Texte d'intervention liminaire - Audition du jeudi 5 juin 2025
Commission spéciale chargée d'examiner le Projet de Loi
« Résilience des infrastructures critiques et Renforcement de la Cybersécurité »
Assemblée Nationale

Monsieur le Président, Monsieur le Rapporteur Général, Mesdames et Monsieur les Rapporteurs, Mesdames et Messieurs les députés,

Nous vous remercions de l'opportunité que vous nous offrez de présenter devant la représentation nationale notre analyse de ce projet de loi. 5 à 10 minutes c'est court, aussi n'insisterai-je que sur les points d'attention qui nous semblent majeurs.

Pour nous au CyberCercle, la transposition de ces trois textes européens dans notre droit à travers ce projet de loi représente une occasion unique de renforcer la cohérence, la lisibilité, la clarté et l'efficacité (avec comme préoccupation l'optimisation des coûts) de la réglementation en matière de cybersécurité et des politiques publiques qui y seront associées.

Notre intervention aura ainsi comme fil rouge la cohérence.

J'aborderai ici six points qui nous semblent particulièrement importants pour renforcer la cohérence à la fois au sein du projet de loi entre les différents dispositifs prévus par les trois textes, mais aussi la cohérence avec les textes et dispositifs existants.

Premier point : la nécessité d'une stratégie nationale

L'article 5bis introduit par le Sénat, qui pourrait être remis en cause par le gouvernement au prétexte que des stratégies plus globales sont en cours de rédaction, nous semble indispensable.

L'élaboration d'une stratégie inscrite dans la loi permettra à l'ensemble des acteurs concernés,
- d'une part, d'avoir régulièrement un cap et un cadre de référence dans lequel s'inscrire ;
- d'autre part, de mieux comprendre l'organisation, la coordination au sein de l'Etat et les responsabilités de chacun, y compris territoriales, visées par le gouvernement, et ainsi de coordonner dans un même cadre et vers les mêmes objectifs les actions de tous ;
- enfin, d'assurer la cohérence des dispositifs. La nécessité d'une stratégie nationale claire de cybersécurité a d'ailleurs été évoquée à plusieurs reprises lors de vos auditions précédentes, notamment celle des collectivités,

Cette stratégie permettra également au Parlement de contrôler et d'évaluer l'efficacité des mesures prises et de la dépense publique consacrée à la cybersécurité.
Afin d'optimiser sa rédaction et au-delà de simples concertations, il serait d'ailleurs pertinent qu'une commission réunissant les parties prenantes élabore cette stratégie, comme c'est le cas pour le Livre Blanc de la Défense et la Sécurité Nationale.

Deuxième point : la cohérence dans les acteurs impliqués.

Ainsi dans la mise en œuvre de NIS2, l'absence des ministères est inexplicable.

Au-delà de notre conviction que pour être efficace envers des secteurs d'activité par nature très différents les uns des autres, une approche par métiers est capitale pour faire de la cybersécurité un axe naturel des organisations - un volet de notre action, à Paris et sur les territoires, depuis bientôt quinze ans -, il s'agit là de mettre en cohérence les trois textes transposés quant au rôle des ministères coordonnateurs des secteurs d'activités concernés par REC, NIS 2 et DORA.

Ainsi, les quelques centaines d'opérateurs d'importance vitale visés au titre 1 du PJL sont identifiés et suivis par les ministères coordonnateurs du secteur d'activité auquel ils appartiennent.

Le même principe s'applique pour le titre 3 du PJL. Ce sont les autorités financières dont les ministères économiques et financiers qui suivent et contrôlent les quelques milliers d'acteurs visés par DORA.

Mais quand dans le titre 2 il s'agit de suivre les dizaines de milliers d'entités visées par NIS 2, c'est l'ANSSI seule qui dans le texte est en charge de l'ensemble. Les ministères étant au final exclus de tout le processus. Or, ce sont les ministères qui de fait connaissent le mieux les métiers, les dépendances et les conséquences d'une défaillance d'un opérateur, les conditions de résilience dans les secteurs d'activité dont ils ont la charge. Ajoutons que dans un objectif d'optimisation de l'action des acteurs et des moyens de l'Etat, le rôle des ministères relève du bon sens.

Il nous semble donc essentiel d'introduire les ministères coordonnateurs dans le titre 2 du projet de loi, au moins dans les 4 étapes du processus que sont :
1 - la validation et le complément éventuel des listes des entités essentielles et importantes (article 12),
2 - la définition des objectifs de sécurité et des référentiels d'exigences (articles 14 et 15),
3 - les contrôles (article 29)
et 4 - la commission des sanctions (article 36).

Si vous le souhaitez, nous pourrons revenir plus en détail sur ces points lors des questions.

Troisième point : la cohérence dans les objectifs de sécurité et les référentiels de mesures techniques et organisationnelles.

- Dans l'article 14 : Un décret fixe les objectifs de sécurité auxquels doivent se conformer les entités essentielles et entités importantes. Le « qui » définit les objectifs et « comment » ne sont pas précisés, alors que plus loin dans le même article ces éléments sont indiqués pour les référentiels d'exigence techniques et organisationnelles.

- Dans l'article 15 : Les entités qui mettent en œuvre tout autre référentiel reconnu équivalent par l'ANSSI (…) peuvent s'en prévaloir lors d'un contrôle. Il y a là une incohérence : ces référentiels équivalents devraient également, comme dans l'article 14, être définis par les métiers, d'autant plus si ces référentiels sont sectoriels, exigés par les marchés, ou issus d'autres réglementations s'imposant à eux.

Nous n'abordons pas ici le sujet des labels qui sera peut-être traité lors des questions.

- Enfin, dans son article 25 portant sur la normalisation, la directive NIS2 précise qu'« afin de favoriser la mise en œuvre convergente des mesures de gestion des risques en

matière de cybersécurité, « les États membres encouragent (…) le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information. ». Cet article qui nous semble important de la directive NIS 2 n'a pas été transposé.

C'est une occasion manquée d'une harmonisation au niveau européen ou international qui aurait soutenu la compétitivité de nos acteurs économiques. Au contraire, le renvoi de l'article 14 du PJL examiné par votre commission annonce un n^{ième} référentiel « franco-français » dont le coût de la conformité technique et organisationnel s'ajoute à celui du coût de la conformité aux normes que les entreprises doivent respecter pour gagner des marchés. D'autant que l'on pointe déjà des oppositions entre les prescriptions du projet de référentiel ANSSI et ce qu'imposent les actes d'exécution pris en application de DORA au niveau européen.

- Quatrième point : la cohérence et la clarté, voire l'égalité devant la loi, en ce qui concerne les contrôles.

L'article 29 qui traite de ce sujet pose que « Les contrôles de l'ANSSI peuvent prendre plusieurs formes dont celle d'audits réguliers et ciblés réalisés par un organisme indépendant désigné par l'ANSSI ». Le coût de cette forme de contrôle est à la charge des personnes contrôlées alors que pour les autres formes ils sont à la charge de l'ANSSI. Il nous semblerait pertinent d'encadrer les termes « réguliers » (quelle fréquence ?) et ce qu'est « un organisme indépendant désigné par l'ANSSI » - peut-on d'ailleurs parler d'indépendance dès lors qu'il y a sélection par l'ANSSI ? Pourquoi cette différence de traitement des entités ? Qui choisira parmi les différentes formes de contrôle celle qu'une entité devra subir et donc si ce contrôle sera ou non à sa charge ? Et toujours aucune mention des ministères.

- Cinquième point : la cohérence dans les sanctions.

Sur l'article 37 relatif aux sanctions, je citerais deux points sujets à questionnement.
La commission des sanctions peut prononcer :

- « une amende administrative pour les entités essentielles et importantes à l'exception des administrations et des collectivités territoriales et d'autres… » donc une amende uniquement pour les entreprises privées ;
- « en dernier recours, pour les entités essentielles, l'interdiction d'exercer des responsabilités de dirigeants dans ces entités jusqu'à ce que l'entité ait remédié au manquement - sauf pour les administrations. Pourquoi cette interdiction ne s'appliquerait-elle pas à l'administration ? De plus, comment appliquer cette interdiction à un élu d'une collectivité ?
  Pour plus de transparence et pour éviter d'avoir le sentiment qu'aucune sanction ne sera prononcée contre l'administration, cet article pourrait ainsi préciser les moyens utilisables par l'État tels qu'ouverts par l'avis du Conseil d'État du 6 juin 2024.

- Enfin, dernier point sur lequel nous nous permettons d'insister quant à la nécessité d'apporter de la cohérence au texte : l'exploitation de l'information relative à la menace non seulement par les entités visées par NIS 2 mais également par leurs prestataires,

Nous n'entrerons pas dans le cœur des débats sur le sujet qui agitent l'écosystème plus encore depuis quelques semaines. Nous ferons juste la constatation que l'article 45 du règlement DORA qui en constitue seul le pilier consacré au partage de l'information, donne un cadre à l'échange d'information entre les acteurs visés par DORA. Ne pas transposer l'article 29 prévu

dans la directive NIS 2 portant sur le même sujet introduit de fait une inégalité et une incohérence pour les entités soumises à DORA et à NIS 2.

*
* *

Pour conclure, et cela bouclera avec la nécessité d'élaborer une stratégie claire, cohérente, efficace soucieuse des impacts financiers, je voudrais citer le rapport d'activité 2024 publié par l'ANSSI le 28 avril dernier relatif aux parcours de cybersécurité dans le cadre du programme de France relance.

Même si ce rapport partiel ne permet pas d'évaluer réellement l'efficacité des 100 millions d'euros dépensés pour les 945 entités publiques sélectionnées parmi plus de 1600 candidatures — collectivités territoriales, établissements de santé, établissements publics —, il met en évidence les deux faits suivants :

- Initialement la « note cyber » moyenne des bénéficiaires de ce programme était de D+ (mauvais) ; ce qui veut dire que 13 ans d'empilement de réglementations s'imposant à la plupart de ces entités (RGS, PSSIE, RGPD, loi santé, eIDAS par exemple) n'ont pas permis d'élever leur niveau de cybersécurité.
- Sans réglementation supplémentaire, le niveau de cybersécurité de ces entités est passé de D+ à B (c'est à dire de mauvais à bon). Et ce pour un montant équivalent voire inférieur à celui annoncé pour NIS 2 si l'on fait le calcul sur la base des chiffres annoncés.

Lors d'une audition par votre Commission, les collectivités ont insisté sur ce point : c'est d'accompagnement dont elles ont besoin, pas de nouvelle réglementation qui, seule, n'apporte pas de maturité. Il en est de même pour les entreprises. Aussi, si nous comprenons le choix de la France de mettre les collectivités dans le cadre de cette loi devant la croissance de la menace, nous nous interrogeons sur le choix de soumettre autant de collectivités à NIS 2, et cela d'autant qu'il n'y a pas eu d'analyse d'impact financier les concernant.

Voilà Monsieur le Président, Monsieur le Rapporteur Général, Mesdames et Monsieur les Rapporteurs, Mesdames et Messieurs les députés, les points essentiels que souhaitait évoquer le CyberCercle.

Cette transposition est une opportunité de renforcer la cybersécurité et la résilience de notre pays en montant le niveau de maturité cyber des acteurs et en les embraquant dans une dynamique vertueuse.
Les questions qui se posent sont donc aujourd'hui :
- à quel niveau faut-il mettre le curseur ;
- comment éviter « la maison des fous » d'Astérix pour reprendre les termes du Directeur Général de l'ANSSI devant votre commission ;
- comment accompagner les acteurs par des politiques publiques adaptées dans un contexte budgétaire restreint.

Le Sénat a permis d'améliorer substantiellement le texte initial du gouvernement. En introduisant encore plus de cohérence entre les différentes parties du texte, votre commission spéciale pourrait faire émerger un texte encore plus pragmatique.

Je vous remercie.

Annexe

Extrait du règlement DORA
CHAPITRE VI
Dispositifs de partage d'informations
Article 45
Dispositifs de partage d'informations et de renseignements sur les cybermenaces
1. Les entités financières peuvent échanger entre elles des informations et des renseignements sur les cybermenaces, notamment des indicateurs de compromis, des tactiques, des techniques et des procédures, des alertes de cybersécurité et des outils de configuration, dans la mesure où ce partage d'informations et de renseignements :
a) vise à améliorer la résilience opérationnelle numérique des entités financières, notamment en les sensibilisant aux cybermenaces, en limitant ou en bloquant la capacité de propagation des cybermenaces, et en soutenant les capacités de défense, les techniques de détection des menaces et les stratégies d'atténuation ou les phases de réponse et de rétablissement ;
b) se déroule au sein de communautés d'entités financières de confiance ;
c) repose sur des dispositifs de partage des informations qui protègent la nature potentiellement sensible des informations partagées et qui sont régis par des règles de conduite dans le plein respect de la confidentialité des affaires, de la protection des données à caractère personnel conformément au règlement (UE) 2016/679 et des lignes directrices sur la politique de concurrence.
2. Aux fins du paragraphe 1, point c), les dispositifs de partage d'informations définissent les conditions à respecter pour y participer et, le cas échéant, précisent les modalités de participation des autorités publiques, et en quelle qualité elles peuvent être associées à ces dispositifs, les modalités de la participation des prestataires tiers de services TIC, ainsi que les aspects opérationnels de ce partage, y compris de l'utilisation de plateformes de TIC spécialisées.
3. Les entités financières notifient aux autorités compétentes leur participation aux dispositifs de partage d'informations visés au paragraphe 1 lors de la validation de leur adhésion ou, le cas échéant, la cessation de leur adhésion, lorsque celle-ci prend effet.

Extrait de la directive NIS 2
CHAPITRE VI
PARTAGE D'INFORMATIONS
Article 29
Accords de partage d'informations en matière de cybersécurité
1. Les États membres veillent à ce que les entités relevant du champ d'application de la présente directive et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente directive puissent échanger entre elles, à titre volontaire, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:
a) vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact ;
b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de

défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services. Cet échange est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

3. Les États membres facilitent la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 du présent article. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. Lorsqu'ils précisent la participation des autorités publiques à ces accords, les États membres peuvent imposer des conditions en ce qui concerne les informations mises à disposition par les autorités compétentes ou les CSIRT. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 7, paragraphe 2, point h).

4. Les États membres veillent à ce que les entités essentielles et importantes notifient aux autorités compétentes leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

5. L'ENISA fournit une assistance pour la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 par l'échange de bonnes pratiques et l'apport d'orientations.