ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission des affaires étrangères

Mercredi
7 mai 2025
Séance de 9 heures

Compte rendu n° 56

SESSION ORDINAIRE 2024-2025

Présidence de M. Bruno Fuchs, *Président*

ASSEMBLÉE NATIONALE

La commission procède à l'audition, ouverte à la presse, de M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information.

La séance est ouverte à 9 h 05.

Présidence de M. Bruno Fuchs, président.

M. le président Bruno Fuchs. Votre audition, Monsieur Vincent Strubel, intervient dans un contexte où notre pays fait face à des défis majeurs en matière de cybermenaces et de manipulation de l'information.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), héritière de la direction technique des chiffres créée en 1943 à Alger, a été instituée par décret le 7 juillet 2009. En tant que service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationales (SGDSN), l'ANSSI a pour mission de veiller à la sécurité des systèmes d'information de l'État, de conseiller et soutenir les administrations et opérateurs d'importance vitale, ainsi que de contribuer à la sécurité de la société de l'information, notamment par la recherche et le développement des technologies de sécurité.

Monsieur Strubel, vous avez pris la direction générale de cette agence en janvier 2023, fort d'une expérience de quinze ans au sein de l'ANSSI et de deux ans et demi à la tête de l'Opérateur des systèmes d'information interministériels classifiés (OSIIC). Vous vous êtes également distingué pendant la pandémie de Covid-19 en proposant des solutions innovantes pour les services essentiels de l'État.

Le panorama de la cybermenace en 2024, publié le 11 mars dernier par votre agence, dresse le bilan d'une année marquée par une pression désormais constante émanant de deux types de menaces principales : d'une part, la menace systémique représentée par les attaquants cybercriminels et, d'autre part, les attaques attribuées principalement à la Russie et à la Chine, visant les systèmes d'information les plus critiques et stratégiques de notre nation. Face à ces menaces, nous sommes constamment sur la défensive, contraints de trouver des parades et des ripostes pour protéger nos systèmes. Notre statut d'État démocratique et de droit nous empêche de recourir aux mêmes méthodes offensives que nos adversaires, nous plaçant ainsi dans une position réactive face à des attaques toujours plus innovantes et imprévisibles.

Une illustration récente de la prégnance de ces dangers nous a été fournie par le ministre de l'Europe et des affaires étrangères, qui a révélé sur le réseau social X, le 29 avril dernier, que le service de renseignement militaire russe déployait un système cyber-offensif nommé APT28, visant à semer le doute et à influencer les opinions publiques. Les investigations de l'ANSSI ont permis de confirmer que les attaques survenues entre 2020 et fin 2024 contre des entités ministérielles, des collectivités locales et des entreprises pouvaient être imputées à la Russie. Il est même possible que la récente opération de manipulation de l'opinion publique concernant les punaises de lit soit attribuable aux Russes, illustrant leur capacité à déstabiliser l'opinion et l'appareil d'État sur des sujets apparemment anodins.

Plus généralement, l'ANSSI a traité 4 386 événements de sécurité l'année dernière, soit une augmentation de 15 % par rapport à 2023. L'agence a récemment publié son plan stratégique 2025-2027, dont nous attendons que vous nous présentiez les grandes lignes et que vous nous expliquiez comment la France se prépare à faire face aux principales menaces.

Le volet cybersécurité du projet de loi relatif à la résilience des infrastructures, visant à transposer la directive NIS 2 en France, constitue un élément essentiel de la réponse juridique et technique aux défis actuels. Le Sénat s'est prononcé sur ce texte le 12 mars dernier et notre Assemblée sera bientôt appelée à faire de même. Vos commentaires d'expert sur ce texte seront précieux dans cette perspective.

Au niveau européen, des efforts sont déployés pour renforcer les maillons les plus faibles. C'est ainsi que notre commission examinera, à l'issue de votre audition, le projet de loi autorisant l'approbation de l'accord portant création du centre de développement des capacités cyber dans les Balkans occidentaux (C3BO), déjà approuvé par le Sénat. Ce centre vise notamment à contrer les cyberattaques qui cherchent à manipuler ou influencer les élections dans des pays tels que la Moldavie, la Géorgie ou la Roumanie.

Monsieur le directeur général, nous souhaitons que vous nous présentiez ce matin un panorama de l'état actuel de la menace cyber et de son évolution, tant pour les administrations et services publics que pour les entreprises et les particuliers, de plus en plus victimes de rançongiciels et de *malwares* divers. En tant que législateurs, nous sommes également intéressés par votre évaluation de la pertinence des dispositifs en place et par vos suggestions pour les améliorer.

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le sujet de la menace russe dans le cyberespace, bien que partiellement confidentiel, mérite d'être abordé publiquement. L'actualité donne une résonance particulière à cette audition, la France venant d'attribuer officiellement et pour la première fois de manière autonome plusieurs cyberattaques au GRU, le service de renseignement militaire russe. Ces attaques, récentes ou plus anciennes, se sont distinguées par leur agressivité et par la nature des cibles choisies.

Avant d'approfondir la menace spécifiquement russe, permettez-moi de dresser un panorama global de la cybersécurité. Le 11 mars dernier, nous avons publié notre rapport annuel sur l'état de la menace, qui met en lumière non seulement une intensification des cyberattaques mais également, de manière plus préoccupante, une diversification des cibles. J'affirme régulièrement qu'aujourd'hui, nul n'est à l'abri et qu'il n'est pas nécessaire d'être une cible désignée pour devenir une victime. Cette situation engendre souvent un sentiment de perplexité chez les victimes, qui peinent à comprendre les raisons de leur ciblage.

Nous distinguons traditionnellement trois catégories d'acteurs malveillants dans le cyberespace, bien que cette classification présente certaines limites. Premièrement, les acteurs étatiques, qui constituent le cœur de l'activité historique de l'ANSSI. Il s'agit de services de renseignement étrangers pratiquant l'espionnage ciblé sur les administrations sensibles et les entreprises stratégiques. Certains États s'adonnent également de plus en plus au sabotage ou à la déstabilisation, visant à perturber les processus démocratiques ou à détruire des infrastructures critiques.

Deuxièmement, l'écosystème du crime organisé, motivé principalement par l'appât du gain. Ces groupes pratiquent l'extorsion par le biais de rançongiciels – paralysant les infrastructures informatiques et exigeant une rançon – ou par le vol de données, qui sont ensuite revendues ou utilisées comme moyen de chantage.

Troisièmement, les activistes ou « hacktivistes », dont la nature est plus variable et dont l'objectif principal est de marquer les esprits et d'attirer l'attention médiatique. Ils se réclament généralement de diverses causes et travaillent leur image personnelle, parfois en combinant leurs actions avec des activités lucratives.

Ces trois types de menaces, en constante évolution, mobilisent toute notre attention. Il est important de noter que cette typologie théorique ne se reflète pas parfaitement dans la réalité et que des convergences, des intersections et des zones grises existent entre ces différentes catégories d'attaquants. Nous observons parfois un alignement idéologique, notamment chez les activistes qui se réclament de causes pro-russes ou pro-iraniennes. De plus, une forme de cohabitation s'est instaurée, particulièrement visible dans le cas du crime organisé qui tend à opérer depuis la fédération de Russie, où il semble bénéficier d'une certaine impunité malgré les capacités répressives avérées du pays. Cette situation soulève des questions sur les liens potentiels de coordination entre ces groupes et les autorités.

Une convergence technique s'opère également, avec une mutualisation des codes d'attaque, dans les outils et les infrastructures. Les groupes d'attaquants, quelle que soit leur nature, utilisent de plus en plus des réseaux de serveurs, soit loués, soit eux-mêmes compromis. Ces infrastructures, parfois composées de dizaines de milliers d'ordinateurs, servent à effectuer des rebonds successifs, à brouiller les pistes et à assurer la persistance des attaques.

Ce paysage est encore complexifié par l'émergence d'acteurs privés spécialisés dans la lutte informatique offensive, qui commercialisent des outils d'attaque – dont le plus connu est *Pegasus* – officiellement destinés à la lutte contre la criminalité. Leur utilisation parfois détournée contribue à obscurcir davantage l'identification des commanditaires réels des cyberattaques.

L'identification des auteurs d'une cyberattaque demeure une science complexe et imprécise. La plupart des attaquants dissimulent leurs traces et l'ANSSI, qui n'est ni un service de renseignement ni un service d'enquête, se limite à identifier ce que nous appelons un mode opératoire d'attaque (MOA). Il s'agit d'un ensemble de techniques et de procédures caractéristiques d'un groupe d'attaquants, sans pour autant permettre d'identifier formellement les auteurs ou les commanditaires.

L'identification des commanditaires nécessite la combinaison d'informations provenant des services de renseignement, de partenaires étrangers et du secteur privé. Dans la doctrine française, l'attribution formelle d'une attaque relève soit de la justice, notamment dans les affaires criminelles, soit des autorités politiques lorsqu'il s'agit de désigner un État attaquant. Ces décisions ne sont prises qu'avec une certitude absolue et s'inscrivent dans le cadre des relations diplomatiques de la France. Pour des raisons de précaution, j'utiliserai l'expression « *mode opératoire d'attaque réputé lié à* » la Russie, par exemple, pour désigner des attaques généralement attribuées à des acteurs russes par d'autres sources, sans que nous ayons nécessairement de preuves indépendantes suffisantes pour confirmer cette attribution mais sans non plus avoir de raisons de la contester.

Concernant spécifiquement la menace russe, il est important de souligner que si la Russie n'est pas le seul acteur à mener des cyberattaques contre la France, deux caractéristiques la distinguent néanmoins dans le cyberespace.

Premièrement, la Russie se singularise par un continuum d'acteurs unique, mêlant des entités étatiques liées aux principaux services de renseignement – le service de renseignement extérieur (SVR), le service fédéral de sécurité de la fédération de Russie (FSB) et le GRU – à des éléments de la criminalité organisée et à une constellation d'activistes pro-russes. Bien qu'une coordination explicite entre ces acteurs ne soit pas toujours démontrable, leur action combinée exerce une pression considérable sur la France et sur l'Occident dans son ensemble.

Deuxièmement, la menace russe se caractérise par la diversité de ses objectifs. Au-delà de l'espionnage, qui est une pratique courante, les acteurs russes s'engagent dans des activités de sabotage, visant la destruction physique d'infrastructures numériques, ainsi que dans des opérations de déstabilisation ciblant notamment nos processus démocratiques. Cette multiplicité d'objectifs, couplée à une désinhibition marquée, distingue la Russie des autres acteurs étatiques dans le cyberespace.

Il convient de préciser que notre domaine d'expertise se limite aux cyberattaques. Les menaces hybrides, incluant la manipulation de l'information, telles que l'affaire des punaises de lit mentionnée par le président Fuchs, relèvent de la compétence du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), également rattaché au SGDSN.

Les acteurs étatiques russes se caractérisent par des modes opératoires sophistiqués, connus sous diverses appellations telles qu'APT28, *Sandworm*, *Turla* ou encore *Nobelium*, chacun étant associé à un service de renseignement spécifique. Leur niveau de sophistication et de furtivité, particulièrement élevé, se manifeste par l'exploitation de vulnérabilités qui n'ont pas encore été corrigées par les éditeurs, par la capacité à mobiliser divers vecteurs – humains ou interception électromagnétique – de collecte de renseignements et par des infrastructures d'attaque élaborées permettant une forte anonymisation. Ces acteurs ciblent intelligemment des équipements ou réseaux moins surveillés, exploitent les vulnérabilités des sous-traitants et excellent dans l'art de se fondre dans le bruit ambiant du cyberespace. Ils sont même capables de détourner les modes opératoires d'autres attaquants pour mener leurs propres opérations.

Leurs activités couvrent un large spectre, de l'espionnage au sabotage. En France, les cibles incluent les administrations régaliennes, particulièrement notre diplomatie, ciblée depuis plusieurs années par le mode opératoire *Nobelium*, ainsi que des think tanks et instituts de recherche en géopolitique, avec un intérêt particulier pour les courriels des individus ciblés ou pour les analyses conduites au profit des autorités françaises. L'industrie de la défense et le secteur aérospatial sont également visés, comme en témoigne l'attaque d'APT28 contre une entreprise clé de notre base industrielle et technologique de défense (BITD) en 2023, ayant conduit à un vol massif de données sensibles, y compris celles liées au soutien à l'Ukraine.

Le secteur des télécommunications est une autre cible récurrente, présentant un double intérêt, à la fois pour l'espionnage et pour le sabotage. Les acteurs du numérique, notamment aux États-Unis, sont également ciblés, comme l'illustrent les attaques intensives contre Microsoft par des modes opératoires réputés liés à la Russie.

Le sabotage constitue une spécificité de la menace russe. L'attaque du 24 février 2022 contre le réseau satellitaire Viasat, attribuée à la Russie par l'Union européenne, en est un exemple frappant. Elle a entraîné la destruction de milliers de terminaux de communication, affectant non seulement l'armée ukrainienne mais également des services

d'urgence en France. L'Ukraine demeure une cible privilégiée de ces attaques, comme l'a démontré l'incident *NotPetya* en 2017, sabotage d'un logiciel de comptabilité qui a paralysé de nombreuses entreprises et administrations ukrainiennes, avec des répercussions internationales. En France, l'entreprise Saint-Gobain a également subi des perturbations pendant plusieurs semaines, entraînant des pertes supérieures à 300 millions d'euros. L'Ukraine fait face à des attaques permanentes depuis 2022, ciblant notamment l'opérateur de télécommunications Kyivstar, ainsi que les secteurs de l'énergie, de la banque et de l'administration.

La France n'est pas épargnée par ces menaces, puisque nous avons récemment attribué formellement l'attaque contre TV5 Monde, en 2015, à APT28. Cette attaque, qui avait paralysé la chaîne et avait d'abord été attribuée au groupe État islamique, soulève des questions sur ses motivations : s'agissait-il d'entretenir l'anxiété dans un contexte post-attentat ou d'une démonstration de capacités ?

La déstabilisation constitue également une menace sérieuse, que l'affaire des « Macron Leaks » en 2017 illustre parfaitement. Le vol de courriels de la campagne d'En Marche, suivi de leur publication assortie de faux documents grossiers à deux jours du scrutin, rappelle des événements similaires survenus aux États-Unis contre la campagne d'Hillary Clinton. Ces actions s'inscrivent dans une stratégie plus large de manipulation de l'information, menée par des acteurs étatiques et soutenue par des acteurs activistes prorusses. Ces derniers, bien que moins sophistiqués techniquement, mènent des actions à forte visibilité. Ils pratiquent notamment le déni de service distribué, saturant des sites web pour les rendre temporairement inaccessibles. Le site de l'Assemblée nationale en est régulièrement victime, particulièrement lorsque la France manifeste son soutien à l'Ukraine. En mars 2024, le réseau interministériel de l'État a subi une attaque particulièrement persistante et adaptable, causant des perturbations malgré sa bonne résistance.

La menace évolue également vers des actions de sabotage d'installations critiques. Tout au long des années 2023 et 2024, nous avons ainsi constaté des attaques contre des éoliennes et des micro-barrages. Bien que ces actes ne mettent pas directement en danger la vie humaine, ils sont néanmoins préoccupants du fait de leur nature destructrice. Ces acteurs ont également tenté, sans succès, de saboter des stations d'épuration dans le but de polluer la Seine pendant les Jeux olympiques et paralympiques de Paris 2024. De telles actions visent à susciter l'anxiété, le doute et à décrédibiliser nos réponses.

Le crime organisé joue également un rôle significatif dans ces menaces. Bien que n'agissant pas nécessairement sur ordre direct de l'État russe, il bénéficie d'une certaine complaisance de sa part. Ces groupes ciblent principalement l'Occident, épargnant généralement la Russie. Certains, comme le groupe Romcom, s'adonnent à l'espionnage stratégique et au sabotage en Ukraine, en plus de leurs activités criminelles habituelles.

Les conséquences de ces attaques sont considérables. Nos hôpitaux en sont victimes de manière récurrente depuis 2019-2020, malgré les progrès réalisés dans leur protection. Les collectivités territoriales et les établissements d'enseignement supérieur sont également fréquemment ciblés, comme en témoigne la paralysie de l'Université Paris-Saclay en août dernier. Les entreprises, particulièrement les petites structures, demeurent les principales victimes de ces attaques.

Il est important de souligner que ces actions ne s'inscrivent pas nécessairement dans une stratégie concertée du crime organisé et qu'elles ne ciblent pas spécifiquement la France. Elles contribuent néanmoins à exercer une pression constante sur notre pays et l'Occident en général, affaiblissant notre économie, sapant la confiance dans nos institutions et nous rappelant notre vulnérabilité.

Ce panorama des menaces conforte le réalisme d'un scénario auquel nous nous préparons, qui est celui d'une escalade impliquant une mobilisation maximale de l'ensemble des composantes hostiles, des services étatiques aux relais activistes en passant par l'écosystème criminel, visant à paralyser de manière concertée l'ensemble des points névralgiques de notre société.

Face à ces défis, l'action de l'État demeure cruciale. Notre meilleure défense consiste à ne pas être des cibles faciles et à renforcer notre niveau de protection. La France se positionne dans le peloton de tête des États en matière de cybersécurité, grâce à une prise de conscience précoce, des moyens conséquents et un modèle efficace incarné par la création de l'ANSSI. Le législateur nous a également dotés de pouvoirs significatifs dès 2013 avec la loi de programmation militaire, anticipant les besoins de régulation du cyberespace.

Pour autant, nous ne devons pas nous reposer sur nos acquis. Le défi majeur qui se présente à nous est celui du passage à l'échelle. Si nous sommes relativement efficaces dans la protection de nos administrations et de nos entreprises stratégiques, nous devons étendre cette protection, au moins à un niveau basique, à l'ensemble de l'économie et des collectivités. Le projet de loi « résilience », dont l'examen débute à l'Assemblée, constituera un levier fondamental en ce sens. L'ensemble de l'écosystème français des entreprises et des relais territoriaux, extrêmement riche et compétent, doit se mobiliser dans un objectif de partage de l'expertise et de formation.

Au-delà de la prévention, la capacité de réponse aux attaques et leur détection sont cruciales. La France dispose d'une capacité autonome d'appréciation, de détection et de caractérisation de la menace, qui repose sur une coordination efficace entre l'ANSSI, les services de renseignement, le commandement de la cyberdéfense du ministère des armées et le ministère de l'Europe et des affaires étrangères, visant à mettre en commun les informations dont chacun dispose et à définir des options de réponse. La première est l'attribution bilatérale d'une cyberattaque, par laquelle la France enjoint à l'État attaquant de cesser ses actions. L'attribution publique, quant à elle, n'est pas proprement dissuasive mais remplit plusieurs fonctions importantes, comme l'a démontré l'action conduite la semaine dernière. Elle permet de signaler les lignes rouges, de démontrer notre capacité à détecter les violations de ces lignes et de mettre la Russie face à ses contradictions, notamment en regard de son discours à l'Organisation des Nations unies (ONU) prônant la régulation des comportements des États dans le cyberespace, et enfin de partager de la connaissance au sujet de la détection de ces modes opératoires.

Enfin, la coopération avec la justice joue un rôle crucial dans notre réponse. Bien que l'arrestation des cybercriminels soit souvent complexe en raison de leur localisation, des opérations menées en coopération internationale ont permis de démanteler des infrastructures utilisées par les attaquants. Ces actions, bien qu'elles ne mettent pas définitivement fin aux menaces, permettent de réduire temporairement la pression exercée sur nos systèmes et d'entraver les activités des groupes malveillants.

M. le président Bruno Fuchs. Je vous remercie. Je passe à présent la parole aux orateurs des groupes politiques.

M. Stéphane Rambaud (RN). L'année 2024 a vu notre pays confronté à une vague sans précédent de cyberattaques, caractérisée par une sophistication technologique accrue, l'implication d'acteurs étatiques tels que le groupe APT28 lié aux renseignements militaires russes et un ciblage stratégique de nos institutions. Ces attaques ont visé nos ministères, collectivités, entreprises de défense et même les infrastructures des Jeux olympiques. Parallèlement, des rançongiciels tels que Lockbit ont ciblé nos hôpitaux, mettant en péril la continuité des soins.

Le 11 août 2024, l'Université Paris-Saclay a subi une paralysie totale de ses services numériques à la suite d'une attaque par rançongiciel, conséquence directe d'années de sous-investissement dans la cybersécurité du monde universitaire. La généralisation des *infostealers*, capables de contourner même l'authentification à deux facteurs, démontre la vulnérabilité croissante des fondations de notre sécurité numérique.

L'ANSSI a également alerté sur une intense activité d'espionnage numérique liée aux intérêts stratégiques chinois, ciblant notamment nos opérateurs télécoms. Selon le CISA – *Certified Information Systems Auditor* ou auditeur certifié des systèmes d'information –, les attaques contre les secteurs critiques de notre pays, que sont l'énergie, la santé et la finance, devraient connaître une augmentation de 40 % cette année.

Cependant, l'évolution la plus vertigineuse reste à venir avec l'avènement de l'informatique quantique, qui menace à court terme de compromettre nos systèmes de cryptographie actuels, garants de la confidentialité de nos données militaires, industrielles et personnelles. Comme l'ont fait les États-Unis, la Chine ou l'Allemagne, il est urgent d'investir dans la cryptographie post-quantique afin de préserver notre souveraineté technologique.

Ainsi, quand la France se dotera-t-elle d'un plan national de cryptographie post-quantique pour protéger ses infrastructures les plus sensibles et stratégiques ?

M. Vincent Strubel. Cette perspective de la menace quantique concerne la possibilité qu'un ordinateur quantique, exploitant les propriétés de la mécanique quantique, parvienne à compromettre une part significative de notre cryptographie actuelle. Il convient toutefois de préciser que la concrétisation d'un tel ordinateur demeure incertaine, tant dans sa faisabilité que dans son échéance. Malgré l'intensité des travaux de recherche et développement dans ce domaine, nous ne sommes pas encore face à une réalité tangible car des verrous technologiques importants restent à lever.

Il est néanmoins impératif de nous y préparer en développant des mécanismes de cryptographie réputés résistants à l'ordinateur quantique, ce que nous appelons la cryptographie post-quantique. La France n'est pas inactive dans ce domaine, puisque notre pays bénéficie d'une expertise reconnue en cryptographie, avec des équipes de recherche de pointe. Dans les compétitions internationales visant à élaborer ces nouveaux mécanismes, notre pays s'est distingué avec des chercheurs français impliqués dans pratiquement tous les mécanismes normalisés ou en voie de l'être.

L'ANSSI travaille par ailleurs depuis plusieurs années à planifier et organiser la migration de la cryptographie déployée vers ces nouveaux mécanismes. Nos infrastructures

les plus critiques, notamment les réseaux protégeant les informations gouvernementales les plus sensibles, sont déjà à l'abri de la menace théorique de l'ordinateur quantique.

Nous collaborons étroitement avec l'industrie pour développer des gammes d'équipements et de produits de sécurité répondant à ces nouveaux besoins. Notre action s'inscrit également dans une dynamique européenne, puisque nous avons publié, avec d'autres États membres, un document préconisant que cette migration soit effectuée pour les données les plus sensibles d'ici 2030. La France codirige avec l'Allemagne et les Pays-Bas un groupe de travail européen visant à définir une politique commune dans ce domaine. Cette approche coordonnée est essentielle pour éviter des disparités de protection et des contraintes inégales pour nos entreprises au sein de l'espace européen.

Mme Eléonore Caroit (EPR). Au nom du groupe Ensemble pour la République, je tiens à saluer votre présence devant notre commission ce matin et à souligner l'action remarquable de l'ANSSI sous votre direction, dans un contexte où la menace cyber se révèle polymorphe, intense et politisée.

La reconnaissance publique par la France, le 29 avril dernier, de la responsabilité du GRU dans plusieurs attaques majeures, telles que les « Macron Leaks » ou les intrusions ciblant les Jeux olympiques, marque un tournant diplomatique significatif. Cette évolution s'inscrit fort heureusement dans un contexte de montée en puissance remarquable de l'écosystème de cybersécurité français. Les chiffres sont éloquents, avec 1 361 incidents traités en 2024, près de 60 000 audits automatisés et un accompagnement resserré de plus de 500 entités critiques pendant les Jeux olympiques. Cette capacité d'anticipation et de coordination interinstitutionnelle est précieuse mais il nous semble qu'elle doit encore être renforcée.

Dans ce contexte, comment l'ANSSI, en collaboration avec d'autres structures telles que Viginum ou la direction générale de la sécurité extérieure (DGSE), anticipe-t-elle aujourd'hui le risque de réitération de ces opérations, notamment à l'approche d'échéances électorales et dans un contexte de désinformation structurée ? Existe-t-il un protocole de coordination opérationnelle spécifique pour faire face à des menaces hybrides combinant intrusion, sabotage et manipulation de l'information ?

À cet égard, le projet de loi « résilience », dont les travaux débutent à l'Assemblée aujourd'hui même, devrait constituer une étape importante. Il ouvre un nouveau cycle, celui de la cybersécurité pensée non plus comme un simple bouclier mais comme un facteur de résilience nationale.

Ce projet de loi s'appliquera également aux entités publiques françaises localisées en dehors du territoire national, notamment nos représentations diplomatiques et consulaires, qui sont des cibles privilégiées pour les cyberattaquants. Quelles sont les priorités de l'ANSSI pour accompagner ces structures souvent isolées et confrontées à des menaces très sophistiquées ? Un dispositif renforcé de supervision ou d'alerte dédié à l'action extérieure de l'État est-il prévu ?

M. Vincent Strubel. Je tiens à exprimer ma gratitude pour cette opportunité de revenir sur le succès remarquable des Jeux olympiques et paralympiques, qui a démontré l'efficacité de notre équipe de France de la cybersécurité face aux menaces. Selon le Comité international olympique (CIO), les Jeux de Paris ont subi douze fois plus d'attaques que ceux de Tokyo, sans pour autant connaître de perturbations significatives ou de perte de confiance

dans l'organisation. Ce succès collectif s'est inscrit dans un contexte favorable, avec une préparation de plusieurs années et une mobilisation générale.

Cette réussite valide l'efficacité du modèle français, caractérisé par une coordination opérationnelle étendue entre des acteurs complémentaires. Notre quotidien dans le traitement des cyberattaques implique une collaboration étroite avec le centre de coordination des crises cyber (C4), où l'ANSSI, bien que n'étant pas un service de renseignement, travaille en synergie avec ce type d'acteurs. Cette coopération permet d'atteindre un haut niveau de confiance dans l'attribution des attaques, tout en respectant les rôles spécifiques de chaque entité.

La coopération avec des entités telles que Viginum, sur le traitement des menaces hybrides, s'est particulièrement développée à l'occasion des Jeux olympiques, qui ont fait émerger des menaces opérant simultanément dans les domaines techniques et de la manipulation informationnelle, comme l'illustre le cas des stations d'épuration. Cette situation a mis en lumière la nécessité d'une approche coordonnée pour contrer à la fois les cyberattaques potentielles et les manipulations de l'information qui les accompagnent. Notre collaboration avec Viginum s'intensifie, tout en respectant scrupuleusement les champs d'intervention et les contraintes spécifiques de chaque entité. Il est crucial de noter que l'activité de Viginum est strictement encadrée, se limitant à certains types de manipulations de l'information portant atteinte à nos intérêts fondamentaux.

Concernant les priorités de l'ANSSI, notre objectif principal est d'opérer un changement d'échelle. Nous visons à adapter notre expertise, initialement conçue pour un nombre restreint d'acteurs hautement stratégiques, à un champ d'action beaucoup plus vaste. Cette transition implique le développement de solutions plus accessibles et adaptées à une multitude d'entités telles que les collectivités, les petites et moyennes entreprises (PME), les entreprises de taille intermédiaire (ETI) et les associations, conformément au projet de loi « résilience ».

Pour réaliser cette ambition, nous mobilisons un collectif étendu comprenant les entreprises de cybersécurité françaises et européennes, les services de l'État, y compris la gendarmerie et la police, ainsi que les collectivités qui développent leurs propres capacités. Notre stratégie repose sur une logique de relais et de proximité, visant à apporter des solutions efficaces aux acteurs de moindre envergure et à construire une résilience globale. En effet, bien que la protection des 500 entités les plus stratégiques soit cruciale, la vulnérabilité du reste du tissu économique et social représenterait un risque majeur pour notre sécurité nationale.

M. Arnaud Le Gall (LFI-NFP). Nous sommes convaincus que les données les plus stratégiques de notre pays bénéficient désormais d'une protection adéquate. Comme vous l'avez souligné, le défi majeur réside dans la généralisation de cette protection, notamment pour les entreprises de taille intermédiaire et les hôpitaux. Plusieurs rapports, dont celui de M. Bastien Lachaud en 2018, ont mis en lumière ces enjeux de cyberdéfense, en particulier concernant la protection des établissements de santé.

Bien que des échéances législatives soient prévues en la matière, je considère que la législation européenne est parfois insuffisante. Je suis notamment au fait que l'un de nos collègues a contesté les accords France-États-Unis sur le régime de protection des données devant la Cour de justice de l'Union européenne, une procédure toujours en cours.

Je souhaite aborder ici la question cruciale de l'autonomie matérielle comme garantie d'une sécurité complète. Face à des menaces multidirectionnelles, dont vous avez détaillé les aspects russes, la problématique des centres de données mérite une attention particulière. Lors du sommet sur l'intelligence artificielle, des investissements considérables ont été annoncés, impliquant des entreprises comme Microsoft et un groupe émirien également impliqué dans le projet *Stargate* aux États-Unis.

Cette collaboration avec des oligopoles et monopoles américains soulève des inquiétudes car leur modèle économique repose essentiellement sur l'exploitation massive de données. Ces données, captées par milliards, tombent sous la juridiction américaine dès lors que des outils états-uniens sont utilisés. Un débat récent à l'Assemblée nationale, dans le cadre du projet de loi de simplification économique, a mis en lumière la volonté de certains de classer automatiquement tout projet de centre de données comme projet d'intérêt national majeur, sans distinction entre un projet d'Amazon et un projet visant à renforcer notre souveraineté numérique.

Aussi, quelles garanties techniques, au-delà des aspects légaux, avons-nous actuellement que les données hébergées dans des centres sur le territoire national mais gérés par des entreprises, notamment les GAFAM – Google, Apple, Facebook, Amazon et Microsoft –, restent effectivement sous le contrôle de notre souveraineté nationale ? Comment s'assurer qu'elles ne sont pas détournées à d'autres fins, sachant que la stratégie gouvernementale semble privilégier la collaboration avec ces géants du numérique pour construire notre souveraineté nationale ?

M. Vincent Strubel. La France adopte depuis longtemps une position singulière en matière d'autonomie stratégique, qui trouve désormais un écho plus favorable auprès de ses partenaires européens. Cette doctrine se manifeste dans plusieurs domaines clés tels que la maîtrise de technologies essentielles que sont la cryptographie et les capacités d'évaluation indépendantes. La souveraineté se traduit également par notre capacité à établir et à imposer nos propres règles à tous les acteurs concernés. L'Union européenne s'est montrée particulièrement efficace dans ce domaine. La directive NIS 2, transposée par le projet de loi « résilience », ainsi que le règlement Cyber Resilience Act (CRA), imposent des normes de sécurité fondamentales à tous les fournisseurs de produits numériques sur le marché européen. Ces initiatives nous permettent d'établir des exigences spécifiques, y compris envers les acteurs majeurs du secteur.

Notre doctrine d'autonomie stratégique s'étend également à l'hébergement des données. L'ANSSI a ainsi développé la qualification SecNumCloud, qui certifie qu'un fournisseur de services cloud offre des garanties élevées de sécurité, tant sur le plan technique que juridique. La politique adoptée, incarnée par la circulaire « cloud au centre » et reprise dans la loi visant à sécuriser et réguler l'espace numérique, identifie certains usages nécessitant un cloud maîtrisé et certifié SecNumCloud. Cette approche, que je considère comme pertinente, s'applique à l'État et s'étendra aux établissements publics. Il ne s'agit pas d'imposer une utilisation exclusive de centres de données européens gérés par des acteurs européens, ni de se priver de la richesse de l'offre internationale. Notre stratégie consiste plutôt à réserver, pour certains cas d'usage spécifiques et justifiés, le recours à des acteurs européens. Ces derniers, bien qu'utilisant parfois des technologies américaines, garantissent néanmoins une maîtrise et une exposition exclusive au droit européen.

M. Stéphane Hablot (SOC). Bien que la plupart des députés ne soient pas des experts techniques, nous avons la responsabilité de réfléchir, de décider et de voter sur ces questions cruciales. Vous avez parfaitement mis en lumière les enjeux et les défis liés à la cybersécurité dans notre monde profondément transformé par le numérique.

Les outils d'innovation, de croissance et de communication sont devenus des terrains d'affrontement stratégique. La cybersécurité n'est plus une option mais une nécessité absolue. Elle s'inscrit dans une logique de résilience, de solidarité européenne et de rayonnement de notre pays. Le contexte actuel est alarmant, avec une multiplication des cyberattaques visant nos institutions, nos entreprises et nos hôpitaux. Les menaces hybrides, orchestrées notamment par la Russie et la Chine, représentent un danger réel pour nos démocraties se manifestant par la désinformation, l'espionnage et le sabotage.

L'ANSSI dispose-t-elle réellement des moyens nécessaires pour anticiper et préparer notre défense ? Comme vous l'avez souligné, la meilleure défense reste la défense elle-même. Comment parvenons-nous à déjouer les stratégies de ceux qui cherchent à nous espionner ? En d'autres termes, comment espionner les espions ?

M. Vincent Strubel. Je rappelle que l'ANSSI n'est pas un service de renseignement. Pour obtenir des informations sur les méthodes d'espionnage des espions, il faudrait s'adresser aux services de renseignement eux-mêmes, même s'ils seraient probablement réticents à divulguer de telles informations.

Je suis convaincu que le modèle que nous avons mis en place est le bon. L'anticipation, qui ne se limite pas à l'espionnage des espions, implique également une compréhension approfondie de l'évolution des technologies et une projection dans l'avenir. Cela concerne des domaines tels que l'informatique quantique ou le déploiement à grande échelle de l'intelligence artificielle dans toutes nos activités.

L'ANSSI, en tant qu'entité administrative unique, abrite des laboratoires de recherche qui collaborent étroitement avec la recherche publique et privée. Nous entretenons des partenariats avec des institutions telles que l'Institut national de recherche en sciences et technologies du numérique (INRIA) et le Centre national de la recherche scientifique (CNRS) pour rester à la pointe de l'état de l'art. Cette expertise se traduit par des avis émis par des experts reconnus internationalement dans leur domaine scientifique.

Le récent sommet d'action pour l'intelligence artificielle a également été l'occasion pour l'ANSSI de se projeter dans l'accompagnement de cette évolution technologique majeure et d'en évaluer les implications en termes de cybersécurité.

Concernant la surveillance des activités des attaquants, notre modèle s'appuie sur le C4, qui réunit quotidiennement des agents de l'ANSSI et des représentants de la DGSE et de la direction générale de la sécurité intérieure (DGSI). Cette collaboration, qui s'appuie sur le strict respect des frontières entre les domaines de compétences de chacun, permet un partage d'analyses sans compromettre la confidentialité des informations brutes.

Le fait que l'ANSSI ne soit pas un service de renseignement garantit la clarté de nos missions et renforce la confiance que nous accordent les victimes de cyberattaques. Cette confiance nous permet d'intervenir auprès d'entreprises privées, de collectivités, de médias et d'autres entités, en assurant une protection rigoureuse des informations auxquelles nous devons accéder. Bien que nous ne partagions pas ces informations avec les services de

renseignement, les constats et les outils d'attaque identifiés sont confrontés avec les observations de ces derniers, traduisant notre capacité à collaborer dans le respect des attributions de chacun. Notre capacité à attribuer publiquement une cyberattaque à un service de renseignement étranger, comme nous l'avons fait récemment pour une unité du GRU basée à Rostov, démontre notre expertise et notre rigueur. Nous ne procédons à de telles attributions que lorsque nous disposons de preuves irréfutables et indépendantes.

M. Jean-Louis Roumégas (EcoS). Le 29 avril dernier, la France a franchi un cap diplomatique majeur en accusant officiellement la Russie d'être à l'origine de cyberattaques sur son territoire. Cette décision sans précédent marque un tournant dans notre posture face aux agressions numériques du Kremlin, qui cible notre pays depuis plus d'une décennie dans le cadre d'une guerre hybride. Les attaques russes ont visé un large éventail d'entités françaises, incluant des ministères, des collectivités, des administrations et des services publics. Leurs méthodes varient de l'hameçonnage à la collecte de renseignements, en passant par des actions de blocage. L'attaque contre TV5 Monde en 2015 illustre parfaitement cette stratégie : les pirates ont non seulement interrompu la diffusion des programmes mais ont également diffusé de faux messages de soutien à Daech sur les réseaux sociaux de la chaîne.

Cette cyberguerre, comme n'importe quelle guerre, vise avant tout à saper la vérité, à manipuler l'information, à diviser l'opinion publique et à influencer les processus électoraux, comme nous l'avons récemment constaté en Roumanie. L'objectif ultime est de déstabiliser nos sociétés par tous les moyens possibles. Par conséquent, garantir la sécurité du cyberespace équivaut à protéger la sécurité globale de notre pays et de notre démocratie.

Dans un contexte de tensions géopolitiques accrues entre les grandes puissances et face à l'incertitude de l'appui américain sous l'administration Trump, il est crucial de développer une cyberdéfense robuste et de construire une puissance numérique européenne indépendante. Cependant, nous sommes encore loin de cet objectif puisque le marché du cloud public, essentiel au stockage des données, reste dominé par les trois géants américains que sont Amazon, Microsoft et Google.

Bien que la France prône la création d'un cloud souverain européen, nous pouvons légitimement nous interroger sur l'adéquation des moyens alloués à cette ambition. Les 100 millions d'euros annoncés par Mme Clara Chappaz en avril semblent dérisoires face aux milliards investis aux États-Unis. Si nous avons souvent évoqué, au sein de cette commission, la construction d'une défense européenne, notamment dans le domaine de l'armement conventionnel, n'est-il pas tout aussi crucial, voire plus urgent, de nous préparer à cette guerre hybride déjà en cours ?

Ma question principale porte donc sur l'adéquation réelle de nos moyens face à l'ampleur des enjeux. Par ailleurs, d'un point de vue plus technique, bien que vous ayez souligné l'importance de la défense, ne devrions-nous pas envisager également des stratégies de contre-attaque ?

M. Vincent Strubel. Je tiens à nuancer l'emploi du terme « *cyberguerre* ». La situation actuelle ne correspond pas à un état de guerre au sens strict, comme celui que subissent les Ukrainiens. La France fait plutôt face à une contestation systématique de son modèle dans toutes ses dimensions, qu'elles soient démocratiques ou économiques. Il convient donc d'être prudent dans l'utilisation de ce terme.

Concernant l'adéquation des moyens à nos ambitions, il est évident qu'un accroissement des ressources serait bénéfique. Cependant, l'échelon européen joue un rôle crucial dans le renforcement de notre cybersécurité. La France a longtemps plaidé pour la construction d'une cybersécurité européenne, qui est aujourd'hui une réalité tangible. La précédente législature européenne a été particulièrement productive en la matière, avec l'adoption de plusieurs normes importantes telles que la directive NIS 2, le Cyber Security Act et le Cyber Resilience Act. Ce cadre réglementaire européen constitue donc un outil extrêmement efficace pour garantir notre sécurité collective et imposer des normes à tous les acteurs du marché, y compris les géants non européens. Des efforts restent néanmoins à fournir. La priorité n'est plus tant de créer de nouvelles normes que de mettre en œuvre celles qui existent déjà, de les simplifier si nécessaire et de renforcer la solidarité dans la réponse aux cyberattaques. Cette solidarité s'incarne notamment à travers le réseau CyCLONe, qui regroupe les directeurs des agences nationales de sécurité des systèmes d'information à l'échelle européenne.

Il est également crucial de soutenir l'industrie européenne dans ce domaine. Bien que des programmes non spécialisés existent déjà, nous devons intensifier les efforts au niveau européen pour développer des acteurs de proximité. La directive NIS 2, en imposant des exigences de sécurité à un large éventail d'acteurs, crée une opportunité pour l'accompagnement par des prestataires et fournisseurs de solutions industrielles, principalement européens ou français.

Quant à la question de la contre-attaque, il faut comprendre que répondre à une cyberattaque par une autre n'est pas toujours la meilleure stratégie. Saboter un hôpital dans la banlieue de Moscou en représailles à une attaque contre un hôpital français serait contraire à nos valeurs et à notre droit. De plus, l'impact d'une telle action pourrait être limité dans une société structurée différemment de la nôtre. Les leviers de réponse que nous mobilisons sont multiples. L'attribution des attaques, qu'elle soit publique ou confidentielle, est un premier pas important. Nous utilisons également tous les outils diplomatiques à notre disposition, y compris les sanctions. La France n'exclut pas, en dernier recours, le recours à des moyens militaires.

Notre doctrine est claire : ce qui se passe dans le cyberespace n'y reste pas nécessairement confiné. Les conséquences peuvent s'étendre au-delà et notre réponse s'inscrit dans le cadre du droit international et de tous leviers qui régissent relations entre États.

Mme Maud Petit (Dem). Le 29 avril 2025 marquera probablement un tournant dans l'histoire de la diplomatie française. Ce jour-là, pour la première fois, la France a officiellement et publiquement accusé un pays étranger d'avoir mené des cyberattaques contre elle. Par le biais d'un communiqué de presse du ministère des affaires étrangères, notre pays a fermement condamné la Russie, l'identifiant comme responsable de plusieurs cyberattaques. Cette démarche constitue une première historique, rompant avec la traditionnelle prudence diplomatique française dans ce domaine, où l'identification des véritables commanditaires s'avère souvent complexe.

Le mode opératoire identifié, connu sous le nom d'APT28 et actif depuis 2024, est publiquement rattaché à la Russie par l'Union européenne. Depuis 2021, ce groupe a mené des opérations de collecte de renseignements stratégiques contre de nombreuses entités en France mais également en Europe, en Ukraine et en Amérique du Nord. Dans notre pays, les cibles ont été diverses et stratégiques : ministères, collectivités territoriales, administrations, entreprises privées, une structure liée à l'organisation des Jeux olympiques de Paris 2024 et,

plus inquiétant encore, des entités du secteur de l'aérospatial et de la défense. Cette diversité des cibles souligne la nature multiforme et l'ampleur des cyberattaques auxquelles nous sommes confrontés.

Nous pourrions être confrontés à une saturation des services d'urgence, des systèmes bancaires empêchant par exemple les retraits d'espèces, ainsi que des réseaux électroniques et électriques. L'Espagne et le Portugal ont récemment connu de telles perturbations, bien que leur origine n'ait pas été attribuée à une cyberattaque. Il existe donc un risque réel d'une cyberattaque majeure, prélude potentiel à une offensive terrestre, même si nous espérons que cela ne se produira pas sur notre territoire.

Le projet de loi relatif à la résilience des infrastructures et au renforcement de la cybersécurité, dont le vote est prévu prochainement, permettra de transposer trois textes européens essentiels : la directive REC sur la résilience des entités critiques, la directive accompagnant le règlement DORA – Digital Operational Resilience Act – et la directive NIS 2. Ce projet confère un rôle prépondérant à l'ANSSI dans la mise en œuvre de ces dispositifs.

Dans ce contexte, comment l'ANSSI peut-elle encourager l'adoption de solutions françaises de cybersécurité, réduisant ainsi notre dépendance aux technologies étrangères et garantissant notre sécurité et notre souveraineté numérique ? Par ailleurs, quelles sont vos attentes spécifiques envers les opérateurs téléphoniques, acteurs cruciaux dans la protection des infrastructures critiques et de nos communications ?

M. Vincent Strubel. Les opérateurs de communications électroniques sont des acteurs majeurs et réguliers en matière de cybersécurité. Leur position les rend particulièrement exigeants et en fait des cibles privilégiées pour les cyberattaquants les plus sophistiqués au monde. L'ANSSI collabore étroitement avec eux depuis de nombreuses années pour faire face à ces menaces. Ces opérateurs sont également des partenaires essentiels dans l'identification des menaces. Grâce aux dispositions législatives dont nous bénéficions, nous pouvons leur demander d'informer leurs clients victimes de cyberattaques, notamment lorsque nous sommes confrontés à des incidents touchant des milliers d'utilisateurs simultanément. Cette coopération s'avère cruciale car les opérateurs ont la capacité d'identifier leurs clients à partir des adresses IP. Notre collaboration avec les opérateurs de télécommunications est constante et évolutive car nous devons sans cesse nous adapter aux progrès des cyberattaquants. Les opérateurs jouent pleinement leur rôle dans cette lutte permanente.

Concernant l'écosystème français et sa mobilisation pour le déploiement de NIS 2 ou le renforcement de notre souveraineté, le rôle principal de l'ANSSI consiste à définir les exigences de sécurité. Je suis convaincu que le cadre offert par NIS 2, intégré dans le projet de loi « résilience », représente une opportunité majeure que l'écosystème français a su saisir et pour laquelle il se prépare activement. Cette directive offre l'occasion de déployer des solutions de cybersécurité et un accompagnement de proximité, domaines dans lesquels la France dispose d'atouts considérables, tant au niveau national qu'européen. Notre expérience en la matière s'est notamment illustrée dans la préparation des Jeux olympiques et paralympiques, qui a servi de test pour l'accompagnement de structures plus modestes, telles que des fédérations sportives et des petites collectivités. Nous avons mobilisé le tissu de prestataires de cybersécurité nationaux à une échelle sans précédent, comme nous l'avions fait pour les parcours de cybersécurité dans le cadre du plan France relance. Ces initiatives nous ont permis d'accompagner près d'un millier de petites structures publiques, incluant des

collectivités, des hôpitaux et des établissements d'enseignement, en nous appuyant sur l'industrie nationale et européenne.

Cette démarche est facilitée par notre cadre de certification, qui permet à l'ANSSI de qualifier des prestataires de services en cybersécurité. Ces acteurs, dont les compétences sont presque équivalentes aux nôtres, constituent des partenaires quotidiens dont nous pouvons garantir à la fois l'expertise et la fiabilité. Nous disposons ainsi d'un catalogue complet d'offres recommandées par l'ANSSI, bénéficiant de ce que nous appelons des visas de sécurité.

Mme Laetitia Saint-Paul (HOR). Comme vous l'avez rappelé et contrairement à l'adage, la meilleure défense n'est pas l'attaque mais bien la défense elle-même. Il est crucial de souligner que la France n'adoptera en aucun cas les méthodes de nos adversaires, excluant catégoriquement toute attaque contre des infrastructures civiles telles que des hôpitaux, quelle que soit la société visée. Notre stratégie demeure résolument défensive. Malgré les révélations des « Kremlin Leaks » indiquant que la Russie consacrerait plus de 1 milliard d'euros à des opérations d'ingérence étrangère, la France ne s'engagera pas dans la création de « fermes à trolls ». Passionnée par ce sujet, je mène actuellement avec mon collègue Alain David une mission d'information pour la commission, relative à l'irruption de l'intelligence artificielle dans les ingérences étrangères. J'ai élargi cette réflexion au nom de l'Union interparlementaire (UIP) en examinant l'utilisation de l'ingérence étrangère par les terroristes et les moyens de lutter contre le terrorisme.

Nous venons également d'adopter la loi sur le narcotrafic, dont le rapport sénatorial comporte un volet substantiel sur l'utilisation de l'intelligence artificielle par les narcotrafiquants et le crime organisé en général. Dans ce contexte, je souhaiterais connaître votre analyse sur l'utilisation de l'IA par les acteurs étatiques, le crime organisé et les activistes.

Au fil de nos auditions, vous êtes le premier à avoir établi des liens entre les acteurs étatiques et la criminalité organisée. La plupart des directions que nous avons rencontrées ont généralement affirmé l'absence de convergence ou de zone grise entre ces entités. Vous avez, au contraire, insisté sur ce point. Pourriez-vous nous apporter des éclaircissements à ce sujet ?

M. Vincent Strubel. S'agissant du lien entre les acteurs étatiques et le crime organisé, je tiens à préciser que je ne dispose d'aucun élément probant indiquant une coordination ou une subordination directe du crime organisé au pouvoir politique russe. Il est cependant légitime de s'interroger sur le fait qu'une part significative des acteurs du cybercrime soit localisée en Russie et ne soit pas inquiétée par les autorités russes. Il paraît peu probable que cela résulte d'une incapacité des services répressifs russes à les identifier ou à les appréhender. Ces individus sont souvent connus et font l'objet de mandats internationaux ou de sanctions. L'absence d'action à leur encontre laisse supposer l'existence de contreparties, dont la nature reste à déterminer. Cette situation nous incite à envisager l'hypothèse d'une coordination potentielle, sans pour autant pouvoir l'affirmer ou la démontrer formellement.

S'agissant du lien entre l'intelligence artificielle et la cybersécurité, ce sujet doit être abordé avec objectivité, en évitant les fantasmes souvent associés aux technologies émergentes. Dans le domaine de la cybersécurité, l'utilisation de l'IA par les cyberattaquants ne constitue pas, à mon sens, un changement de paradigme fondamental. Elle ne lève pas de verrou majeur qui empêcherait les attaques mais facilite certainement leur mise en œuvre,

comme elle le fait dans d'autres domaines. Il est important de souligner que l'IA bénéficie également aux défenseurs, ce qui en fait une technologie duale. L'enjeu principal réside, une fois encore, dans le rythme d'appropriation de cette technologie. Notre objectif est que les défenseurs s'approprient les apports de l'IA aussi rapidement que possible, malgré des contraintes différentes de celles des attaquants. Nous utilisons déjà largement l'IA dans nos activités quotidiennes pour détecter et caractériser les attaques et nous devons poursuivre dans cette voie.

La question plus large de l'apport de garanties de cybersécurité sur l'IA est un sujet complexe sur lequel nous avons publié, à l'occasion du sommet dédié, une analyse de risques visant à objectiver les enjeux et à dépasser les discours parfois irrationnels. Ce rapport, cosigné par dix-neuf de nos partenaires internationaux, s'efforce d'identifier les risques liés à l'utilisation de l'IA, les réponses possibles ainsi que les domaines nécessitant des recherches supplémentaires.

Un défi majeur consiste à favoriser le dialogue entre le monde de l'IA et celui de la cybersécurité, qui ne communiquent pas naturellement. Nous avons organisé, lors du sommet pour l'IA, un exercice de crise à grande échelle réunissant 250 experts des deux domaines, issus de tous les pays participants. Cet exercice les a confrontés à un scénario hypothétique de cyberattaques ciblant des implémentations d'intelligence artificielle, les amenant à réfléchir collectivement aux réponses possibles et, idéalement, aux moyens de prévention.

Bien que nous n'ayons pas toutes les réponses sur ces sujets, il est donc crucial de souligner que nous disposons déjà de certaines solutions et que nous identifions clairement les domaines où des recherches supplémentaires sont nécessaires.

M. Jean-Paul Lecoq (GDR). Cette audition, qui aborde un sujet qui suscite à la fois la curiosité, l'inquiétude et l'intérêt de nos concitoyens, se révèle passionnante. Il me semble essentiel de vulgariser ces questions afin de les rendre accessibles au plus grand nombre.

Nous avons récemment débattu, au sein du conseil municipal du Havre, de l'utilisation des machines à voter et des risques de cyberattaques les concernant. Bien que le maire ait souhaité rassurer le conseil municipal en affirmant l'impossibilité d'intrusion dans ces systèmes, les citoyens peuvent légitimement s'inquiéter, compte tenu des précédents comme le logiciel *Pegasus* ou l'attaque au Liban ayant provoqué l'explosion de matériel. Ces incidents soulèvent la question de vulnérabilités potentiellement intégrées en amont, dès la conception des équipements.

Je m'interroge donc sur les garanties dont nous disposons concernant les composants, tels que les microprocesseurs, provenant d'autres pays. Comment pouvons-nous nous assurer de l'absence de pièges ou d'attaques prépositionnées susceptibles d'être activés à un moment donné ?

Par ailleurs, en tant que membres de la commission des affaires étrangères, nous sommes fréquemment amenés à examiner des traités internationaux. Dans ce contexte, où en sommes-nous concernant l'adaptation de la charte des Nations unies à ce nouveau monde numérique ? Vous avez indiqué que la Russie interpelle les Nations unies sur la nécessité de réglementer et de réguler ces domaines. Quelle est la position de la France à cet égard ? Quels messages porte-t-elle au sein des Nations unies et auprès des membres permanents du Conseil de sécurité ? Quelles avancées avons-nous obtenues dans ce domaine ?

M. Vincent Strubel. Je vous remercie de souligner l'importance de la vulgarisation. J'ai la conviction profonde que, bien que la cybersécurité reste un domaine d'expertise pointue, elle constitue également un enjeu sociétal majeur qui doit être compris par le plus grand nombre. Cette compréhension collective participe à la résilience de notre société face aux cybermenaces, qu'il s'agisse de manipulation de l'information ou de cyberattaques. Elle permet également d'éviter de devenir la victime de cyberattaquants qui, parfois, notamment dans le domaine de l'activisme, exagèrent considérablement les conséquences de leurs actions pour susciter la peur au-delà de leurs réelles capacités.

Concernant les relations internationales, je me dois de préciser que les diplomates seraient plus à même d'en parler en détail. La France a eu l'intelligence de s'organiser également dans ce domaine en nommant des « cyberdiplomates », notamment un ambassadeur pour le numérique. Une direction spécifique au Quai d'Orsay se consacre largement à ces questions et collabore quotidiennement avec nous, y compris sur l'attribution potentielle des attaques.

La France a adopté une position claire dans les enceintes internationales, y compris à l'ONU, plaidant pour un comportement responsable des États. Dans un domaine connexe, nous œuvrons à la lutte contre la prolifération des outils d'attaque. Récemment, nous avons réuni plusieurs partenaires internationaux dans le cadre du processus de Pall Mall, une initiative lancée conjointement avec nos homologues britanniques dont l'objectif est de lutter contre la prolifération d'outils de type *Pegasus* et de définir des normes de comportement responsable quant à l'utilisation de ces technologies.

La France se positionne donc comme un fervent défenseur des comportements responsables dans le cyberespace, y compris au sein des Nations unies. Le débat international sur ce sujet se heurte principalement à des divergences concernant la définition et l'étendue de ce comportement responsable. Certains États, moins avancés que le nôtre dans leur consolidation démocratique, considèrent notamment que la censure des médias critiques envers des régimes étrangers fait partie de cette responsabilité. La France s'oppose catégoriquement à cette vision et défend une conception plus restrictive de la cyberattaque. Nous condamnons fermement les attaques contre des infrastructures critiques comme les hôpitaux, tout en réaffirmant notre attachement indéfectible à la liberté de la presse et d'expression, piliers fondamentaux de notre démocratie.

Malgré ces divergences, il est impératif de poursuivre ces discussions. La cybersécurité est abordée dans diverses enceintes internationales telles que l'Organisation de coopération et de développement économiques (OCDE), le G7 et, bien évidemment, l'Union européenne, où nous avons développé une approche collective de la cybersécurité, ce qui constitue une avancée significative.

M. Lionel Vuibert (NI). Je souhaite aborder la question cruciale des cyberattaques visant les collectivités territoriales, qui se trouvent souvent démunies face à ces menaces. Prenons l'exemple de Charleville-Mézières, une commune située dans mon département et victime d'une attaque en 2020. Les conséquences ont été considérables puisque les coûts directs s'élèvent à près d'un demi-million d'euros sur trois ans et demi, sans compter le temps investi par le personnel.

Dans ce contexte, l'ANSSI envisage-t-elle de renforcer sa collaboration avec les collectivités territoriales ? Cette réflexion pourrait s'étendre aux PME, également vulnérables.

Pouvons-nous espérer une approche plus territorialisée de la cybersécurité publique, notamment en matière de prévention, de gestion de crise et de reconstruction post-attaque ?

M. Vincent Strubel. Les collectivités territoriales, tout comme les établissements de santé et les PME ou les ETI, sont effectivement des cibles récurrentes de cyberattaques. Ces attaques ne proviennent pas nécessairement de services de renseignement étrangers sophistiqués mais plutôt d'une menace systémique émanant du crime organisé et d'activistes qui ciblent les entités les plus vulnérables. La réalité est que ces structures, en raison de leur taille et de leurs ressources limitées, ne peuvent pas devenir des expertes en cybersécurité.

Notre mission est donc de développer des solutions adaptées pour renforcer leur résilience, sans pour autant viser à contrer les attaquants les plus sophistiqués du monde. L'ANSSI s'efforce de simplifier ses messages et de proposer des services plus accessibles. Nous avons récemment lancé le portail *Mes services cyber* pour rendre notre offre de services et notre documentation plus compréhensibles et accessibles aux structures de taille modeste.

Le projet de loi « résilience » imposera des exigences de sécurité élémentaires aux intercommunalités, régions et départements, acteurs suffisamment importants et souvent responsables de la mutualisation des ressources. Ces mesures, bien que basiques, visent à offrir une protection significative contre les menaces courantes.

Nous collaborons également étroitement avec les échelons locaux, notamment au niveau régional, en soutenant la création de centres de réponse à incidents régionaux – *Computer Security Incident Response Team* ou CSIRT. Ces centres, financés en partie par le plan de relance et bénéficiant de notre expertise méthodologique, sont devenus des partenaires quotidiens de l'ANSSI. Ils ne remplacent pas notre agence mais traitent un large éventail d'incidents quotidiens et de victimes de proximité, apportant une compréhension approfondie de l'écosystème local et s'intégrant dans les initiatives de développement économique régional.

Nous poursuivons notre collaboration avec divers relais sur le terrain, tels que la gendarmerie, les chambres de commerce et d'industrie et les fédérations professionnelles. Cette coopération s'étend à la co-construction du projet de loi « résilience » et au-delà. Notre objectif est de constituer un réseau élargi, une véritable équipe de France de la cybersécurité, qui s'étend au-delà des opérateurs d'importance vitale que nous accompagnons depuis longtemps et des prestataires de services que nous qualifions ou certifions. L'enjeu majeur des prochaines années sera de diffuser cette expertise dans tous les territoires.

M. le président Bruno Fuchs. Je donne à présent la parole aux collègues qui souhaitent intervenir ou vous interroger à titre individuel.

M. Michel Guiniot (RN). Ma première question porte sur l'objectif n° 3 de l'axe n° 1 de votre plan stratégique 2025-2027, qui vise à amplifier et coordonner la réponse cyber face à la massification de la menace, notamment par le déploiement d'un nouveau système de supervision interministérielle. Pourriez-vous nous fournir davantage de détails sur ce projet ?

Ma seconde interrogation concerne les risques liés aux intelligences artificielles génératives, un sujet qui suscite l'inquiétude de nombreux scientifiques. Ces derniers mois, nous avons assisté à l'émergence d'intelligences artificielles de plus en plus performantes en matière de piratage informatique, laissant présager que les informaticiens humains pourraient bientôt être dépassés par ces IA moins contraintes. Dans ce contexte, et considérant

l'importante levée de fonds annoncée par le président de la République pour soutenir le développement de l'IA, comment l'ANSSI, en tant que garante de la protection de la nation, envisage-t-elle de nous prémunir contre le développement de logiciels autonomes malveillants basés sur l'intelligence artificielle ? Cette préoccupation est d'autant plus pressante que les fonds alloués au développement de la cybersécurité ne semblent pas avoir été augmentés en conséquence.

M. Vincent Strubel. La supervision interministérielle constitue l'un de nos axes de développement prioritaires. Si j'ai largement évoqué la nécessité d'un changement d'échelle pour déployer une cybersécurité de base sur l'ensemble du territoire, touchant tous nos concitoyens ainsi que le tissu des PME et des collectivités, nous ne devons pas pour autant négliger notre cœur de métier historique qui est la protection de l'État et des entreprises les plus stratégiques.

Dans cette optique, l'ANSSI supervise les réseaux de l'État et coordonne la supervision des réseaux des opérateurs d'importance vitale, sans l'effectuer elle-même. Nous avons engagé un vaste projet de refonte de notre supervision des réseaux de l'État, visant à développer des mutualisations utiles pour générer des économies et gagner en efficacité. Ce projet nous occupera pendant plusieurs années, en collaboration notamment avec la direction interministérielle du numérique (Dinum), qui gère certaines infrastructures mutualisées. Ces projets permettent non seulement de réaliser d'importantes économies mais également d'améliorer notre efficacité en matière de supervision et de réponse aux incidents.

Parmi les plus grandes réussites numériques de l'État ces dix dernières années figure le réseau interministériel de l'État (RIE), qui nous offre un point de supervision particulièrement adapté et nous permet de réagir efficacement. Il a d'ailleurs démontré sa résilience face à une attaque de déni de service en mars 2024. Nous continuerons à investir, en étroite collaboration avec la construction d'un socle informatique mutualisé pour l'État, afin de capitaliser sur cette base et développer nos capacités de supervision.

Concernant l'intelligence artificielle et les risques liés aux logiciels autonomes, j'ai déjà souligné que l'IA facilitera la tâche tant des attaquants que des défenseurs. Je ne perçois pas de rupture majeure dans les scénarios souvent évoqués, prédisant que l'IA décuplerait les capacités des attaquants au point de provoquer un « cyberarmageddon ». Nous en revenons rapidement à l'idée que l'IA permettra de créer des faux messages plus convaincants, incitant les utilisateurs à cliquer et ainsi infecter leur ordinateur. Bien que ce phénomène commence à s'observer, force est de constater que même des messages mal rédigés parviennent déjà à tromper certains utilisateurs. L'IA ne lève donc pas un verrou technologique fondamental dans ce domaine.

Certes, l'IA permettra des attaques à grande échelle mais les attaquants n'ont pas attendu son avènement pour automatiser et massifier leurs opérations. Elle facilitera leur tâche sans pour autant changer radicalement la donne. Quant aux risques posés par des logiciels autonomes, nous avons publié un rapport d'évaluation lors du sommet sur l'IA et continuerons à travailler sur ce sujet en évolution rapide, en étroite collaboration avec la recherche. L'essentiel est d'objectiver ces risques et de ne pas tout mélanger dans le discours sur l'IA, qui tend à amalgamer des problématiques diverses telles que la cybersécurité, l'éthique, la fiabilité et même des scénarios quasiment métaphysiques, à la *Terminator*, de rébellion des machines contre l'humanité.

Notre approche consiste à décomposer ce vaste problème en sous-problèmes plus gérables, que nous traitons individuellement. Nous nous concentrons sur l'aspect cybersécurité de manière objective et rationnelle, sans ignorer les autres dimensions mais en cherchant à apporter de l'objectivité dans chacune d'elles. C'est dans cet état d'esprit que travaillent toutes les administrations françaises mobilisées sur ces sujets, y compris la ministre en charge de l'intelligence artificielle que vous avez récemment auditionnée.

Mme Laetitia Saint-Paul (HOR). Monsieur le directeur général, vous avez évoqué la perplexité des victimes, qui se demandent pourquoi elles ont été ciblées. J'ai effectivement constaté cette perplexité dans ma circonscription, ainsi que la honte ressentie par les entreprises ayant subi une cyberattaque. Cette honte entrave le partage d'expérience, les entreprises craignant d'effrayer leurs clients ou d'entacher leur réputation. Vous avez indiqué que l'objectif actuel de l'ANSSI est d'étendre ses efforts à l'ensemble de la société et des entreprises. Je me demande donc si la question pertinente est encore : serons-nous victimes d'une cyberattaque ? Ne devrions pas plutôt nous demander : quand serons-nous victimes d'une cyberattaque ?

M. Vincent Strubel. Je confirme que la question pertinente est effectivement quand serons-nous victimes d'une cyberattaque ?

La perplexité des victimes est une réalité que nous constatons quotidiennement. À l'ANSSI, des agents travaillent en permanence sur le standard 3218, dédié au traitement des déclarations de cyberattaques. Leur rôle combine conseil technique, coordination de la réponse aux incidents et, bien souvent, soutien psychologique car ils sont fréquemment confrontés à des interlocuteurs en détresse, une cyberattaque constituant indéniablement un choc psychologique majeur.

La meilleure réponse face à cette situation est la préparation. La gestion de crise cyber nécessite une préparation spécifique, distincte de la gestion de crise classique. Nous avons constaté des retours extrêmement positifs à la suite des entraînements mis en place. Cette approche a été déployée en priorité pour protéger les hôpitaux, compte tenu des enjeux vitaux en jeu, et s'est révélée efficace. Nous avons généralisé ces démarches d'entraînement dans l'ensemble des établissements hospitaliers publics, y compris au niveau des équipes de direction, pour simuler une crise cyber et apprendre à y réagir.

Bien que cela ne résolve pas entièrement le problème ni n'empêche les attaques de se produire, cette préparation permet d'en limiter considérablement les conséquences. C'est grâce à cela qu'aujourd'hui, bien que des attaques contre des hôpitaux persistent, nous observons beaucoup moins de paralysies complètes comme celles constatées entre 2020 et 2022, où les attaques détruisaient l'intégralité de l'infrastructure informatique. Désormais, la réaction est plus rapide et efficace. Cela ne signifie pas pour autant que nous devons relâcher nos efforts et nous continuerons à travailler dans le cadre du plan du ministère de la santé pour renforcer leur niveau de sécurité et les protéger contre les attaques.

Une bonne réaction est cruciale et porte ses fruits, comme nous l'avons constaté dans notre préparation pour les Jeux olympiques. Nous appliquerons également cette approche dans l'accompagnement que nous mettrons en œuvre autour de la directive NIS 2 auprès de l'ensemble du tissu des petits acteurs, pour les aider à se préparer efficacement.

Je partage votre avis sur le fait qu'il ne faut plus avoir honte, aujourd'hui, d'être victime d'une cyberattaque. La législation nous a aidés en ce sens avec le règlement général de protection des données (RGPD) de l'Union européenne, qui a instauré une forme d'obligation de notification, et la directive NIS 2, qui introduira également une obligation de notification des incidents, sans nécessairement les rendre publics mais en incitant à en parler. Le fait que chacun communique sur les incidents dont il a été victime aide l'ensemble des victimes à s'exprimer plus librement sur le sujet.

Les attaques de type sabotage ou rançongiciel ont paradoxalement contribué à sensibiliser le public à la cybersécurité car leurs effets sont immédiatement visibles, contrairement à l'espionnage qui reste souvent invisible. J'estime qu'il est crucial d'encourager les victimes de ces attaques à témoigner. Cette approche s'est avérée particulièrement efficace dans le secteur hospitalier, dans la mesure où le témoignage d'un directeur d'hôpital ayant vécu une cyberattaque a un impact bien plus fort et concret que celui d'un technocrate parisien tel que moi, éloigné des réalités du terrain. Cette stratégie de mobilisation des victimes pour sensibiliser s'applique également aux collectivités territoriales.

M. Bertrand Bouyx (HOR). J'aimerais approfondir le sujet de la cryptographie quantique en m'intéressant plus particulièrement à la situation française concernant les processeurs quantiques. Une célèbre entreprise américaine communique régulièrement sur les performances de ses processeurs quantiques, qui atteignent aujourd'hui jusqu'à 150 qubits. Pourriez-vous nous éclairer sur l'état d'avancement de la France dans ce domaine ? Plus précisément, quelles sont les perspectives d'évolution, sachant que ces processeurs quantiques sont appelés à révolutionner l'intelligence artificielle ?

M. Vincent Strubel. Il convient tout d'abord de relativiser certaines affirmations, qui sont souvent guidées par des logiques marketing ou de levée de fonds. Sans remettre en cause la légitimité de ces démarches, il faut noter qu'à l'heure actuelle, nous n'avons pas encore atteint le stade d'un ordinateur quantique capable d'impacter significativement la cryptographie.

Parmi les différents types de calculs réalisables par un ordinateur quantique, ceux qui concernent particulièrement la cryptographie, notamment l'algorithme de Shor, sont encore hors de portée des capacités actuelles des processeurs quantiques mis en avant sur le marché. Des verrous technologiques importants restent à lever.

Concernant l'intelligence artificielle, je considère qu'il s'agit davantage d'une évolution progressive que d'une rupture brutale. En revanche, l'avènement d'un ordinateur quantique significatif du point de vue de la cryptographie représenterait un changement radical et immédiat. Le jour où un tel ordinateur verra le jour, toute la cryptographie non résistante au quantique s'effondrera instantanément. Nous devrons alors nous préoccuper non seulement de la protection des secrets futurs mais également de tous ceux protégés antérieurement par des mécanismes cryptographiques devenus obsolètes.

Bien que l'avènement prochain d'un tel ordinateur me semble improbable, l'horizon temporel se situe probablement autour d'une dizaine d'années. Ce délai correspond à la fois au temps nécessaire pour lever les verrous technologiques et à celui requis pour déployer à grande échelle une nouvelle cryptographie. Il est donc impératif de s'y préparer dès maintenant, malgré la difficulté à se projeter face à une menace hypothétique à moyen terme.

M. Jean-Louis Roumégas (EcoS). Permettez-moi de revenir sur le risque de cyberguerre, que vous semblez avoir minimisé. Est-il possible que la principale menace ne réside pas tant dans les attaques numériques directes ou les destructions de systèmes mais plutôt dans la manipulation de nos processus démocratiques ? Il n'est en effet plus nécessaire de mener une guerre conventionnelle lorsque l'élection de dirigeants favorables à ses intérêts peut être favorisée.

Prenons l'exemple des États-Unis, où un simple changement de président a déjà permis à la Russie d'obtenir des résultats significatifs, ou encore de l'élection de George Simion en Roumanie. Certains craignent même une possible ingérence en France, avec l'hypothèse d'une élection d'un dirigeant du Rassemblement national. Dans ce contexte, les puissances étrangères telles que la Russie ou les États-Unis n'auraient pas besoin de recourir à des cyberattaques directes puisqu'il leur suffirait de favoriser l'élection de leurs alliés. Sommes-nous réellement protégés contre ce type de menace, qui me semble être le plus critique ?

M. Vincent Strubel. Sans m'engager dans une appréciation politique de la situation, je tiens à clarifier mon propos concernant l'usage du terme de guerre. Ma réserve ne vise pas à minimiser la gravité de la situation mais plutôt à souligner que le mot évoque un affrontement armé conventionnel, dans lequel le cyber peut certes jouer un rôle. L'Ukraine, par exemple, subit simultanément des attaques de missiles de croisière, de drones et des cyberattaques, ce qui n'est pas le cas de la France. C'est pourquoi je préfère parler de logique de contestation et de confrontation plutôt que de guerre. Cela ne signifie pas que nous sous-estimons la gravité des attaques contre nos infrastructures critiques, nos hôpitaux ou nos processus démocratiques. Ces menaces nous préoccupent grandement et nous ne sommes pas démunis face à elles.

Depuis plusieurs années en effet, l'ANSSI se mobilise particulièrement autour des séquences électorales, en sécurisant notamment les infrastructures numériques associées aux élections, qui restent heureusement assez limitées en France, le vote étant majoritairement effectué sur papier. Nous surveillons étroitement ces systèmes, y compris le vote par internet des Français de l'étranger pour certains scrutins spécifiques.

En tant qu'émanation de l'Exécutif, l'ANSSI intervient avec la plus grande prudence dans l'accompagnement des processus électoraux. Lors des séquences électorales, nous nous mettons à la disposition du juge de l'élection, qu'il s'agisse du Conseil constitutionnel, du Conseil d'État ou de la commission spécifique pour le contrôle de l'élection présidentielle. Nous partageons toutes nos observations concernant les cyberattaques potentiellement liées au contexte électoral, non seulement avec nos autorités politiques mais également avec le juge de l'élection.

L'ANSSI propose par ailleurs systématiquement ses services aux partis politiques et aux équipes de campagne avant chaque séquence électorale, sans toutefois les imposer car cela serait contraire aux principes démocratiques qui s'imposent à un organisme étatique. Les partis politiques constituent potentiellement un maillon faible car leurs infrastructures numériques s'apparentent davantage à celles d'une PME ou d'une start-up, ce qui rend leur sécurisation plus complexe.

Nous restons donc à la disposition des partis politiques et de la représentation nationale, en menant des actions de sensibilisation en collaboration avec les services de l'Assemblée nationale. Notre intervention dans ce domaine est effectuée avec toutes les

précautions nécessaires, nous positionnant comme une ressource à votre disposition sans rien imposer, afin de ne pas interférer dans un jeu politique qui n'est pas le nôtre.

M. le président Bruno Fuchs. Pour conclure, pourriez-vous nous éclairer brièvement sur les initiatives de l'Azerbaïdjan ? Ce pays est apparu depuis quelques mois sur la scène internationale comme un acteur potentiel d'ingérence ou d'influences déloyales. Que pouvez-vous nous en dire de manière plus précise et mesurée, au-delà des informations relayées par les médias ?

M. Vincent Strubel. Dans le domaine qui est le mien, à savoir les cyberattaques et les intrusions dans les systèmes d'information, l'Azerbaïdjan ne se distingue pas particulièrement comme un acteur majeur. Cependant, d'après les informations provenant de Viginum, cet État a mené des actions avérées dans le domaine de la manipulation de l'information, qui ont été publiées et dénoncées par la France. Si l'Azerbaïdjan intervient donc dans ce champ spécifique, nous n'avons pas, en revanche, identifié de mode opératoire clairement attribuable à des cyberattaques azerbaïdjanaises.

M. Arnaud Le Gall (LFI-NFP). Dans le même ordre d'idées, nous évoquons fréquemment la Russie, la Chine et, dans notre domaine, les États-Unis, mais nous négligeons souvent l'Inde. Bien qu'il ne s'agisse pas de cyberattaques au sens strict, ce pays s'est illustré par des opérations de manipulation de l'information visant à modifier son image en Europe. La plus importante attaque concertée de la dernière décennie provenait d'ailleurs de serveurs indiens. Bien que ne ciblant pas nécessairement des enjeux hautement stratégiques, cette attaque s'est distinguée par son ampleur massive.

M. Vincent Strubel. Je tiens à rester prudent dans mes commentaires concernant la manipulation de l'information car ce domaine ne relève pas directement de mes compétences, ni nécessairement de celles de Viginum. Le champ d'action de Viginum est en effet strictement encadré et se limite aux opérations artificiellement amplifiées par des États portant atteinte à nos intérêts fondamentaux. La simple publicité ne constitue pas nécessairement une manipulation de l'information. La définition de ce qui constitue une manipulation grave est subtile et Viginum veille naturellement à ne pas outrepasser le cadre légal de ses missions.

Je tiens toutefois à préciser, puisque nous avons largement évoqué les menaces russes, que la Russie n'est évidemment pas le seul pays à mener des cyberattaques. Le panorama des menaces publié par l'ANSSI met également en évidence des acteurs réputés liés à la Chine ou à l'Iran comme étant très actifs dans ce domaine. Nous avons publié et cité les éléments les plus saillants mais cela n'épuise certainement pas l'ensemble du paysage des menaces.

Il est important de souligner que l'ANSSI ne se focalise pas *a priori* sur une menace particulière. Notre vocation est de défendre nos systèmes d'information les plus critiques contre tout type de menace, avec des mesures de précaution qui ne sont pas spécifiques à un type d'attaque en particulier. Nous adoptons une approche sans complaisance ni aveuglement vis-à-vis d'autres attaques potentielles, même si celles-ci ne sont pas aussi prégnantes que celles que nous avons évoquées.

M. le président Bruno Fuchs. Nous constatons que votre rôle, aussi discret qu'essentiel, contribue à sécuriser les installations nationales tout en veillant à la sécurité et à la souveraineté de notre pays. Nous relevons également une dimension transnationale dans la défense, soulignant l'importance cruciale de rechercher des partenariats et des actions

conjointes avec d’autres acteurs européens, voire d’autres continents partageant notre vision de la gouvernance.

***

La séance est levée à 10 h 45.

———

Membres présents ou excusés

Présents. – M. Pieyre-Alexandre Anglade, M. Bertrand Bouyx, M. Jorys Bovet, M. Jérôme Buisson, Mme Eléonore Caroit, M. Sébastien Chenu, Mme Sophia Chikirou, M. Pierre Cordier, Mme Christelle D'Intorni, M. Alain David, Mme Dieynaba Diop, Mme Stella Dupont, Mme Christine Engrand, M. Marc de Fleurian, M. Bruno Fuchs, M. Julien Gokel, M. Michel Guiniot, M. Stéphane Hablot, Mme Marine Hamelet, Mme Sylvie Josserand, Mme Brigitte Klinkert, M. Xavier Lacombe, M. Arnaud Le Gall, M. Jean-Paul Lecoq, Mme Élisabeth de Maistre, Mme Alexandra Masson, Mme Sophie Mette, Mme Maud Petit, M. Jean-François Portarrieu, M. Stéphane Rambaud, M. Franck Riester, M. Jean-Louis Roumégas, Mme Laetitia Saint-Paul, Mme Liliana Tanguy, M. Lionel Vuibert

Excusés. – Mme Nadège Abomangoli, M. Hervé Berville, M. Pierre-Yves Cadalen, M. Olivier Faure, M. Perceval Gaillard, Mme Pascale Got, Mme Amélia Lakrafi, Mme Marine Le Pen, M. Laurent Panifous, Mme Mathilde Panot, M. Davy Rimane, Mme Laurence Robert-Dehault, Mme Marie-Ange Rousselot, Mme Sabrina Sebaihi, Mme Michèle Tabarot, M. Laurent Wauquiez

Assistait également à la réunion. – Mme Constance Le Grip