? Il y est aussi mentionné la rareté des contrôles de l'Anssi. Pourriez-vous nous apporter des précisions sur ces contrôles, le temps et les ressources qu'ils prennent ? Pourriez-vous également nous indiquer la part de contrôle inopiné qu'effectuent vos services ?

Enfin, l'article indique que le contrôle de l'ANTS ne relève pas de l'Anssi, l'ANTS n'étant pas considérée comme étant d'importance vitale. Pourriez-vous nous indiquer combien d'organismes sont jugés d'importance vitale et auprès desquels vous agissez pour leur surveillance et leur protection ?

M. Vincent Strubel. Je tiens à être parfaitement clair : il n'existe pas de tension entre le Premier ministre et l'Anssi. D'ailleurs, si une telle tension existait, elle se résoudrait très rapidement dans le fonctionnement de l'État, notamment par le remplacement d'un directeur général, ce qui n'est absolument pas à l'ordre du jour à ma connaissance. Je réfute donc totalement ce qui est avancé dans cet article. En réalité, il y a une mécompréhension fondamentale de la réforme annoncée, qui ne porte pas sur l'Anssi, mais sur le pilotage numérique.

Il n'y a aucune remise en cause des missions de l'Anssi ni de l'efficacité de son travail. De la même manière, il n'y a pas de remise en cause de la qualité du travail de la Dinum. L'objectif est simplement de renforcer les moyens, les capacités d'action et le champ de mission pour construire un numérique plus solide, qui constitue la base d'une cybersécurité de qualité et d'une véritable cyber résilience.

Au-delà de mon cas personnel, je regrette profondément les attaques qui visent indirectement les agents de l'Anssi. Ces agents accomplissent un travail remarquable, souvent au prix de sacrifices importants, qu'il s'agisse de leurs week-ends, de leurs soirées ou de leurs congés. Leur engagement est total, leur compétence est reconnue, et leur dévouement est exemplaire. Les comparer à des « cyber-pompiers » n'est pas une simple métaphore : ils interviennent en permanence pour éteindre des incendies numériques. Les mettre en cause revient à fragiliser un dispositif essentiel.

S'agissant des capacités de contrôle, l'Anssi dispose de moyens d'audit lui permettant de tester la sécurité de certains systèmes d'information. À titre indicatif, nous sommes en mesure de réaliser environ cinquante audits par an. Ce chiffre doit être mis en perspective avec les milliers de systèmes existants, au sein de l'État comme chez les opérateurs d'importance vitale. Ces derniers sont environ 300. Il est donc évident que nous ne pouvons pas tout auditer systématiquement.

Nous fonctionnons donc selon une logique de priorisation, en concentrant les efforts sur les systèmes les plus critiques, les plus sensibles et les plus complexes, notamment ceux qui relèvent des enjeux régaliens, comme certaines infrastructures stratégiques ou les centrales nucléaires. Pour étendre cette capacité, nous avons développé depuis 2014 un dispositif de prestataires d'audit qualifiés (Passi) par l'Anssi, qui permet de démultiplier les audits, qu'ils soient volontaires ou inopinés.

Par ailleurs, la mise en œuvre de la directive NIS 2 constitue une avancée majeure. Elle permettra de renforcer les capacités de contrôle, de préconisation et surtout de sanction. Aujourd'hui, l'Anssi peut saisir le juge dans le cadre de sanctions pénales. Demain, elle disposera de sanctions administratives, plus rapides et plus efficaces, ce qui introduira un véritable levier supplémentaire.

L'exemple de l'ANTS illustre bien cette logique. L'ANTS regroupe une multitude de systèmes d'information de niveaux de criticité différents. Certains systèmes, comme le fichier TES, qui contient des données biométriques, ont été audités et sécurisés par l'Anssi. D'autres, comme France Identité Numérique, ont fait l'objet de certifications au plus haut niveau européen, au prix d'un travail approfondi.

Toutefois, compte tenu du nombre de systèmes, il est impossible de tous les traiter avec la même intensité. Le portail qui a été attaqué n'était pas le plus critique. Cela ne signifie

pas que l'attaque est anodine, puisqu'elle a concerné des données personnelles. Toutefois, il ne s'agissait pas des données les plus sensibles, comme les données biométriques.

Cette situation illustre l'enjeu de priorisation, lequel s'inscrit dans une démarche plus large de rationalisation des systèmes d'information.

Mme Josy Poueyto (Dem). Notre groupe est très sensible aux actions portées par l'Anssi. La France est un pays des plus touchés au monde par des cyberattaques. L'année 2026 est marquée par des niveaux sans précédent, puisque 54 000 incidents de sécurité ont été enregistrés au premier trimestre, soit une hausse de 37 % par rapport à 2025, si j'en crois la presse spécialisée. Tous les secteurs d'activité sont concernés et les organisations publiques représentent environ 18 % du nombre total d'attaques.

Le service public est ainsi devenu une cible privilégiée des cybercriminels, soit en raison de la nature des données qu'il est amené à traiter et à stocker, soit en raison de motivations plus politiques qu'économiques des hackers en cause. Quoi qu'il en soit, la liste des cibles atteintes dont le public a eu connaissance est impressionnante. Cette situation met en lumière une vulnérabilité assez élevée de nos protections, alors que nos concitoyens sont contraints de confier leurs données de manière dématérialisée aux services de l'État.

Monsieur Strubel, même si je comprends bien qu'il est très délicat d'évoquer toute forme de faille dans nos systèmes, comment expliquer cette vulnérabilité du secteur public, alors que celui-ci devrait être extrêmement protecteur, pour ne pas dire imperméable, à la menace cyber ? S'agit-il d'un manque de moyens financiers ou humains ? Je voudrais également vous entendre sur le rôle de l'Agence dans les actions menées au plus près des territoires, en termes de prévention et de stratégie proactive.

De quels soutiens locaux auriez-vous encore besoin pour gagner en efficacité ? S'agit-il de la préfecture, de la délégation militaire départementale, de la gendarmerie ?

M. Vincent Strubel. Je reviens en premier lieu sur l'idée selon laquelle la France serait le pays le plus touché au monde. Nous n'en savons, à proprement parler, rien. Aujourd'hui, personne n'est en mesure de compter de façon fiable, homogène et universelle les cyberattaques. Cette difficulté méthodologique empêche toute comparaison rigoureuse entre pays. J'ajoute, pour compléter une réponse précédemment omise, que nous ne savons pas davantage quantifier la part des cyberattaques qui échouent. Il n'existe tout simplement pas de métrique universelle permettant de saisir l'ensemble du phénomène.

Dans les faits, je constate que la majorité des attaques échouent, en particulier sur les systèmes que nous supervisons, notamment ceux de l'État. Chaque jour, nous observons des dizaines et des dizaines de tentatives d'attaques. Toutefois, la manière de les compter varie considérablement. L'exemple des Jeux olympiques et paralympiques de 2024 est à cet égard particulièrement éclairant. Alors même que de nombreuses analyses prédisaient une catastrophe et remettaient en cause la capacité de la France à sécuriser l'événement, nous avons démontré qu'il était possible d'y parvenir. Nous avons, pour notre part, comptabilisé environ 500 cyberattaques. Le Comité international olympique, de son côté, en a recensé 55 milliards.

Ces chiffres, en apparence contradictoires, renvoient en réalité à des méthodes de comptage différentes. Nous considérons une attaque comme l'association d'une cible, d'un

attaquant et d'un effet recherché et obtenu. D'autres approches consistent à dénombrer le volume de messages émis par l'attaquant, qui peut atteindre des millions, voire des milliards pour une seule opération, notamment dans le cas de tentatives de saturation. Il n'existe donc aucune unité de mesure commune. Dans ce contexte, il est évident que la France, en raison de son positionnement géopolitique et de son statut de grande nation, constitue une cible. Pour autant, affirmer qu'elle serait plus ou moins attaquée ou plus ou moins vulnérable que d'autres pays dépasse ce que nous sommes en mesure d'établir.

Je suis néanmoins convaincu que nous n'avons pas à rougir de nos capacités en matière de cybersécurité. Les Jeux olympiques en ont été une démonstration concrète. La France est reconnue pour son expertise, même si cela ne doit en aucun cas conduire à un relâchement. Des progrès restent nécessaires, notamment dans le service public, qui demeure fortement exposé. Cette exposition s'explique par son ampleur, par l'étendue de ses missions et, pour certaines de ses composantes, par son caractère régalien.

Depuis plus d'une décennie, certaines administrations font l'objet d'attaques d'espionnage, souvent peu visibles, mais persistantes. Aujourd'hui, ces mêmes cibles sont également visées pour la portée symbolique qu'elles représentent. Sans me prononcer sur des motivations strictement politiques, je relève l'existence d'enjeux réputationnels chez certains attaquants. Les vols de données récents ont parfois été motivés par la recherche du coup d'éclat susceptible d'accroître leur notoriété au sein de leur écosystème. Certaines revendications ont, par ailleurs, été formulées en réaction à l'action de la justice, notamment à la suite d'arrestations de cyberattaquants. Je tiens d'ailleurs à saluer le travail des services de police, de gendarmerie et de la justice, dont l'action est déterminante.

Face à ces dynamiques, j'insiste sur un point : il s'agit d'une trajectoire sans issue favorable pour ceux qui s'y engagent. Les interpellations sont inévitables et il est regrettable de voir des jeunes, parfois âgés de 15 ans, se retrouver dans de telles situations.

Enfin, la question des moyens doit être abordée en lien avec celle des modèles. Nous disposons, en France, d'un modèle particulièrement efficace. L'Anssi, avec environ 660 agents, accomplit ses missions avec une grande efficacité, malgré des effectifs inférieurs à ceux de certains de nos homologues européens. Cette performance repose notamment sur une coopération étroite avec les autres services de l'État et sur le développement d'un maillage territorial structuré.

Ce maillage, construit avec les collectivités, notamment les régions, s'appuie sur des dispositifs tels que les CSIRT territoriaux et les campus cyber. Il favorise le dialogue entre besoins et offres, et contribue à diffuser la culture de cybersécurité au plus près des acteurs. Ce modèle de proximité est essentiel et appelé à se renforcer. Les CSIRT, en particulier, offrent un cadre harmonisé et opérationnel de traitement de l'information.

Ils s'inscrivent dans un réseau dynamique, fédéré notamment par l'association InterCERT France, qui regroupe aujourd'hui de nombreux CSIRT issus de différents niveaux et secteurs. Cette organisation permet, en cas de crise, un partage rapide, structuré et contextualisé de l'information au profit d'un territoire, d'un secteur d'activité.

M. Antoine Valentin (UDR). En avril 2025, les services de renseignement norvégiens attribuaient formellement à des hackers russes la prise de contrôle à distance d'un barrage dans l'ouest du pays, à travers l'exploitation de vulnérabilités sur des équipements

industriels exposés en ligne. En Pologne, fin 2025, des attaques coordonnées frappaient des infrastructures énergétiques, une première dans un État membre de l'Union européenne.

Dans les deux cas, le vecteur était identique : des équipements exposés, non protégés, dont les interfaces de gestion étaient accessibles sans authentification sérieuse. En France, votre rapport établit qu'à la fin 2025, plus de 6 200 actifs restaient affectés par des vulnérabilités connues depuis 2023 et 2024. Lors d'une seule alerte sur une faille Fortinet, le CERT-FR a recensé 3 700 interfaces d'administration exposées. Ensuite, 29 % des vulnérabilités exploitées en 2025 l'ont été le jour même de leur publication ou avant. Vous documentez vous-mêmes les tentatives de sabotage d'installations hydroélectriques et d'énergies renouvelables sur le territoire national en 2025. La Directive NIS 2 sera, on l'espère, bientôt transposée.

Le *Cyber Résilience Act* entre en vigueur le 11 septembre 2026. Vous disposerez bientôt d'un cadre juridique qui oblige les opérateurs à notifier, à corriger, à rendre compte. Mais entre la norme et la réalité que vous documentez vous-mêmes, il existe aujourd'hui un gouffre. Au regard des sabotages d'infrastructures chez nos alliés européens, des tentatives sur le territoire national, des vulnérabilités critiques non corrigées dans la durée, ce modèle est-il encore tenable ? Si la réponse est négative, quelle évolution du cadre législatif appelez-vous de vos vœux ? S'agit-il d'un pouvoir d'injonction, de mise en conformité, d'un régime de sanctions administratives comparable à l'Anssi allemande, d'un modèle semblable à celui de vos homologues britanniques ?

M. Vincent Strubel. Je reviens brièvement sur la menace de sabotage. Elle est bien réelle, et elle fait l'objet d'échanges constants avec nos homologues norvégiens, polonais et, plus largement, européens, sans exclusivité. Nous partageons nos appréciations de la menace, nos constats opérationnels et nous cherchons à maintenir, ensemble, une vigilance collective structurée.

S'agissant du sabotage visant certains équipements, notamment hydroélectriques de petite taille, nous avons déjà observé en France des incidents significatifs. Il ne s'agissait pas d'acteurs étatiques au sens strict, mais d'acteurs relevant du registre hacktiviste. Certains peuvent néanmoins constituer des proxys d'État, sans être formellement des agents publics ; d'autres peuvent même, à l'occasion, appartenir à la sphère étatique de manière plus informelle. Ce type de situation n'est pas inédit. Nous avons ainsi vu des acteurs pro-russes revendiquer de manière particulièrement bruyante des attaques contre des barrages hydroélectriques. Ces attaques ont touché des micro-installations industrielles caractérisées par un niveau de sécurité extrêmement faible.

Dans plusieurs cas, ces installations étaient exposées directement sur Internet, administrables à distance avec des dispositifs de protection dérisoires, allant jusqu'à l'utilisation de mots de passe par défaut tels que « 1-1-1-1 », jamais modifiés. Cette situation illustre parfaitement la problématique actuelle : la vulnérabilité technique élémentaire, combinée à une exposition numérique non maîtrisée, ouvre des opportunités à des acteurs hostiles.

Ces mêmes acteurs ont tenté de s'en prendre aux stations d'épuration dans le but de polluer la Seine à l'occasion des Jeux olympiques. Ils n'y sont pas parvenus, mais ont cherché à en donner l'illusion. Cette tentative constitue un exemple éclairant d'attaque

hybride, agissant simultanément sur le plan technique et sur le plan réputationnel. Bien que l'action ait échoué, l'effet de communication et de désinformation était recherché. Il est important de souligner que cette menace, bien que contenue, mobilise un facteur de masse considérable.

En effet, parmi les missions de traitement des signalements de vulnérabilités, il nous incombe d'alerter un grand nombre de victimes potentielles. Or, chaque campagne d'exploitation peut concerner des milliers d'entités, face à des attaquants capables de tirer parti à grande échelle de la moindre faille. Cette réalité a conduit, depuis plusieurs années, à anticiper une réponse structurée à l'échelle européenne.

C'est dans ce contexte qu'a été élaborée la directive NIS2. Elle vise à renforcer nos capacités de contrôle, mais surtout à généraliser les bonnes pratiques de cybersécurité. L'enjeu fondamental consiste à diffuser ces pratiques sur une large partie de notre économie et de notre société afin d'éviter des points de fragilité critiques. Il s'agit ainsi de ne plus être exposé à la première vulnérabilité triviale identifiée.

Par ailleurs, le règlement européen sur la cyberrésilience, le *Cyber Resilience Act* (CRA), apporte une réponse directe à la prolifération d'équipements non sécurisés. Demain, il ne sera plus possible de déployer des dispositifs connectés, comme des éoliennes ou des microbarrages, à l'aide de mots de passe par défaut ou des mécanismes de sécurité insuffisants. Ce cadre introduira un véritable pouvoir de contrôle harmonisé à l'échelle européenne.

Dès lors, la question des évolutions nécessaires dans nos capacités appelle une réponse pragmatique : il convient avant tout de mettre en œuvre les dispositifs existants et en cours d'adoption. Le chantier est considérable. Il inclut notamment le projet de loi relatif à la résilience, mais aussi le travail engagé depuis plusieurs années pour préparer l'application du CRA. Ce travail implique le développement d'une capacité renforcée de contrôle et, le cas échéant, de sanction.

À cet égard, une commission des sanctions indépendante sera amenée à statuer, conférant à l'Anssi un levier effectif. Ce cadre constitue déjà une transformation majeure ; il ne paraît pas nécessaire, à ce stade, d'y ajouter des évolutions structurelles supplémentaires. En revanche, il importe d'inscrire cette dynamique dans des logiques économiques. La directive NIS2 conduira à superviser environ 20 000 entités régulées en France, ce qui est significatif, mais ne couvre pas l'ensemble du tissu économique.

Il n'est pas opportun d'imposer des obligations excessives aux très petites entreprises ou aux particuliers. En revanche, d'autres leviers existent. Les assureurs et les établissements bancaires jouent un rôle croissant de prescripteurs en matière de sécurité. Il existe donc un travail structurant à mener avec ces acteurs pour diffuser les bonnes pratiques au-delà du cadre strictement réglementaire.

Mme Sabine Thillaye, présidente. Quel regard portez-vous sur la notion de « hacker éthique » ?

M. Vincent Strubel. Il s'agit d'un terme dont la définition demeure incertaine, faute de référentiel stabilisé. Néanmoins, ces acteurs font pleinement partie de l'écosystème de la cybersécurité avec lequel nous collaborons quotidiennement. Cet écosystème est vaste et

hétérogène ; il n'existe pas de frontière stricte entre ces composantes. Nous parlons volontiers d'une « équipe de France de la cybersécurité », qui inclut des entreprises privées, des opérateurs, des associations, des acteurs académiques, des services de l'État, des collectivités et même des particuliers.

Dans ce cadre, certains individus adoptent des démarches responsables en signalant des vulnérabilités. Un dispositif juridique existe pour encadrer ces pratiques. Il existe des dispositions issues de la loi pour une république numérique, mais aussi des textes européens qui prolongent la loi Sapin sur la notion de lanceur d'alerte, qui nous permettent de recevoir des signalements et d'assurer la protection des lanceurs d'alerte.

Chaque année, plusieurs centaines de signalements sont ainsi traitées. Toutefois, ce dispositif reste perfectible, notamment en matière de connaissance et d'appropriation par les acteurs concernés. Il convient néanmoins de rester vigilant : tous ceux qui se revendiquent « éthiques » ne le sont pas nécessairement. Des cas récents ont révélé l'existence d'individus signalant des vulnérabilités tout en commercialisant les données sur des réseaux clandestins. Dans de telles situations, les faits sont portés à la connaissance de l'autorité judiciaire.

Enfin, il importe de renforcer le dialogue avec cet écosystème, notamment pour améliorer la compréhension de la menace auprès du grand public, sans céder à la dramatisation ni relayer les discours des attaquants. Nous n'avons pas fini de travailler avec cet univers des hackers éthiques dans sa pluralité. Au passage, je les remercie pour leur contribution essentielle dans le cadre de missions de l'Anssi, et plus généralement, en faveur de notre cybersécurité collective.

Mme Sabine Thillaye, présidente. Je vous remercie

La séance est levée à midi trente.

*

* *

Membres présents ou excusés

Présents. - Mme Delphine Batho, M. Michel Criaud, Mme Sophie Errante, M. Emmanuel Fernandes, M. José Gonzalez, Mme Nadine Lechon, Mme Patricia Lemoine, Mme Josy Poueyto, Mme Natalia Pouzyreff, M. Thierry Sother, Mme Sabine Thillaye, M. Romain Tonussi, M. Antoine Valentin, Mme Corinne Vignon

Excusés. - Mme Anne-Laure Blin, M. Matthieu Bloch, M. Manuel Bompard, M. Hubert Brigand, Mme Cyrielle Chatelain, Mme Geneviève Darrieussecq, M. Moerani Frébault, M. Thomas Gassilloud, M. Frank Giletti, M. Damien Girard, Mme Catherine Hervieu, M. Jean-Michel Jacques, M. Pascal Jenft, M. Bastien Lachaud, Mme Lise Magnier, Mme Michèle Martinez, Mme Alexandra Martin (Alpes-Maritimes), Mme Mereana Reid Arbelot, Mme Marie-Pierre Rixain, M. Aurélien Saintoul, Mme Isabelle Santiago, M. Mikaele Seo, M. Boris Vallaud, M. Laurent Wauquiez

Assistait également à la réunion. - Mme Florence Goulet