ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

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

Mercredi 4 juin 2025
Séance de 15 heures 30

Compte rendu n° 6

SESSION ORDINAIRE DE 2024 - 2025

Présidence de M. Philippe Latombe, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à 15 heures 30

La commission spéciale a organisé une table ronde réunissant des entreprises de cyberdéfense : M. Michaël Barthellemy, responsable de la gestion des risques cyber et des actifs d'Airbus et représentant de la commission Cyber du Groupement des industries françaises aéronautiques et spatiales (Gifas), M. Thierry Racaud, président-directeur général d'Airbus Protect, M. Yves Berthe, coordinateur sécurité d'Airbus France, M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing d'Orange Cyberdéfense, M. Vivien Mura, directeur des technologies d'Orange Cyberdéfense, Mme Katuiscia Benloukil, vice-présidente communication de Tehtris et M. Arnaud Dechoux, directeur des affaires publiques de Sekoia.io.

M. le président Philippe Latombe. Mes chers collègues, nos auditions sur le projet de loi relatif à la résilience des infrastructures critiques au renforcement de la cybersécurité se poursuivent aujourd'hui avec une table ronde réunissant des représentants d'entreprises présentes dans les domaines de la cyberdéfense et de la cybersécurité. Cette audition sera donc à la fois consacrée à l'impact de la directive NIS 2 sur les entreprises soumises à la réglementation et sur les services de cybersécurité qu'offrent vos groupes respectifs, notamment aux infrastructures critiques.

Airbus sera représenté par M. Barthellemy, responsable de la gestion des risques cyber et des actifs et représentant de la commission cyber du groupement des industries françaises aéronautiques et spatiales (Gifas), M. Thierry Racaud, président directeur général d'Airbus Protect et M. Yves Berthe, coordinateur sécurité d'Airbus France. M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing, et M. Vivien Murat, directeur des technologies, représentent Orange Cyberdéfense. L'entreprise Tehtris est représentée par Mme Katuiscia Benloukil, vice-présidente communication et Sekoia.io par M. Arnaud Dechoux, directeur des affaires publiques.

Avant de vous céder la parole, je souhaite vous poser une question liminaire. Vos activités sont souvent implantées dans plusieurs pays de l'Union européenne. Comment envisagez-vous de vous adapter aux différents modèles de transposition retenus par les États membres ?

M. Michaël Barthellemy, responsable de la gestion des risques cyber et des actifs d'Airbus et représentant de la commission cyber du Gifas. Je vous remercie de nous accueillir aujourd'hui pour cette audition. La résilience digitale présente plusieurs enjeux cruciaux pour nos organisations, notamment critiques – catégorisées entreprises essentielles ou entreprises importantes –, notre capacité à anticiper, prévenir, dissuader, détecter, retarder, défendre, répondre et résister aux attaques et à nous remettre des incidents de cybersécurité.

Il faut également citer la protection de l'intégrité informatique et fonctionnelle face aux risques croissants ; la limitation des pertes financières, d'image et de confiance en cas d'incident majeur ; la continuité des activités et le maintien de la productivité malgré les attaques et la préservation et la sécurisation des données, y compris dans le cadre du règlement général sur la protection des données (RGPD) et de la loi « informatique et libertés » en France.

Cette résilience, quand elle parvient à être démontrée, conditionne l'instauration d'un climat de confiance avec nos usagers, clients, fournisseurs et autorités de tutelle. Une fois

rappelés ces enjeux importants que représentent la résilience digitale et la cybersécurité pour notre filière, je souhaiterais attirer votre attention sur quelques points qui ressortent de notre étude du projet de loi. Sans vouloir déposséder le Parlement français de ses prérogatives, il n'est plus envisageable aujourd'hui que ce type de texte soit du niveau d'une directive européenne. En réalité, il devrait être porté par un règlement européen. Imaginez la difficulté pour un groupe comme Airbus, présent dans la quasi-totalité des États membres de l'Union européenne (UE). Nous allons devoir appliquer vingt-sept réglementations différentes, ce qui engendrera des coûts supplémentaires et posera des complexités techniques.

Ensuite, il faut analyser plus globalement l'impact de la réglementation sur la continuité des dispositifs existants, qui représente pour notre filière une double surtransposition de la directive européenne, comme nous aurons peut-être l'occasion de le démontrer. La France va en effet au-delà des demandes de la directive et la proposition de transposition actuelle vient en doublon d'un certain nombre de contraintes qui sont déjà requises dans le corpus juridique existant : la loi de programmation militaire (LPM), l'instruction générale interministérielle (IGI) n° 1300, l'IGI n° 900 et l'IGI n° 901.

L'augmentation des sanctions fera également peser une pression financière sur nos entreprises, transformant le dispositif existant, qui est fondé sur la coopération et la confiance entre acteurs, en une relation qui sera plus contractuelle. Nos concurrents internationaux, y compris européens, non soumis à ces mêmes règles, seront avantagés, laissant nos entreprises dans une position désavantageuse. Il faut donc veiller à ne pas créer, par cette surtransposition, une opportunité de « *dumping* de cybersécurité » pour les autres États membres.

En revanche, le véritable risque concerne particulièrement les petites et moyennes entreprises (PME) et les entreprises de taille intermédiaire (ETI), qui sont déjà vulnérables et qui pourraient être fragilisées par des exigences qui seraient trop contraignantes et une mise en œuvre précipitée. En effet, une demande de mise en œuvre trop rapide risquerait de créer chez eux des déséquilibres importants. Leur soutien et leur préservation constituent donc une priorité à laquelle nous devons répondre de manière concrète.

Ensuite, la question de la souveraineté numérique et de l'indépendance géostratégique figure au cœur de nos préoccupations. Parfois, la résilience opérationnelle contredit en partie le principe de souveraineté, notamment sur les aspects liés aux Gafam, qui occupent une place prépondérante. En conséquence, les choix qui sont réalisés aujourd'hui détermineront notre capacité à maintenir l'équilibre entre notre indépendance et nos interdépendances, dans un contexte de concurrence globale.

Enfin, pour que nos entreprises puissent réussir cette transition vers la directive NIS 2 et la résilience, un soutien au bon niveau des services de l'État est indispensable, sous forme technique, financière et d'aide au développement de solutions de confiance adaptées aux PME et aux ETI. Cet investissement permettra d'assurer la pérennité et la compétitivité de notre filière. Nous pensons que l'Agence nationale de la sécurité des systèmes d'information (Anssi) doit jouer un rôle central dans ce dispositif.

Je cède la parole à mon collègue Thierry Racaud d'Airbus Protect, société qui est déjà conduite à supporter notre écosystème et la nation de façon plus générale, sur les sujets de cybersécurité et de cyberrésilience.

M. Thierry Racaud, président-directeur général d'Airbus Protect. Airbus Protect est une société française filiale du groupe Airbus, créée en juillet 2022. La société résulte du regroupement d'activités cyber au centre du groupe et bénéficie ainsi d'un héritage d'excellence et d'une compréhension approfondie des enjeux de la cybersécurité dans les secteurs les plus critiques. La mission d'Airbus Protect consiste à contribuer à la cyberprotection d'Airbus, c'est-à-dire ses produits, ses usines et ses filiales, sa chaîne logistique, sa chaîne de valeur et plus largement le secteur aérospatial, les infrastructures critiques et les institutions nationales et européennes.

Ainsi, à travers Airbus Protect, Airbus met ses meilleurs experts au service de ses sous-traitants, partenaires, clients, partout en Europe. Nos services couvrent l'ensemble du cycle de vie de la cybersécurité en offrant une approche holistique et sur mesure pour répondre aux besoins particuliers de nos clients et partenaires, du conseil à l'audit de cybersécurité, pour les aider à se mettre en conformité avec les règlements nationaux et européens : protection des systèmes critiques, service de détection et de réponse aux incidents de cybersécurité, cybersécurité des produits, formation et sensibilisation, tests d'intrusion et recherche de vulnérabilité cyber. Les services d'Airbus Protect sont, dans leur majorité, labellisés par l'Anssi. Ainsi, en combinant son héritage industriel avec une expertise pointue en cybersécurité, Airbus est le partenaire cyber du secteur aérospatial. Les salariés d'Airbus Protect, au nombre de 500 en cybersécurité, sont fiers de contribuer à la protection des intérêts stratégiques français.

M. Olivier Bonnet de Paillerets, vice-président exécutif chargé de la technologie et du marketing d'Orange Cyberdéfense. Orange Cyberdéfense, compagnie majoritairement acquise par Orange, est une société de services sur l'ensemble du cycle de la cybersécurité : analyse de la menace propre, détection, protection, remédiation, gestion de crise et conseil. Orange Cyberdéfense traite l'ensemble des segments du marché, les multinationales, les PME et TPE, y compris les clients Orange, c'est-à-dire le *BtoC*.

La société évolue dans un marché extrêmement concurrentiel : nous sommes leaders en France avec 12 % de parts de marché et en Belgique avec 5 %. Dans ce marché très concurrentiel, nos clients font face à trois complexités. La première a trait à une menace toujours évolutive en degré. L'Europe continue à souffrir d'un nombre croissant d'attaques (plus de 20 % l'année dernière), dans la mesure où l'activisme atteint depuis deux ans le monde des affaires et pas uniquement les institutions nationales. De surcroît, ce monde des affaires est concerné de plus en plus dans le bas du marché. Ainsi, 53 % de PME supplémentaires ont été touchées par rapport au référentiel de l'année dernière.

Au-delà de cette menace toujours grandissante en nature et en degré, la deuxième complexité est liée à la complexité de la surface de nos clients, avec le mouvement vers le cloud hybride, souverain. Ils sont confrontés à une complexité technique pour laquelle ils nous demandent des idées.

La troisième complexité est relative à la régulation. Le projet de loi touche Orange Cyberdéfense comme fournisseur essentiel en tant que société de services numériques. Pour nous, le coût d'adaptation n'est pas très important, puisque nous étions déjà très certifiés et en conformité avec la régulation nationale. En revanche, il offre une opportunité de continuer à accompagner, y compris les TPE PME qui seront concernées par NIS 2. Dans le cadre de sa transposition, la loi concerne moins les services numériques, puisque seulement trois articles nous concernent.

Globalement, dans le cadre de cette transposition, il conviendra de ne pas faire de surenchère pour demeurer compétitif, mais également de veiller à la simplification dans les décrets qui suivront. À titre d'exemple, se pose la question de la diversité de la mise en œuvre de NIS 2 dans l'ensemble de la géographie européenne, et même au-delà. Quand on dispose de systèmes extrêmement décentralisés dans l'Union européenne, ou dans nos systèmes *offshores*, quels seront les systèmes d'environnement en technologies de l'information (ITALIE) concernés ou non par la directive NIS 2 ? En fonction de la nature des réseaux, de notre chaîne d'approvisionnement, de notre modèle opérationnel, de notre relation client, la gestion sera probablement complexe. En conséquence, il faudra être très attentif à la manière dont certains décrets seront rédigés.

De plus, il importe ne pas réinventer de nouvelles certifications ou de nouveaux processus de remontée d'informations des incidents. Il en existe déjà, autant les utiliser et maximiser ce qui a été mis en place par l'Anssi en matière de certification.

Mme Katuiscia Benloukil, vice-présidente communication de Tehtris. Tehtris est une société française à l'échelle internationale spécialisée aujourd'hui dans les solutions de cybersécurité pour détecter et neutraliser automatiquement, de manière autonome et en temps réel, le cyber espionnage et le cybersabotage.

Je partage les propos de mes confrères sur les enjeux de souveraineté, mais aussi l'importance de donner une obligation de moyens à toutes les entreprises. L'objectif de la directive NIS 2, qui reprend les mécanismes du RGPD, vise à rendre le cyberspace plus sûr, afin que chaque entreprise, petite, moyenne ou grande, puisse bénéficier d'une couverture cyber et se protéger des menaces qui évoluent. Aujourd'hui, nous constatons en effet une augmentation du volume des attaques, mais aussi de leur sophistication.

Ces attaques sont polymorphes et leurs variants changent très rapidement grâce aux techniques cyber utilisées, du côté des attaquants. Les entreprises doivent donc être soumises à une obligation de moyens, en matière de défense et de couverture cyber. En conséquence, ce texte de projet de loi rentre parfaitement dans le cadre mis en place actuellement en matière de régulation. Toutefois, cette transposition ne doit pas constituer une difficulté supplémentaire pour les entreprises.

M. Arnaud Dechoux, directeur des affaires publiques de Sekoia.io. Sekoia est une *scale-up*, une grande start-up d'une centaine de personnes implantée notamment à Paris et à Rennes, mais également dans différents pays européens. Nous sommes un éditeur de technologies *BtoB* dédiées à deux domaines de spécialisation. Il s'agit d'une part du renseignement d'intérêt cyber, produit par une vingtaine de chercheurs qui suivent les groupes d'attaquants, qu'ils soient cybercriminels ou des espions affiliés des États. À ce titre, Sekoia est partenaire d'Europol et coopère régulièrement avec les forces de l'ordre et la justice dans la lutte contre la cybercriminalité.

D'autre part, Sekoia développe une plateforme en mode SaaS (*Software as a Service*) à l'attention des centres d'opérations de sécurité (SOC) permettant de détecter les cybermenaces grâce au renseignement cyber et à l'intelligence artificielle (IA) et d'y répondre automatiquement. Cette solution, également décrite par l'acronyme XDR, vient s'imbriquer avec d'autres rubriques de sécurité, comme les logiciels de détection et de réponse aux *endpoints* (EDR) produits par exemple par Airbus, des pare-feu et des sondes, pour assurer une supervision étendue du système d'information.

Cette solution est commercialisée auprès de grandes organisations qui sont matures en cybersécurité, mais aussi et surtout de manière indirecte, via un modèle *BtoB*, grâce à des partenariats avec des prestataires de services, comme Orange Cyberdéfense, qui utilisent notre technologie pour protéger leurs clients finaux qui sont constitués autant de grands groupes que de PME et de TPE. L'ambition consiste à démocratiser une cybersécurité de haute performance pour les petites entreprises ou administrations. À ce titre, Sekoia s'inscrit dans la chaîne d'approvisionnement de toutes ces entités qui seront soumises à NIS 2. Sur ces deux spécialités, nos concurrents sont quasi exclusivement des grands groupes américains ou israéliens.

En matière de conformité, Sekoia ne part pas de zéro. Nous avons misé pour l'instant sur des certifications reconnues internationalement, ISO 27001, PCI DSS dans le secteur des cartes de paiement, ou des labels comme Cybersecurity Made in Europe pour France Cybersecurity, labels déclaratifs, mais qui ont le mérite d'exister.

S'agissant du projet de loi actuellement en discussion devant votre commission spéciale, nous souhaitons également rappeler que la directive représente une avancée significative pour assurer un niveau élevé et commun de résilience dans l'ensemble de l'UE, qu'il s'agisse d'un enjeu de sécurité nationale, mais aussi de souveraineté.

Initialement, nous avons émis un doute sur le fait que Sekoia entre directement dans le périmètre des entreprises soumises à la NIS 2, peut-être en tant que fournisseur de services d'informatique en nuage, ce qui ferait de nous une entité importante. Ceci est probable, mais pas certain. Quoi qu'il en soit, en tant que membre de la chaîne d'approvisionnement de ces entités essentielles ou importantes, nous serons soumis indirectement aux mêmes obligations.

Pour Sekoia, les enjeux se joueront principalement au niveau réglementaire, avec les décrets et les arrêtés qui seront pris. Je pense notamment au référentiel des exigences techniques et organisationnelles, actuellement en préparation par l'Anssi.

À ce sujet, je souhaite mettre en avant trois points concernant ce projet de loi, certains étant portés par les associations dont Sekoia est membre, notamment l'Alliance pour la confiance numérique (ACN) et Hexatrust, que vous auditionnerez demain. Premièrement, le texte impose aux entités entrant dans son champ de renforcer leurs actions en matière de gestion des risques et de protection cyber. Ceci bénéficiera sans doute, premièrement, aux consultants, aux auditeurs et aux prestataires de services de proximité. Mais à ce stade, rien ne garantit qu'il en soit de même pour les équipements et les solutions, car le texte n'établit pas de préférence européenne. Au contraire, il nous apparaît que le risque est élevé aujourd'hui si les organisations privées comme publiques font appel en majorité à des solutions cyber non européennes, suivant la tendance actuelle.

Si tel était le cas, la directive et sa transposition ne feraient ainsi que renforcer leur dépendance à des acteurs extra-européens, à rebours de l'objectif d'accroître la souveraineté numérique française et européenne. À ce titre, le crédit d'impôt cyber bien ciblé constitue peut-être une piste de réflexion, peut-être un vœu pieux. Cependant, nous soutenons le vote au niveau européen d'un Buy European Tech Act ou d'un Small Business Act qui permettraient d'appuyer l'innovation en Europe grâce à la commande publique.

Deuxièmement, nous appelons à assurer autant que possible une proportionnalité et une application harmonisée de ces nouvelles obligations. Pour une start-up comme Sekoia, qui investit déjà dans des certifications comme ISO 27001, l'ajout de nouvelles obligations

passant par des audits, des certifications ou des labels – pas nécessairement obligatoires, mais très fortement recommandés – auprès de consultants externes représenterait des coûts importants et ne ferait que renforcer la complexité à se déployer à l'international.

Troisièmement, une de nos propositions concernerait l'association continue des experts du secteur à la rédaction des textes réglementaires, par exemple en précisant que la mise à jour du référentiel de l'Anssi devra s'opérer en concertation avec les organisations professionnelles de la filière cyber française. L'idée porte ainsi sur un comité de suivi associant notamment les représentants de la filière, pour assurer la cohérence et l'efficacité du dispositif dans le temps. L'objectif consiste à mieux s'adapter à l'évolution rapide des cybermenaces, mais aussi des technologies de cybersécurité.

En synthèse, NIS 2 et sa transposition constituent une opportunité pour le tissu économique français et pour une start-up comme Sekoia. Nous espérons qu'elle sera également une opportunité en matière de souveraineté pour la filière cyber, qu'il s'agisse des services, mais aussi des solutions, et non un accroissement de la complexité qui ne bénéficiera certainement qu'aux grands éditeurs, notamment extra-européens.

M. Éric Bothorel, rapporteur général. Je fais partie de ceux qui souhaitent limiter toute surtransposition dans le contexte géopolitique actuel. Il ne s'agit pas d'empiler des textes réglementaires dans chaque pays, mais de faire émerger un écosystème et un cadre régulatoire au niveau européen aussi harmonieux et homogène que possible.

Ayant relu les auditions qui ont eu lieu au Sénat sur ce projet de loi, dont les vôtres, j'ai perçu à la fois la totale conviction de la nécessité de lutter contre les attaques, votre connaissance de l'accroissement du risque, mais aussi une forme de crainte face à un risque d'empilement entre les contraintes initiées par la loi d'orientation et de programmation du ministère de l'intérieur (Lopmi) et les questions actuelles autour de la résilience. L'exercice de la Lopmi a-t-il été si difficile pour vous, acteurs et opérateurs de la cyberdéfense ? Votre retour d'expérience pourrait peut-être nous éclairer.

Ensuite, la mise en œuvre de la LPM a contribué au développement d'une politique industrielle autour des schémas de qualification de services. Ces schémas ont permis d'accroître le niveau d'exigence, non seulement vis-à-vis des opérateurs d'importance vitale (OIV), mais surtout vis-à-vis des offreurs. Il me semble important de prendre cela en compte et de réfléchir à la mise en place d'une politique industrielle qui permette la construction d'une offre répondant aux besoins.

Or tel n'a pas été le cas de l'offre qui a été développée avec la Lopmi. Le cadre est probablement ici trop contraignant ; les enjeux liés à la sécurité tenant plus de la souveraineté que de la résilience. Cependant, il faut une politique qui garantisse une offre de qualité tout en permettant agilité et compétitivité. Avez-vous le sentiment que la simplification de ces dispositifs et leur remise à la vie civile constitueraient une piste ?

En ce qui concerne la politique industrielle de solutions cyber, il me semble que le comité stratégique de filière cyberdéfense est aujourd'hui quelque peu en sommeil. Me le confirmez-vous ? N'y a-t-il pas là une opportunité, par le passage au civil de tout ou partie de ce qui a été mis en œuvre pour la défense, de relancer ce comité stratégique ?

Nous sommes aussi à l'écoute de votre point de vue sur les exigences concernant les OIV et leurs filières nationales et européennes, ainsi que leurs sous-traitants. Certains

estiment que le maillon le plus faible permet d'évaluer la force de résistance d'une chaîne. D'autres nous disent que les contraintes seraient trop fortes pour leurs filiales. Quel est votre point de vue ?

Mme Anne Le Hénanff, rapporteure. Je souhaiterais savoir si chacun d'entre vous est concerné par des dispositions du titre II du projet de loi ou du titre Ier qui transpose la directive sur les résiliences des entités critiques (REC). Si tel est le cas, dans quelle mesure ?

Les sénateurs ont procédé à une modification substantielle de certaines définitions qui vont dans le bon sens selon moi, notamment sur la partie concernant NIS 2. Va-t-elle assez loin ? Faut-il procéder à de plus amples clarifications ?

J'imagine également que certains d'entre vous seront concernés par le régime dérogatoire appliqué aux entités essentielles, aux entités importantes, aux administrations d'État, à leurs établissements publics administratifs qui exercent, entre autres, des activités dans le domaine de la sécurité publique, de la défense nationale ; et pour leurs réseaux et systèmes d'information prévus à l'article 14. Que pensez-vous de cette dérogation et de la rédaction de l'article ? Cette dérogation s'appliquerait-elle, le cas échéant, à l'ensemble de vos sous-traitants ?

M. Mickaël Bouloux, rapporteur. Je suis rapporteur du titre III du projet de loi, c'est-à-dire les articles qui concernent la transposition de la directive européenne sur la résilience opérationnelle numérique du secteur financier, dite Dora. Êtes-vous conduits à intervenir auprès des entités financières ? Comment appréciez-vous leur maturité pour la cybersécurité ? Comment intervenez-vous dans ce domaine, le cas échéant ? Le secteur financier présente-t-il des spécificités par rapport à d'autres secteurs économiques ou industriels s'agissant des attaques et des menaces ?

M. Michaël Barthellemy. NIS 2 ne constitue pas un grand changement pour Airbus, dans la mesure où nous sommes déjà fortement réglementés, par la LPM ou NIS 1 notamment, d'autant plus que la France était en avance dans ce domaine par rapport aux autres pays européens.

En revanche, NIS 2 suscite une grande quantité de travail dans la démonstration de la preuve. Comme nous l'avons indiqué aux sénateurs, nous serions favorables à un label, un « tampon » que fournirait l'Anssi pour attester que nous avons bien répondu aux différentes contraintes, qui éviterait de devoir procéder à de nouveaux audits, qui sont à la charge de l'entreprise.

M. Arnaud Dechoux. Sekoia n'est pas concerné par la Lopmi ou des discussions spécifiques sur la défense ou les OIV. En revanche, je partage l'idée selon laquelle le maillon le plus faible constitue la bonne mesure de la résilience de la filière. Une start-up comme Sekoia, qui est productrice de solutions, s'inscrit dans la chaîne d'approvisionnement des entités qui seront soumises autant à REC et à NIS 2, qu'à Dora. De notre côté, l'attente portera sur les impacts contractuels de ces directives sur les entreprises concernées. En effet, les obligations qu'elles devront respecter auront également une répercussion à notre niveau, par exemple en termes de notification d'incidents.

Nous sommes également soumis à l'acte d'exécution pour NIS 2 qui a été publié l'été dernier et qui fournit de nombreux détails, par exemple les éléments constitutifs d'un incident et les délais associés en matière d'intervention.

Ensuite, les entités financières sont généralement plus matures en termes cyber, même si certains acteurs de la fintech devront monter en compétences. Très concrètement, Dora constitue une opportunité commerciale pour une entreprise comme la nôtre. Pour le renseignement cyber, les entités financières devront par exemple faire appel à des consultants pour passer des tests de résilience basés sur des menaces de type *Threat-Led Penetration Testing (*TLTP). Encore une fois, nous espérons que les acteurs européens ne seront pas oubliés ou du moins qu'ils pourront être promus par ce genre de dispositifs. Enfin, en matière de menaces spécifiques, je précise que les Nord-Coréens sont experts dans la conduite d'opérations lucratives ciblant notamment la finance.

M. Olivier Bonnet de Paillerets. Orange Cyberdéfense sera concerné au titre de la *supply chain* des entreprises qui devront répondre aux exigences de la directive Dora. Certains de nos clients européens dans le secteur financier, notamment allemands, nous ont ainsi fait part de leurs exigences. Il faudra donc procéder à une forme d'éducation pour éviter que Dora ne soit transposée intégralement pour des organisations qui ne sont pas contraintes de se conformer totalement à cette réglementation.

Le secteur financier est de plus en plus mature. À titre d'illustration, il a connu une baisse de 20 % du nombre de victimes, l'année dernière en Europe. Le secteur est conscient des enjeux, notamment de souveraineté, et il est prêt à consentir des efforts financiers pour augmenter la certitude d'éviter un risque sur le réseau.

Je me garderais de formuler un avis définitif sur le comité stratégique, mais souhaite vous apporter un témoignage. Je reviens de San Francisco, où je suis allé rencontrer de grands fournisseurs américains. J'ai été marqué par l'accélération de l'innovation sur les capacités en GPU (*Graphics Processing Unit*), les agents IA et l'augmentation de l'intelligence des robots, grâce aux milliards de dollars qui ont été injectés dans le secteur. L'innovation figure bien au cœur de la proposition de valeur et je pense qu'il s'agit là de la réponse, y compris aux enjeux de souveraineté.

Compte tenu de la diffusion descendante de la menace, la chaîne d'approvisionnement revêtira une criticité encore plus marquée qu'auparavant pour les acteurs essentiels. Il convient donc d'accorder des investissements à la *supply chain*.

Enfin, en tant que prestataire numérique, nous sommes assez peu concernés par le projet de loi tel que vous le mentionnez. Je crois qu'il s'agit essentiellement de trois articles, dont l'article 14.

M. Vivien Mura, directeur des technologies d'Orange Cyberdéfense. Orange Cyberdéfense accompagne une grande partie de la chaîne de valeur du numérique sur les différentes mises en conformité concernant NIS, Dora et prochainement le Cyber Resilience Act. Nous observons une hétérogénéité dans la maturité des différents maillons de la chaîne d'approvisionnement, dans la compréhension de la menace qui est pourtant de plus en plus transverse. Les attaquants sont animés par des objectifs très lucratifs et cherchent à s'infiltrer là où les portes sont ouvertes. L'hétérogénéité se constate également dans la capacité à faire face à ces différentes menaces. Les PME sont très ciblées, mais toutes n'ont pas les moyens de se mettre en conformité, ni même d'apporter une réponse sécuritaire aux différents scénarios de menace.

Quoi qu'il en soit, il n'y a pas d'alternative : il faudra investir collectivement, de manière homogène au sein de l'écosystème européen si nous voulons relever le défi de la

résilience. Cet investissement pourra d'ailleurs constituer un facteur de compétitivité s'il est mené à bon escient. Il doit s'accompagner effectivement d'une politique industrielle forte et de démarches pédagogiques pour expliquer le rapport entre les textes, mais aussi leur bien-fondé au regard des enjeux de sécurité. Certaines entreprises très matures le comprennent déjà, d'autres ont besoin de s'approprier ces textes pour pouvoir mener les actions correctement.

Il faut également améliorer la coopération entre le secteur public et le secteur privé, entre l'État et les tissus industriels, notamment être capable de déléguer davantage des missions d'intérêt public vers le secteur privé. En effet, de telles actions participent aussi à la compétitivité du secteur privé, des prestataires, des fournisseurs de solutions face à une concurrence qui est assez féroce. Enfin, la capacité à prendre des risques en matière d'investissement, notamment par des capitaux privés, dans des entreprises du numérique européennes sera clef. C'est aussi de cette manière que nous pourrons nous assurer d'une forme de résilience et de respect des valeurs européennes.

Mme Katuiscia Benloukil. Selon les chiffres d'Orange Cyberdéfense, environ 60 % à 70 % des attaques concernent les PME, tout simplement parce qu'elles sont les moins bien protégées. Le secteur de l'assurance oblige les entreprises, surtout les PME, à se protéger, à être couvertes en matière de cybertechnologie. Par exemple, une attaque par un rançongiciel ne sera peut-être pas prise en charge si la PME ne démontre pas qu'elle a tout mis en œuvre pour se protéger technologiquement.

Au même titre qu'Arnaud Dechoux, je suis intéressée par les obligations contractuelles qui pèseront sur les entreprises, c'est-à-dire l'obligation de moyens. Les PME sont inquiètes des attaques qu'elles reçoivent, mais s'interrogent aussi sur la manière de prioriser un budget et une superficie financière pour pouvoir se préparer d'un point de vue assurantiel et technologique à cette conformité.

M. le président Philippe Latombe. Certains d'entre vous ont évoqué la question des certifications, qui est revenue à plusieurs reprises lors des travaux sénatoriaux. Par exemple, les Belges ont adopté dans leur transposition la référence à un certain nombre de normes internationales. Lors de son audition, l'Anssi a indiqué qu'elle ne soutenait pas cette démarche. De votre côté, seriez-vous favorable à une transposition intégrant ce type de référence, de la même manière qu'en Belgique ?

M. Aurélien Lopez-Liguori (RN). Le gouvernement a publié il y a quelques jours une stratégie nationale pour la cybersécurité qui détaille en quatre piliers sa réponse, notamment celle du ministère de l'intérieur, face à la montée de la cybermenace. Mais elle ne mentionne à aucun moment la souveraineté, ni l'exclusion des entreprises étrangères des marchés sensibles, et encore moins une préférence nationale ou européenne dans les marchés publics. Elle n'évoque pas non plus une politique industrielle à long terme capable de faire émerger des géants français et européens face aux géants extra-européens.

Ces enjeux sont pourtant vitaux ; vous en êtes l'incarnation. En tant qu'entreprises françaises, vous êtes en effet des acteurs clés de notre cybersécurité nationale. Vous protégez des hôpitaux, des collectivités, des infrastructures vitales, et vous êtes en première ligne face à la cybermenace de notre pays. Il est donc de notre devoir de vous soutenir ; il y va de l'avenir de notre pays.

Comment pouvons-nous aujourd'hui vous aider à travers NIS 2, afin que les externalités positives, les retombées économiques générées puissent en premier lieu être récupérées par des acteurs français et européens ? Dans les certifications, faudrait-il insérer des critères d'immunité aux règles extraterritoriales, afin de vous favoriser ?

Mme Sabine Thillaye (Dem). Plusieurs d'entre vous nous ont invités à ne pas surtransposer. Il me semble que l'Allemagne a déjà transposé dans son droit national les directives européennes. Quelle est votre vision à ce propos ? Plus largement, regardez-vous la manière dont les autres États membres transposent ? Quels seront les points de vigilance pour nous permettre de garantir une concurrence loyale ?

M. Michaël Barthellemy. En réalité, dans leur transposition, les Belges ont effectué un copier-coller de l'ISO 27001. Cela ne me paraît pas nécessairement être une bonne approche, mais cette solution présente l'avantage de la rapidité. La Hongrie a également procédé à une transposition et a mis en place un système d'audit accordant une préférence nationale : l'audit doit être mené en Hongrie, par des sociétés hongroises, dûment autorisées par les autorités.

La « préférence nationale » est donc déjà mise en œuvre dans d'autres pays européens. C'est la raison pour laquelle nous souhaiterions que l'Anssi propose une forme de reconnaissance, un « tampon », sans qu'il soit forcément nécessaire de l'inscrire dans la loi. Cela permettrait, pendant une période donnée, d'être exempté de demandes d'audits complémentaires.

M. Vivien Mura. Je souhaite répondre à la proposition de M. Lopez-Liguori concernant l'intégration d'une immunité contre des lois à portée extraterritoriale dans des certifications. Comme tout autre risque cyber, les accès à ses propres données qui peuvent être jugés légitimes font partie de l'analyse de risque.

Ensuite, les différentes entités ont besoin d'être outillées pour pouvoir effectivement mettre en place ces protections si elles le jugent nécessaire. En ce sens, la certification de sécurité peut offrir ce moyen, en tout cas pour des niveaux élevés. Il revient donc aux autorités compétentes d'indiquer comment cela doit intervenir, plutôt à échelle européenne. En effet, comprendre comment il est possible de mettre en place des mesures de différentes natures contre ce type de risques et de menaces est compliqué. En outre, la démarche nécessite une forme d'expertise technique, juridique, organisationnelle. Enfin, la certification constitue probablement à ce titre l'un des meilleurs leviers.

M. Arnaud Dechoux. Je partage les propos de M. Barthellemy en matière de certification. Il faudrait sans doute établir un tableau d'équivalence clair entre ISO 27001 et les choix de la France.

Je n'ai pas lu les différents textes de transposition existant dans les autres pays de l'UE. Néanmoins, il conviendra sans doute de passer des accords de reconnaissance mutuelle, qui me semblent très importants. J'étais d'ailleurs assez surpris que ces modalités n'aient pas été prévues dès le départ dans la directive.

S'agissant de la souveraineté et de la préférence européenne, nous n'avons pas envie de tomber dans un certain fatalisme. Une telle préférence est probablement difficile à introduire dans la loi en France, mais cela devra sans doute passer par des dispositifs au niveau européen, afin de soutenir les PME de l'UE. Elle devra également se manifester par la

commande publique pour favoriser ces PME et l'innovation. Les Américains l'ont fait depuis longtemps ; cette démarche prendra plus de temps en Europe, mais nous devons agir de la sorte.

Mme Katuiscia Benloukil. La réflexion doit s'effectuer sur l'ensemble de la chaîne de la donnée, qui concerne non seulement nos offres de solutions technologiques de protection cyber, mais aussi les clouds souverains, qu'il faut privilégier. Je rappelle à ce titre que 80 % des logiciels utilisés aujourd'hui par les entreprises du monde entier sont américains. Il est ici question d'autonomie stratégique, dont les entreprises doivent aussi bénéficier.

Je rejoins donc les propos d'Arnaud Dechoux concernant la réglementation, la rédaction des textes de loi. Dans les commandes publiques, il est nécessaire de privilégier les éditeurs et les fournisseurs de solutions souveraines, qu'elles soient cloud ou cyber.

M. Aurélien Lopez-Liguori (RN). La position française concernant le projet de certification européenne pour les services de cloud (EUCS) risque de ne pas prévaloir. La présente transposition nous offre une occasion qui est peut-être historique. Ne faudrait-il pas trouver des solutions pour que l'effort, les externalités positives induites par NIS 2, profitent aux entreprises françaises et européennes ? Avez-vous des idées à partager dans ce domaine ? Je parlais de certification, mais peut-être existe-t-il également d'autres pistes.

M. le président Philippe Latombe. Faudrait-il profiter du texte pour adopter une définition du renseignement d'origine sources ouvertes (Osint) ? En effet, un certain nombre d'acteurs déplorent son absence et incitent le législateur à établir un cadre dans ce domaine. De son côté, l'Anssi nous a indiqué qu'elle ne voyait pas de raison particulière de légiférer sur le sujet. Qu'en pensez-vous ?

M. Éric Bothorel, rapporteur général. Je prolonge la question de M. Lopez-Liguori. Comment nous organisons-nous pour nous assurer que cette transposition se transforme en bienfaits pour l'écosystème cyber et non uniquement pour les cabinets d'avocats ou les sociétés de conseil qui ne manqueront pas de vendre des prestations de conformité ? Comment renforcer « l'équipe de France » du numérique, au-delà des effets d'aubaine dont profiteront certains ?

M. Michaël Barthellemy. À mon avis, il n'est pas nécessaire de formuler une définition de l'Osint. En revanche, lorsque nos chercheurs effectuent des recherches de failles lors de tests d'intrusion (*pentests*) il leur arrive de déceler des vulnérabilités *zero-day*. Lorsque nous entrons en relation avec le prestataire de la solution pour l'en informer, une fois sur deux, il nous rétorque qu'il n'effectuera pas de modifications et peut même nous menacer d'une action en justice si nous les publions. Dans ce cas, nous bénéficions du support de l'Anssi, qui vérifie que le travail a été mené dans les règles, même si cela ne nous offre pas de couverture juridique. Pendant les six à neuf mois où nous discutons avec l'éditeur de la solution afin qu'il effectue une correction, la vulnérabilité est exploitable dans le monde entier.

De son côté, la Belgique a inscrit dans sa loi la protection de sa recherche sur les vulnérabilités. Cela n'est pas le cas en France, où nous pouvons subir une action en justice sur deux éléments : la propriété intellectuelle et les droits d'auteur. En effet, lorsque nous décompilons du code, nous revenons au code original, qui relève des droits d'auteur. En

conséquence, nous souhaiterions que nos recherches puissent être protégées. Encore une fois, lorsque nous décelons une vulnérabilité, cela profite généralement à la communauté entière.

M. Thierry Racaud. Vous nous avez interrogés sur l'opportunité que peut présenter NIS 2. Les solutions et les produits de cybersécurité sont en très grande majorité américains, même s'il existe des solutions souveraines. Une filiale d'Airbus, Storm Shield, produit ainsi des solutions et des produits de cybersécurité qui sont estampillés par l'Anssi.

Ensuite, nous ne sommes pas en contact avec des cabinets d'avocats dans nos activités de conseil et d'audit auprès de la *supply chain* aéronautique. L'Anssi a mis en place cette labellisation de prestataire d'audit et de conseil à la cybersécurité (PACS). Des entreprises comme la nôtre, qui disposent de ce label, sont en mesure d'intervenir auprès des sociétés pour les auditer. Ce label fait foi et montre l'expertise de nos sociétés face à des concurrents qui pourraient venir de l'extérieur.

M. Vivien Mura. Je ne suis pas certain que la certification soit le bon levier pour activer la préférence européenne, si tant est que cela soit possible. En effet, il existe un problème de rapport et de nature entre l'objectif d'une certification – qui traite plutôt des aspects de sécurité – et les objectifs de politique industrielle, où il est possible d'agir dans le cadre du code des marchés publics, ou établir des préférences d'origine dans certains cas de figure, pour couvrir des usages sensibles.

De fait, la commande publique fait partie des leviers de politique industrielle les plus forts, comme nous pouvons le constater dans d'autres pays. En conséquence, il ne faut absolument pas négliger les autres leviers, bien plus évidents que ceux relevant purement de la sécurité.

M. le président Philippe Latombe. Monsieur Barthellemy, vous nous avez posé une question sur les *pentests*, que nous prenons en note, même si cet aspect est sans doute trop incident pour pouvoir être intégré dans le projet de loi.

M. Arnaud Dechoux. Le « label volontaire » a été ajouté à la loi. Il s'agit d'une avancée, mais le caractère volontaire doit être conservé en tant que tel : il ne doit pas devenir obligatoire et entraîner *de facto* un recours à des consultants, qui constituerait un risque économique assez important pour les start-up.

M. Olivier Bonnet de Paillerets. Je partage ce point de vue. Certaines sociétés de conseil se précipitent sur ce créneau, car elles y voient des éléments de croissance très importants. Il faut donc être très attentif à ce sujet. Enfin, s'agissant de la commande publique, si nous sommes leaders en France et dans certains pays européens, nous sommes très peu présents dans l'administration française.

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

La séance est levée à 16 heures 40

Membres présents ou excusés

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

Réunion du mercredi 4 juin 2025 à 15 h 30

Présents. - Mme Bénédicte Auzanot, M. Éric Bothorel, M. Mickaël Bouloux, M. Philippe Latombe, Mme Anne Le Hénanff, M. Aurélien Lopez-Liguori, M. Stéphane Rambaud, M. Aurélien Saintoul, Mme Sabine Thillaye

Excusé. - M. Laurent Mazaury