ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Jeudi
30 avril 2026
Séance de 9 heures

Compte rendu n° 35

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures dix.

M. le président Philippe Latombe. Les missions de l'Anssi sont au cœur des préoccupations de notre commission d'enquête. Quelle est votre analyse de la vulnérabilité des administrations publiques et, plus généralement, de l'économie française aux solutions et technologies numériques extra-européennes ? Pouvez-vous décrire l'action que mène l'Anssi pour certifier des solutions souveraines ?

Je vous prie tout d'abord de déclarer tout intérêt public ou privé de nature à influencer vos déclarations. Je vous rappelle également que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité, rien que la vérité. Je vous invite donc à lever la main droite et à dire « je le jure ».

(M. Vincent Strubel prête serment.)

M. Vincent Strubel, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Bien que le mot ne figure pas strictement dans l'intitulé de votre commission, et bien que je professe régulièrement de me méfier de ce terme, je comprends que derrière l'ensemble de ces sujets se posent des questions de souveraineté. J'axerai donc mon propos liminaire sur les trois déterminants que j'identifie généralement pour notre souveraineté numérique, en précisant à chaque fois leur intersection avec les missions de l'Anssi puisque cette dernière n'est pas, à proprement parler, en charge de la souveraineté numérique, même si elle y contribue. J'adopterai cet angle de lecture lié à nos dépendances extra-européennes ou, plus généralement, à nos dépendances numériques, car je pense que le seul critère de lecture européen ou non européen n'est pas toujours le plus significatif.

Je rappelle rapidement, à titre d'introduction, que du point de vue de l'Anssi, la souveraineté numérique recouvre trois enjeux. Le premier est la cybersécurité au sens propre, c'est-à-dire notre capacité à ne pas être une victime facile de cyberattaques. Lorsque l'État échoue à protéger les données des concitoyens ou lorsque les services publics sont paralysés, ces atteintes à la sécurité deviennent des atteintes fondamentales à la souveraineté. Y répondre et les éviter autant que possible constitue la mission fondamentale de l'Anssi. Le deuxième pilier de la souveraineté numérique est celui du droit. Il s'agit d'appliquer notre droit et nos règles telles que nous les avons choisies dans l'expression de la souveraineté définie par notre Constitution, et de ne pas subir les règles définies par d'autres, sur lesquelles nous n'aurions pas voix au chapitre, ce qui renvoie à toute la question du droit extraterritorial. C'est un sujet de préoccupation pour l'Anssi lorsqu'il se matérialise par des risques qui impactent nos missions en termes de confidentialité, d'intégrité et de disponibilité des données. C'est évidemment un sujet bien plus vaste, puisque l'on pourrait ranger dans la même catégorie la modération des contenus sur les plateformes en ligne, l'accès des mineurs aux réseaux sociaux ou aux contenus pornographiques, qui ne relèvent pas du registre de l'Anssi mais qui, fondamentalement, procèdent du même problème. Le troisième pilier est la liberté de choix d'usage des technologies critiques pour les missions de l'État. Cela renvoie à des enjeux de politique industrielle, qui ne sont pas la mission première de l'Anssi, même si elle y contribue.

Le défi que posent les dépendances numériques se retrouve dans ces trois dimensions de la souveraineté avec, à mes yeux, un même enjeu fondamental. Si je l'observe avec un regard

historique, nous vivons un moment de prise de conscience collective : le paysage numérique construit ces 30 ou 40 dernières années s'inscrit dans cette « parenthèse dorée » des dividendes de la paix, en laissant de côté des crises et des tensions internationales qui reviennent aujourd'hui au premier plan. Ce contexte se reflète directement dans la manière dont ce paysage a été conçu : un numérique insuffisamment sécurisé, traversé de vulnérabilités, marqué par des dépendances mal maîtrisées et une complexité excessive, et dans lequel les risques n'ont ni été véritablement verbalisés ni formalisés. Pour le dire plus directement, nous avons trop souvent privilégié la rapidité et la facilité dans la construction de cet environnement numérique, et ces choix se traduisent aujourd'hui par des risques que nous peinons à maîtriser. Cela vaut pour l'État français comme pour les autres États, ainsi que pour les entreprises, même si la notion de souveraineté ne s'y applique pas pleinement.

Si j'entre dans le détail de ces trois piliers, la cybersécurité constitue évidemment notre cœur de métier, et le défi fondamental tient à l'omniprésence de vulnérabilités basiques, présentes de longue date mais désormais mises en évidence par une menace qui s'est massifiée. Les cyberattaquants n'épargnent plus personne, sans même évoquer l'accélération que promet l'intelligence artificielle (IA), au bénéfice des attaquants comme de l'ensemble des acteurs. La menace apparaît donc importante et susceptible de s'aggraver. C'est le constat posé dans la Revue nationale stratégique, qui retient comme scénario central une escalade géopolitique se traduisant par une massification et une coordination des cyberattaques. Cela met en évidence un enjeu de diffusion des bonnes pratiques, au cœur de la stratégie nationale de cybersécurité et de la transposition de la directive NIS 2.

Mais au-delà de ces bonnes pratiques, se pose également la question de la maîtrise des dépendances, dans la mesure où elles contribuent directement à notre vulnérabilité. À cet égard, l'Anssi a publié en mars son panorama de la menace, qui détaille ses observations pour 2025 et fait apparaître un constat majeur inscrit dans une tendance de fond : les attaques que nous traitons sont de plus en plus liées à la chaîne d'approvisionnement. Les prestataires et sous-traitants informatiques deviennent ainsi des points d'entrée privilégiés dans les systèmes d'information des victimes finales, qu'il s'agisse de prestataires de maintenance, d'infogérance ou du cloud, qui n'est pas exempt de vulnérabilités, tandis que les composants logiciels eux-mêmes sont de plus en plus ciblés.

Collectivement, à l'échelle mondiale, nous sommes en train de perdre la bataille contre les vulnérabilités logicielles puisque leur nombre a progressé de 18 % par an en moyenne sur les cinq dernières années pour atteindre 50 000 vulnérabilités rendues publiques chaque année, un tiers d'entre elles étant exploitées dès le jour de leur publication, à un rythme bien trop rapide pour permettre leur correction. Cette course est perdue d'avance et se trouve encore compliquée par la complexité et la réutilisation des chaînes de valeur logicielles. Deux exemples récents l'illustrent avec des briques open source comme Axios et LightLLM, qui ont fait l'objet d'attaques par piégeage, c'est-à-dire d'intrusions au sein même de leur communauté de développement. Même lorsque ces attaques sont détectées très rapidement, nous nous heurtons à un problème majeur de traçabilité pour identifier l'ensemble des réutilisations de ces fragments de code. J'exprime souvent cette difficulté de manière imagée : nous disposons de davantage d'informations lorsque nous achetons une saucisse, dont nous pouvons retracer l'origine jusqu'au cochon, que lorsque nous acquérons un logiciel. La traçabilité fait défaut et la chaîne de contamination est, en pratique, impossible à retracer rigoureusement. Aujourd'hui, ni l'État ni les entreprises ne disposent d'une cartographie complète de leur environnement logiciel et je constate, à chaque attaque que nous traitons, que l'attaquant connaît souvent mieux le système d'information de sa victime que la victime elle-même. Une partie de la réponse viendra du règlement européen sur la cyber-résilience, le CRA, qui imposera une première

forme de traçabilité avec le SBOM (*Software Bill of Materials*), mais il faudra évidemment étendre cette exigence à l'intelligence artificielle, sujet que nous portons notamment dans le cadre du G7.

L'enjeu du droit recoupe quant à lui directement les risques de cybersécurité, notamment à travers le droit extraterritorial, qui peut conduire à des accès non maîtrisés aux données, sans voie de recours. On pense au Cloud Act, aux lois FISA américaines ou à la loi chinoise sur le renseignement, ainsi qu'au risque de *kill switch*, c'est-à-dire la possibilité de couper des services numériques à travers l'application du contrôle export. Ces risques ne sont pas théoriques, ils sont déjà utilisés contre nous et, si ces dispositions existent, c'est pour être mises en œuvre. Aucune réponse purement technologique ne permet de faire face à ces risques puisque le chiffrement ne protège pas du Cloud Act et encore moins d'un *kill switch*. Cette réalité conduit à s'interroger sur la nationalité des fournisseurs, sans pour autant s'en tenir à une lecture binaire, car c'est l'ensemble de la chaîne de valeur qu'il faut examiner.

Pour des technologies structurantes comme la 5G ou le cloud, la complexité est réelle. Le référentiel SecNumCloud comporte 1 200 points de contrôle mêlant exigences techniques et non techniques, notamment sur la nationalité, la capitalisation et la gouvernance des fournisseurs. Il n'interdit pas le recours à des technologies étrangères, inévitables dans la pile logicielle du cloud, mais exige qu'elles soient maîtrisées par un prestataire européen. Dans ce cadre, cette qualification offre aujourd'hui le niveau de garantie le plus élevé face aux effets du droit extraterritorial. Cela vaut pour des approches hybrides, comme l'offre S3NS opérée par Thales reposant sur des technologies Google, comme pour des offres présentées comme non hybrides, qui intègrent elles aussi des briques américaines.

Sur ces sujets, il convient de distinguer le court et le moyen terme, qui relèvent de la maîtrise des risques, du long terme, qui renvoie à des enjeux de politique industrielle visant à multiplier les alternatives. Personne ne dispose aujourd'hui d'une solution face à une coupure généralisée d'accès aux technologies américaines ou chinoises, et si l'Europe se trouvait demain privée de mises à jour, la situation deviendrait rapidement intenable. Se pose également un enjeu de passage à l'échelle au niveau européen, car il n'est pas possible de traiter chaque technologie au cas par cas. Un cadre juridique plus générique est nécessaire et dans cette perspective, la révision du Cyber Security Act, le CSA II, constitue un vecteur pertinent : loin de clore le débat sur les risques non techniques, elle l'ouvre, la Commission ayant introduit un dispositif spécifique pour en assurer la prise en compte. L'essentiel est donc de rouvrir cette discussion à l'échelle européenne.

Enfin, l'Anssi, comme toute administration, est contrainte par ses dépendances numériques : lors du traitement d'un incident dans un cloud, elle dépend du prestataire et, lors d'une investigation sur un téléphone, du fabricant. Les options en matière d'outils spécialisés en cybersécurité sont souvent limitées, ce qui explique le développement interne d'outils, ensuite publiés en open source, et l'Anssi figure ainsi parmi les principales administrations productrices de logiciels libres. Répondre à ces contraintes liées à l'absence d'alternatives suppose donc une politique industrielle structurée car, dans certains cas, la diversité des offres mondiales suffit à éviter les situations de monopole et, dans d'autres, une maîtrise par des acteurs européens s'impose, sans pour autant viser une autarcie irréaliste. L'open source constitue un levier essentiel, sans être une solution unique. Son fonctionnement, sa pérennité et, le cas échéant, son financement doivent être examinés.

L'Anssi n'est pas chargée de conduire la politique industrielle, mais elle y contribue car ses visas de sécurité, qualifications et certifications peuvent éclairer les choix en tant qu'acteur neutre. Elle participe également à l'orientation des financements de France 2030 et des dispositifs européens pour combler les lacunes, notamment afin d'accompagner les plus petites structures appelées à relever de la directive NIS 2. Le principe est clair : mettre la politique industrielle au service de la cybersécurité, et non l'inverse. Les jugements en matière de cybersécurité ne sont pas infléchis pour promouvoir des solutions, même françaises ou européennes. Au sein de l'État, certaines administrations veillent à la sécurité des Airbus et des Boeing, tandis que d'autres soutiennent Airbus, et cette séparation répond à une logique fondée. Une vigilance particulière est également portée aux évolutions majeures, telles que l'intelligence artificielle ou la cryptographie post-quantique.

Pour conclure, la maîtrise des dépendances numériques apparaît comme un enjeu à la fois complexe et structurant, dont dépend notre sécurité et notre liberté d'action. Le fait que ce débat s'ouvre chez nos partenaires européens constitue une évolution positive, sans que cela doive conduire à en sous-estimer ni la complexité, ni les temporalités, ni le coût. Reprendre la maîtrise de ces dépendances, notamment en recourant à des fournisseurs européens, se fait rarement à coût nul ou à performance équivalente. Cela suppose d'entrer dans une logique d'investissement, les solutions européennes étant vraisemblablement plus coûteuses, mais relevant d'un choix d'investissement pertinent.

M. le président Philippe Latombe. Ma question fait écho à deux auditions récentes : celle d'un général spécialisé dans le numérique à l'Otan et nos échanges avec la DG Connect à Bruxelles, qui convergent sur l'importance des réseaux. Dans le contexte géopolitique actuel, les États-Unis ont commencé à recommander de ne plus acquérir de routeurs ou de cross-connects chinois. La France a engagé une démarche comparable avec la loi sur la 5G et la DG Connect envisage d'en reprendre les principes dans de futures réglementations européennes. En parallèle, la Chine adopte une approche similaire. La DG Connect souligne toutefois que la situation n'est pas symétrique puisque les Chinois seraient des adversaires, tandis que les Américains demeurent des alliés proches, ce qui rendrait difficile toute mesure discriminatoire à leur encontre. À l'inverse, le général de l'Otan insiste sur la nécessité de retrouver une capacité industrielle pour produire ces équipements, la maîtrise des réseaux étant essentielle. Quelle est, dans ce contexte, la position de l'Anssi sur ces enjeux, et comment entend-elle contribuer aux discussions européennes à venir ?

M. Vincent Strubel. C'est une question qui comporte de nombreuses ramifications. Les réseaux sont évidemment essentiels. L'attention se porte volontiers sur des technologies visibles et innovantes comme l'intelligence artificielle, alors même qu'elles reposent sur des infrastructures d'hébergement et de connectivité qu'il faut considérer en permanence. C'est dans cet esprit que la France a anticipé, au moins pour la 5G, en abordant la sécurité de ces réseaux non seulement sous l'angle technique mais aussi au regard des risques d'ingérence. La loi de 2019 n'est pas dirigée contre Huawei, mais vise à affirmer la souveraineté de nos réseaux numériques face à toute ingérence non européenne.

La question n'est pas de savoir s'il faut se protéger des Chinois, des Américains ou des deux, et la réduire à une opposition entre alliés et adversaires serait une erreur. L'enjeu réside dans les leviers que des États étrangers peuvent actionner à notre encontre, qu'ils le fassent ou non de manière hostile, en s'appuyant sur un droit à l'égard duquel nous ne disposons d'aucun recours. Cela ne revient pas à placer ces deux pays sur un même plan, car les États-Unis sont formellement nos alliés, mais des choix technologiques qui engagent sur 20 ou 30 ans ne peuvent reposer sur la seule configuration actuelle des alliances, au risque de supposer

qu'elle restera inchangée à cette échéance, hypothèse que rien ne permet de garantir. C'est la logique à l'œuvre dans SecNumCloud ou dans la loi 5G : il ne s'agit pas de qualifier des partenaires, mais d'objectiver les leviers susceptibles d'être utilisés contre nous, sans présumer de l'intention de ceux qui les détiennent. Ces leviers existent, et la question est celle de leur acceptabilité. La 5G ne constitue qu'un volet des réseaux de télécommunication, mais elle montre que, même lorsque l'enjeu est identifié, sa prise en compte s'inscrit dans le temps long : la transformation d'infrastructures de réseau s'opère sur plusieurs années, pour des raisons à la fois économiques et industrielles.

Mme Cyrielle Chatelain, rapporteure de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Si j'ai bien compris votre réponse, la question est de savoir comment objectiver les risques d'ingérence étrangère, quelle que soit la nationalité, selon une grille de lecture applicable sur le temps long. Pouvez-vous nous donner les grandes caractéristiques qui permettent d'objectiver ces risques ?

Concernant la cybersécurité, plusieurs témoignages nous ont indiqué que les outils de sécurité actuels étaient très majoritairement américains. Partagez-vous ce constat ? Si oui, quel est votre degré d'inquiétude quant à la limitation de notre capacité de choix, et comment anticipez-vous le risque de *kill switch* pour ces infrastructures critiques ? La question de l'absence de mise à jour fait-elle partie des tests que vous prenez en compte ?

Enfin, nous avons beaucoup parlé des États, mais nous voyons aujourd'hui des acteurs économiques qui prennent des positions politiques. Je pense particulièrement à Palantir, qui a publié un manifeste il y a quelques jours. Ces acteurs fournissent des services que l'on peut considérer comme critiques en matière de renseignement. Quel regard portez-vous sur ces acteurs ?

M. Vincent Strubel. Objectiver ces leviers implique de passer par une analyse rigoureuse des risques. Le processus consiste à recenser les risques, à en apprécier la plausibilité et à évaluer l'effectivité des contre-mesures. Cette analyse se conduit au cas par cas, car celle applicable à la 5G diffère de celle du cloud. Sur le cloud, il est possible de concevoir un montage où un prestataire européen de confiance, soumis en priorité au droit européen, opère une technologie étrangère. C'est le modèle de SecNumCloud, qui apporte une garantie solide contre l'accès extraterritorial aux données et contre un éventuel *kill switch* décidé par des autorités étrangères. Pour la 5G, l'analyse conduit en revanche à conclure que l'intervention directe du fournisseur sur le réseau étant indispensable, certains fournisseurs doivent simplement être écartés.

Sur les outils actuels de sécurité, l'idée selon laquelle seules les solutions américaines seraient performantes ne me semble pas correspondre à la réalité. La France et l'Europe disposent d'offres de cybersécurité de très haut niveau, qui figurent dans les catalogues de solutions recommandées par l'Anssi parce qu'elles satisfont aux critères de qualification. Les produits qualifiés sont, pour l'essentiel, français ou européens. Le choix se porte pourtant souvent sur des solutions mises en avant dans le Magic Quadrant de Gartner, rarement européennes, car il est perçu comme plus sûr à titre individuel. Cette logique de confort entretient une forme de monoculture qui constitue en elle-même un facteur de risque. L'épisode intervenu juste avant les Jeux olympiques et paralympiques l'a illustré : une mise à jour défaillante de la solution dominante sur le marché a paralysé des millions d'ordinateurs dans le monde, la France ayant été relativement moins touchée, en partie grâce à une moindre dépendance à cette monoculture.

S’agissant de Palantir, il ne s’agit pas d’entrer dans une analyse politique, mais de rappeler que le fonctionnement de notre démocratie suppose de ne pas dépendre de fournisseurs qui, par leurs prises de position, en viendraient à contester les règles fixées par le législateur. Une entreprise n’a pas vocation à se substituer à celui-ci et lorsque certains acteurs du numérique affirment qu’une disposition législative serait impossible à mettre en œuvre, il convient de rester vigilant. Cet argument peut en effet traduire avant tout une incompatibilité avec leur modèle économique, ce qui ne constitue pas un motif recevable dans le cadre du processus législatif.

M. le président Philippe Latombe. Pour prolonger la question sur l’écosystème cyber, on observe une concentration des acteurs, avec des acquisitions importantes de la part d’entreprises américaines. Comment analysez-vous ce phénomène ? Vous est-il déjà arrivé de saisir le service de l’information stratégique et de la sécurité économiques (Sisse) ou d’être interrogé par lui, sur l’opportunité de s’opposer à la cession d’une entreprise française ? Comment fonctionne la coopération entre le Sisse et l’Anssi ?

M. Vincent Strubel. Cela relève en effet d’un processus quotidien et encadré. Par construction, tout investissement étranger dans une entreprise française du secteur de la cybersécurité donne lieu à une saisine de l’Anssi par le Sisse afin d’évaluer les risques. Cette analyse fait partie de notre activité courante. Une vigilance particulière s’exerce pour prévenir toute prise de contrôle étrangère d’entreprises fournissant des solutions critiques pour des enjeux régaliens ou pour les opérateurs d’importance vitale et il nous arrive, le cas échéant, de nous opposer à ce type d’opérations.

M. le président Philippe Latombe. Lorsque l’entreprise se situe en dessous des seuils de revue du Sisse, disposez-vous de la faculté de signaler qu’elle présente, selon vous, un caractère critique justifiant un examen, même si elle n’entre pas formellement dans le champ de contrôle ?

M. Vincent Strubel. Nous contribuons en effet au dispositif de protection et de sécurité économique pour identifier les entreprises stratégiques à protéger en priorité. Lorsqu’il s’agit de bloquer un investissement étranger, les critères de droit s’appliquent et en dessous des seuils, il est possible d’alerter mais pas de s’opposer.

Plus largement, la recomposition du paysage industriel impose d’éviter les situations de monopole, tout en répondant à un enjeu de taille critique pour les offres françaises et européennes, aujourd’hui très morcelées. L’existence de PME innovantes et agiles constitue un atout, mais beaucoup n’atteignent pas la masse nécessaire. Une forme de consolidation apparaît donc souhaitable, qu’elle soit capitalistique ou fondée sur des coopérations et des offres communes. Là où un grand acteur permet d’accéder à une gamme complète de solutions, le recours à une multitude de PME suppose de multiplier les actes d’achat et d’en assurer l’intégration. Ce morcellement demeure une faiblesse de l’offre européenne.

Mme Cyrielle Chatelain, rapporteure. Pour revenir sur SecNumCloud et la question de l’extraterritorialité du droit, vous avez affirmé que le chiffrement ne protégeait pas du Cloud Act. Pourriez-vous développer ce point ?

Par ailleurs, le fait de stocker des données sensibles d’opérateurs d’importance vitale (OIV) doit-il relever de SecNumCloud ? Quelle est votre appréciation de la protection actuelle de ces données par les OIV ?

S’agissant enfin des solutions hybrides, comment garantir concrètement l’absence d’accès, notamment lors des mises à jour ? Vous avez indiqué que le *kill switch* constituait un risque pour toute solution comportant une composante américaine. Combien de temps un service peut-il fonctionner sans mises à jour ? Dès lors que les solutions les plus répandues sont aussi les plus ciblées, une telle situation n’engendre-t-elle pas une vulnérabilité accrue ?

M. Vincent Strubel. Sur le chiffrement, l’argument souvent avancé par certains acteurs du cloud est insuffisant car même si les données sont chiffrées, leur traitement implique que la clé de déchiffrement soit présente dans le cloud, aux côtés des données, ce qui permet au prestataire d’y accéder. Les technologies de *confidential computing* visent à remédier à cette limite, mais elles ne sont aujourd’hui ni suffisamment fiables ni généralisables, ce qui ne permet pas de se dispenser de la confiance accordée au prestataire. C’est pourquoi SecNumCloud ne garantit pas la protection des données contre l’opérateur de cloud, mais par celui-ci contre des tiers, et impose qu’il soit européen.

La notion de solution hybride est en réalité trompeuse puisque toutes les offres SecNumCloud reposent, à des degrés divers, sur des technologies non européennes, qu’il s’agisse de systèmes d’exploitation, de bases de données ou de solutions de virtualisation. Une infrastructure de cloud agrège une multitude de composants, qu’aucun acteur ne maîtrise intégralement. L’enjeu ne réside donc pas dans l’origine de chaque brique, mais dans l’organisation de l’exploitation : le prestataire européen opère l’infrastructure, tandis que les fournisseurs de technologies n’ont ni accès aux données ni rôle dans son fonctionnement quotidien. Dans ces conditions, ils ne peuvent pas interrompre le service, et le scénario de *kill switch* ne s’applique pas. En revanche, une interruption prolongée de l’accès aux mises à jour poserait un problème majeur, quel que soit le modèle de cloud, car le niveau de sécurité se dégrade rapidement. Cette dépendance est généralisée et souvent mal connue, du fait de la complexité des chaînes logicielles.

Pour les OIV, l’exigence est claire : tout système d’information critique hébergé dans le cloud doit relever de SecNumCloud. Pour les autres systèmes, il convient d’identifier les données sensibles, d’éviter leur concentration et de ne pas les placer dans des environnements soumis à des droits extraterritoriaux.

Mme Cyrielle Chatelain, rapporteure. Pour continuer sur les offres en partenariat franco-américain, comment les mises à jour se passent-elles concrètement ? J’imagine que des équipes de Windows ne peuvent pas prendre la main sur les équipements. Les employés de la société française ont-ils connaissance du code des logiciels installés ? L’objectif est-il de pouvoir reconstruire à partir de ce code ? Une vérification du code des mises à jour est-elle effectuée ?

M. Vincent Strubel. Sans promouvoir un modèle en particulier, le cas de S3NS, seule offre dite hybride aujourd’hui qualifiée SecNumCloud, illustre un point précis : le cycle de mise à jour repose sur un flux continu, au sein duquel des équipes françaises disposent, dans leurs processus, de la capacité d’inspecter, tester et vérifier chaque mise à jour. Elles ont accès au code source et procèdent à une analyse systématique. Cette capacité a évidemment ses limites puisque l’examen du code ne permet pas de détecter toutes les vulnérabilités, faute de quoi la question de la cybersécurité serait déjà résolue. Mais ce droit de regard existe. On peut même observer, non sans une certaine ironie, que les mises à jour de Google dans un environnement comme S3NS font l’objet d’un contrôle bien plus attentif que celles de Microsoft, déployées quasi automatiquement sur les systèmes de nos administrations et de nos entreprises. Cette situation rappelle que la dépendance aux technologies américaines ne se limite pas au cloud.

Enfin, sans que cela constitue un objectif recherché par l'Anssi, le fait que des acteurs européens développent une capacité de maîtrise de technologies américaines produit un effet positif. Il ne s'agit pas de renoncer à construire des alternatives, mais cette maîtrise renforce notre capacité d'analyse et de compréhension, tout en offrant un point d'appui pour appréhender plus finement le fonctionnement ou les éventuelles difficultés liées à ces technologies.

M. le président Philippe Latombe. Je souhaite aborder la question des dépendances propres à l'Anssi. La stratégie nationale cyber française a été publiée concomitamment à la stratégie américaine, qui s'inscrit dans une perspective sensiblement différente. Cette dernière évoque notamment le transfert au secteur privé de capacités cyberoffensives sur des réseaux communs, un point absent de la stratégie française, tandis que, parallèlement, la communauté du renseignement cyber a été affectée par d'importantes coupes budgétaires. Dans ce contexte géopolitique marqué par une évolution notable de la stratégie américaine, l'Anssi et ses homologues européens disposent-ils aujourd'hui d'une capacité réelle d'autonomie en matière de renseignement cyber ?

M. Vincent Strubel. Je ne m'aventurerai pas à comparer le degré d'offensivité des deux stratégies, la France ayant fait le choix clair de distinguer les composantes offensive et défensive. Ces dernières dialoguent et partagent du renseignement dans le respect de leurs rôles respectifs, mais je n'ai ni vocation à connaître nos capacités offensives ni à les commenter.

S'agissant du cœur de métier de l'Anssi, la compréhension de la menace repose sur des sources multiples. Elle s'appuie tout d'abord sur nos propres observations, issues de la supervision des réseaux de l'État et des investigations menées lors des incidents : en intervenant, nous traitons la crise, mais nous analysons également les modes opératoires, afin d'enrichir nos capacités de détection et d'analyse. Cette connaissance est complétée par les services de renseignement, par les apports du secteur privé en matière de *Cyber Threat Intelligence*, ainsi que par les échanges avec nos partenaires étrangers dans le cadre d'une coopération fondée sur le partage d'alertes et d'analyses.

La France dispose ainsi aujourd'hui d'une véritable autonomie d'appréciation de la menace, puisque ces apports extérieurs enrichissent notre analyse, mais ne la conditionnent pas. Nous sommes en mesure de détecter et de comprendre des menaces par nous-mêmes, y compris celles émanant d'acteurs peu documentés. Autrement dit, nous ne sommes pas dépendants de ces contributions, même si nous en tirons naturellement bénéfice.

Mme Cyrielle Chatelain, rapporteure. Pour poursuivre sur le cloud, vous évoquez un travail quotidien, et j'imagine en effet qu'il y a des interventions constantes à mener. Dans le cadre des solutions de partenariat franco-américain intégrant des technologies américaines, une partie des mises à jour est-elle de nature standard, ou s'agit-il de mises à jour quotidiennes émanant du fournisseur qui doivent être analysées au jour le jour ? Vous avez par ailleurs indiqué que la plupart des offres actuelles intègrent des composantes américaines. Si ces dernières requièrent des mises à jour quotidiennes, un délai de six mois pour qualifier une nouvelle offre peut sembler long. J'ai le sentiment que des failles de sécurité majeures pourraient apparaître et que la dégradation pourrait être rapide.

Concernant les référentiels de souveraineté du cloud, l'autorité de cybersécurité allemande a retenu une approche plus granulaire, avec des barèmes et plusieurs niveaux de maîtrise. Quelle est votre analyse de cette logique et comment peut-elle s'articuler avec une approche comme celle de SecNumCloud ?

Enfin, plus globalement, vous avez défini la souveraineté comme la capacité à faire appliquer nos propres règles. L'Union européenne a adopté des réglementations extrêmement ambitieuses comme le RGPD (règlement général sur la protection des données), le DSA (*Digital Services Act*) ou DMA (*Digital Markets Act*). Toutefois, plusieurs témoignages suggèrent que leur application n'est pas encore pleine et entière. Quel est votre regard sur le niveau d'application effectif de ces réglementations ?

M. Vincent Strubel. S'agissant des mises à jour, leur flux est effectivement quotidien, mais c'est une caractéristique inhérente à toute infrastructure numérique complexe, quel que soit le prestataire. Un prestataire de cloud ne fournit pas seulement de l'infrastructure mais aussi un catalogue très large de logiciels que les clients peuvent instancier à la demande. La valeur du cloud tient précisément à cette capacité à déployer en quelques clics des environnements hétérogènes, combinant par exemple plusieurs systèmes d'exploitation et différentes bases de données. L'ensemble de ces composants, au-delà de la seule couche d'infrastructure, doit être maintenu et mis à jour, ce qui implique un flux continu portant sur un nombre très important de logiciels.

S'agissant des logiques de barème et de notation, de légères divergences existent avec nos partenaires allemands. La différence tient à l'approche, puisqu'eux n'ont pas fait le choix d'une certification exigeante comme SecNumCloud, qui repose sur un processus lourd et structuré. Ce choix peut se discuter, mais il correspond à une exigence de garantie que nous estimons nécessaire. Le débat européen portera donc autant sur les critères eux-mêmes que sur les modalités de leur vérification, qui constituent, à mon sens, le véritable point de différenciation. Les approches par notation présentent un intérêt, mais elles demeurent complémentaires et ne sauraient se substituer à une qualification. Cette logique de barème a d'ailleurs été reprise par la Commission européenne dans son *Cloud Sovereignty Framework*, ainsi que par des initiatives françaises comme l'indice de résilience numérique. Ces outils permettent d'approfondir l'analyse des dépendances et de tenter d'en mesurer l'intensité en évaluant, par exemple, la part de composants non européens. Si cette démarche est utile, elle ne constitue pas une réponse en matière de couverture des risques car lorsqu'il s'agit de se prémunir contre l'application du droit extraterritorial, la logique ne peut être graduelle et est nécessairement binaire. Or dans ces systèmes de notation, ce critère ne représente qu'une part limitée de l'évaluation globale, ce qui peut conduire à obtenir une bonne note tout en restant pleinement exposé à ce risque.

La démarche la plus pertinente consisterait donc à articuler une certification permettant de garantir que les risques majeurs sont effectivement couverts, et une notation visant à apprécier le niveau de dépendance. Ce dernier point revêt également une dimension économique, car la dépendance à un fournisseur unique expose à des évolutions tarifaires subies. La question des dépendances ne se limite donc pas à l'accès ou à la sécurité, et renvoie aussi au risque d'enfermement technologique et financier.

M. le président Philippe Latombe. Une nouveauté récente est l'arrivée de l'IA, notamment sa capacité à produire et à inspecter du code. Je pense en particulier à Mythos. Avez-vous eu accès à Mythos ? Avez-vous pu l'évaluer et que pouvez-vous nous en dire ? Ce modèle a fait suffisamment de bruit pour que le président de la Réserve fédérale américaine convoque les banquiers pour leur dire d'y recourir face à un risque jugé réel, alors même que ces derniers sont censés être familiers de l'IA depuis des années.

Par conséquent, envisagez-vous d'intégrer dans vos réflexions et vos futures certifications l'utilisation de l'IA comme moyen de réaliser des tests d'intrusion, de la vérification de code ou de la recherche de failles ? Envisagez-vous de modifier vos référentiels à la lumière de ces évolutions technologiques ?

M. Vincent Strubel. Nous n'avons pas accès à Mythos. Comme la plupart des observateurs, nous l'analysons à partir de témoignages indirects, ce qui invite à une certaine prudence. Ce qui en ressort, au-delà du discours porté par Anthropic, c'est moins une rupture qu'une étape marquante dans une trajectoire déjà engagée. L'évolution était prévisible et elle va se poursuivre. En cela, Mythos ne constitue pas un cas isolé appelé à dominer durablement le paysage car d'autres acteurs atteignent déjà des niveaux comparables, et les prochaines générations de modèles iront plus loin. Nous sommes face à une dynamique d'amélioration continue, dont l'accélération impose de raisonner à moyen terme plutôt qu'en termes de rupture ponctuelle.

Dans ce contexte, l'intelligence artificielle devient effectivement de plus en plus apte à identifier des vulnérabilités et à produire du code permettant de les exploiter. Cela ne signifie pas qu'un modèle comme Mythos soit aujourd'hui capable de conduire de manière autonome une cyberattaque de bout en bout, mais il peut fournir à un attaquant humain des éléments crédibles, tant pour la détection des failles que pour leur exploitation. La conduite complète de l'attaque, avec la compréhension de l'infrastructure et l'enchaînement des actions, demeure en revanche du ressort humain. Il s'agit d'une évolution significative et la réponse à votre deuxième question est donc positive : il faut intégrer ces évolutions dans nos logiques de certification et, plus largement, dans la production logicielle. Nous sommes déjà, collectivement, en difficulté face aux vulnérabilités puisque des dizaines de milliers sont découvertes chaque année, non pas seulement à la sortie des logiciels, mais sur des systèmes déjà en circulation, et elles peuvent être exploitées très rapidement. Cela impose de traiter un flux continu de correctifs, que la plupart des organisations ne parviennent pas à absorber dans les délais, même sans l'apport de l'IA. Des architectures de défense en profondeur permettent d'en atténuer les effets, mais elles ne dispensent pas de traiter le problème à la source, dès la conception des logiciels.

Dans cette perspective, la certification peut constituer un levier, mais elle ne suffit pas : le recours à l'IA doit s'inscrire au cœur du cycle de développement, au même titre que les outils d'analyse existants. Se contenter d'accélérer la détection et la correction des vulnérabilités reviendrait à rester en position défensive, l'enjeu étant d'empêcher leur apparition dans les produits diffusés, ce qui suppose une transformation profonde du cycle de vie logiciel.

À titre prospectif, on peut envisager qu'une future évolution du cadre européen impose qu'un produit numérique mis sur le marché ait fait l'objet d'une analyse par des outils d'IA. Une telle orientation soulèverait toutefois des questions de dépendance technologique, selon les acteurs capables de fournir ces outils. Sur ce point, il existe néanmoins des perspectives de développement d'acteurs européens capables d'atteindre rapidement des niveaux de performance comparables en matière de détection et de correction des vulnérabilités.

Mme Cyrielle Chatelain, rapporteure. L'écriture de code par l'IA représente-t-elle selon vous un risque de perte de qualité et de création de vulnérabilités ? Quelle est votre analyse sur ce point ?

Pour changer de sujet, vous avez rappelé que la mission première de l'Anssi n'est pas de mener une politique industrielle. Vous avez néanmoins vocation à encourager le développement d'offres de services et de produits de sécurité, et vous avez notamment été fortement impliqué dans le volet cybersécurité de France Relance. Quel regard portez-vous sur ce qui a été fait et quels outils vous semblent pertinents pour dynamiser cette filière industrielle ?

M. Vincent Strubel. S'agissant de l'IA générant du code, la principale difficulté tient à l'évaluation de sa propre sécurité. L'usage de l'IA comme outil, qu'il serve les attaquants ou les défenseurs, constitue un enjeu, mais le risque majeur apparaît lorsque l'IA remplace progressivement les logiciels traditionnels, soit en produisant le code, soit en prenant directement des décisions. Or, il faut garder à l'esprit qu'aucune méthode ne permet aujourd'hui d'apporter à ces systèmes des garanties de sécurité comparables à celles que l'on peut offrir pour un logiciel classique. Leur évaluation demeure imparfaite et leur certification n'est pas maîtrisée. Cette question constitue une priorité des travaux engagés dans le cadre de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (Inesia) réunissant notamment l'Anssi et l'Institut national de recherche en sciences et technologies du numérique (Inria). Elle se double d'une difficulté d'analyse *a posteriori* : face à un comportement anormal, il est souvent impossible de déterminer de manière certaine s'il résulte d'une attaque ou d'un dysfonctionnement propre au modèle. Contrairement à un logiciel traditionnel, une IA ne peut pas être corrigée par un simple correctif puisque sa modification suppose un réentraînement, avec des cycles et des incertitudes différents.

Ces éléments introduisent des risques significatifs, d'autant qu'une pression forte existe pour déployer rapidement ces technologies. Les biais constituent également un point d'attention : les IA apprennent à partir de données produites par les humains et sont susceptibles de reproduire leurs erreurs. Là où des développeurs commettent des fautes variées, une IA peut systématiser un même défaut, créant ainsi un risque de vulnérabilités à grande échelle. Ces enjeux font partie des axes de travail en cours, sans qu'une solution pleinement satisfaisante n'existe à ce stade.

Concernant France Relance et les dispositifs d'accompagnement associés, nous avons mobilisé ce plan conformément à sa finalité initiale de soutenir une économie fragilisée par la crise sanitaire en y contribuant par le renforcement de la cybersécurité. Le bilan est, à mon sens, très positif. Sur les 176 millions d'euros engagés, 100 millions ont été consacrés aux parcours de cybersécurité, qui ont permis de mobiliser des prestataires labellisés par l'Anssi au bénéfice de petits établissements publics. Près d'un millier de collectivités, d'établissements d'enseignement et d'autres structures ont ainsi été accompagnés pour amorcer une démarche de sécurité, avec des effets concrets, puisque certains hôpitaux ont évité des cyberattaques susceptibles de les paralyser. Ce dispositif a également eu un effet structurant sur la filière, puisque les financements ont bénéficié très majoritairement à des prestataires français et européens sans que cela résulte d'un choix délibéré de l'Anssi. Les autres actions menées dans ce cadre, notamment le financement d'équipements de cybersécurité, ont suivi la même logique, en soutenant l'acquisition de pare-feux, de solutions de chiffrement ou de VPN figurant dans les catalogues qualifiés.

Ce dispositif a donc permis de renforcer la sécurité des acteurs publics, de soutenir la filière nationale et européenne et d'accélérer l'équipement des structures concernées. La question de sa reproductibilité demeure toutefois ouverte, tant au regard des contraintes du droit européen en dehors d'un contexte exceptionnel que de la situation des finances publiques, mais son utilisation apparaît, rétrospectivement, pleinement justifiée.

M. le président Philippe Latombe. Si, au fil des auditions que vous avez suivies, des points vous paraissent importants à souligner ou si, à l'inverse, vous estimez que certaines idées sont mauvaises ou non conformes à votre analyse, n'hésitez pas à nous en faire part par écrit.

La séance s'achève à dix heures trente.

Membres présents ou excusés

Présents. – Mme Cyrielle Chatelain, M. Philippe Latombe