N° 624
SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 13 mai 2026

PROPOSITION DE RÉSOLUTION EUROPÉENNE PORTANT AVIS MOTIVÉ

AU NOM DE LA COMMISSION DES AFFAIRES EUROPÉENNES,
EN APPLICATION DE L'ARTICLE 73 *OCTIES* DU RÈGLEMENT,

sur la **conformité** *au* **principe** *de* **subsidiarité** *et de* **proportionnalité** *de la* **proposition** *de* **règlement** *du* **Parlement européen** *et du* **Conseil relatif** *à l'***Agence** *de l'***Union européenne** *pour la* **cybersécurité** (**ENISA**), *au* **cadre européen** *de* **certification** *de* **cybersécurité** *et à la* **sécurité** *de la* **chaîne** *d'***approvisionnement** *des* **TIC**, *et abrogeant le* **règlement** (**UE**) *2019/881* (**règlement** *sur la* **cybersécurité** *2*) - *COM*(*2026*) *11 final et de la* **proposition** *de* **directive** *du* **Parlement européen** *et du* **Conseil** *modifiant la* **directive** (**UE**) *2022/2555 en ce qui concerne l'***introduction** *de* **mesures** *de* **simplification** *et l'***alignement** *sur* [*la* **proposition** *de* **règlement** *sur la* **cybersécurité 2**] - *COM*(*2026*) *13 final,*

PRÉSENTÉE

Par Mmes Catherine MORIN-DESAILLY et Audrey LINKENHELD,

Sénatrices

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Soulignant des **menaces cyber croissantes et de plus en plus complexes**, la Commission européenne a présenté le 20 janvier 2026 un **train de mesures destiné à renforcer la résilience et les capacités de l'Union européenne (UE) à faire face aux défis en matière de cybersécurité**.

Alors que, d'une part, les États membres font l'objet de cyberattaques et d'attaques hybrides ciblant incessamment leurs entreprises, leurs institutions démocratiques ainsi que des services essentiels, et que, d'autre part, ces attaques sont perpétrées par des groupes étatiques et/ou criminels usant de méthodes de plus en plus sophistiquées, amplifiées par l'intelligence artificielle (IA), la Commission entend **moderniser et renforcer le cadre juridique applicable dans l'UE**. Celui-ci est aujourd'hui essentiellement fondé sur le règlement sur la cybersécurité de 2019[1].

Le paquet présenté par la Commission le 20 janvier 2026, dit « cybersécurité 2 », est composé de **deux propositions d'actes législatifs** :

- une proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2), COM(2026) 11 final ;

- une proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2], COM(2026) 13 final.

---

[1] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).*

Au cœur des mesures proposées, **l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA, qui constitue le pivot de la cybersécurité en Europe, verrait ses prérogatives encore renforcées, au détriment des agences nationales compétentes**.

Or, une telle évolution ne serait pas sans poser de **difficultés au regard du principe de subsidiarité, comme l'avait déjà souligné la commission des affaires européennes en 2017**, à l'occasion de l'examen de la proposition de règlement sur la cybersécurité. Déjà, à l'époque, le Sénat avait adopté une résolution européenne portant avis motivé sur le respect du principe de subsidiarité[2].

À l'aune du renforcement des compétences de l'ENISA, des menaces grandissantes en matière de cybersécurité dans un contexte géopolitique incertain et des perspectives adverses nouvelles ouvertes par les modèles d'IA comme Claude Mythos d'Anthropic, **la commission des affaires européennes du Sénat souhaite rappeler la nécessité d'un exercice partagé de façon équilibrée et proportionnelle de la surveillance et de la mitigation des risques cyber entre l'Union européenne et les États membres**.

I – Les menaces en matière de cybersécurité vont croissant dans un contexte géopolitique incertain et du fait des risques nouveaux issus de l'IA

a) Des menaces cyber en forte évolution

La Commission européenne dresse le constat que **depuis l'adoption du règlement sur la cybersécurité en 2019, le panorama des menaces en la matière a fortement évolué** : les menaces cyber sont devenues plus hostiles – de surcroît dans un contexte géopolitique incertain –, et plus complexes du fait de leur caractère hybride. Les cyber-attaques ciblant les entreprises ou les institutions publiques, y compris dans leurs services essentiels, se sont multipliées et élargies aux citoyens, notamment à travers l'activité de rançongiciels.

---

[2] *Résolution européenne du Sénat n° 25 (2017-2028), du 6 décembre 2017, sur la conformité au principe de subsidiarité de la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) - COM (2017) 477 final.*

Ce bilan inquiétant se trouve aujourd'hui **renforcé par les perspectives adverses ouvertes par les systèmes d'IA** (rapidité des attaques au-delà des capacités humaines traditionnelles de défense, attaques par *prompt injection*, production et utilisation de contenus d'influence manipulés par l'IA, tels les *deepfakes*, etc.).

Dans son rapport concernant le panorama des cybermenaces en Europe en 2024[3], l'ENISA souligne que le paysage numérique européen se caractérise par une **augmentation sans précédent des cyberattaques, une professionnalisation croissante des acteurs malveillants, et une complexification des techniques exploitant les vulnérabilités logicielles, humaines et organisationnelles, avec des répercussions majeures sur la résilience des infrastructures critiques et la sécurité des citoyens**.

L'ENISA tire **cinq principales conclusions** de son analyse fondée sur l'étude de 11 079 incidents (dont 322 transfrontaliers), 19 754 vulnérabilités (dont 9,3 % critiques), et des sources ouvertes et de renseignement cyber (CTI) multiples :

- une **stabilité à un niveau très élevé des attaques pas rançongiciel** (*ransomeware*) : environ 1 000 incidents rapportés par trimestre ;

- une **explosion de certains logiciels malveillants** (*malwares)* dit « *infostealers* » (ou voleurs d'information), créés dans le but de dérober des informations critiques ou sensibles au sein des systèmes d'information qu'ils pénètrent, ainsi que des attaques sur les équipements mobiles souvent opérées via des services malveillants (MaaS). Ces attaques aboutissent à des vols massifs de données, voire à la compromission de chaînes d'approvisionnement ;

- une forte **hausse des techniques d'ingénierie sociales** comme les techniques de *phishing*, notamment ciblées (*pearphishing*, *smishing*, *vishing*), et d'**usurpation d'identité** (avec par exemple des faux profils sur les réseaux sociaux tels LinkedIn), à des fins de fraudes financières ou d'accès aux réseaux ;

- le **maintien à un niveau élevé des menaces sur la disponibilité** (attaques par saturation des infrastructures notamment, qui peuvent cibler des services publics critiques), y compris à des fins d'interférences électorales dans certains cas ;

---

[3] *Rapport "2024 Report on the State of the Cybersecurity in the Union", publié par l'ENISA le 3 décembre 2024.*

- des **campagnes d'influence et de manipulation de l'information, utilisant notamment l'IA** pour générer des contenus trompeurs (désinformations, *deepfakes*), pouvant atteindre les processus démocratiques.

Nonobstant des biais potentiels liés au sous-signalement des incidents, l'ENISA note que **l'année 2023-2024 a vu une hausse de près de 20 % par rapport à l'année précédente des incidents cyber qui lui ont été rapportés**. Pour les attaques sur les équipements mobiles ciblant notamment les applications bancaires et les systèmes de paiement, la hausse s'élève à près de 200 % par rapport à l'année précédente.

Concernant la France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) présente également, dans son panorama de la cybermenace en 2025[4], **un bilan national marqué par le maintien à un niveau élevé des menaces et attaques cyber à l'encontre de cibles françaises**, malgré une légère diminution comparativement à 2024, laquelle s'explique par les pics de signalements observés lors de la tenue des Jeux Olympiques et Paralympiques de Paris, entre les mois de mai et d'août 2024. En 2025, l'ANSSI a ainsi traité 3 586 événements de sécurité.

L'ANSSI fait en outre deux constats importants. D'une part, elle note en 2025 « l'émergence d'un brouillard technologique et organisationnel qui apparaît comme un levier d'action pour les acteurs étatiques et cybercriminels », entre lesquels la frontière s'érode, *via* « une collaboration plus étroite entre ces attaquants à travers le partage de capacités, mais aussi l'adoption croisée de pratiques qui jusqu'à présent, caractérisaient davantage certains plus que d'autres ». D'autre part, en 2025, quatre secteurs d'activité concentrent 76 % des incidents portés à la connaissance de l'ANSSI : l'éducation et la recherche (34 %), les ministères et les collectivités territoriales (24 %), la santé (10 %) et les télécommunications (9 %), ce qui **confirme la tendance forte du ciblage d'acteurs publics**, majoritaires dans ces secteurs[5].

L'ANSSI note enfin que des attaques informatiques menées à des fins d'espionnage sont le plus souvent menées contre des entités liées au périmètre gouvernemental ou fournissant des services essentiels, ou contre des individus qui constituent des cibles d'espionnage stratégique d'intérêt pour des États adverses et notamment des « attaquants réputés russes et chinois.

---

[4] Rapport intitulé « panorama de la cybermenace 2025 », publié par l'ANSSI, le 11 mars 2026.

[5] Il faut toutefois là encore noter un biais déclaratif, les entités publiques étant potentiellement plus enclines que les acteurs privés à déclarer les incidents cyber auxquels elles font face.

b) L'IA est porteuse de risques nouveaux et particulièrement aigus en matière de cybersécurité

Ainsi que le résume l'ANSSI, « l'IA générative et l'évolution rapide de ses usages représentent un potentiel accélérateur des capacités offensives associées aux cybermenaces, qui appelle à une réévaluation régulière de la menace. Toutefois, leur utilisation par des attaquants dépend de leurs objectifs et surtout de leur niveau de maturité ».

Sur ce plan, le dévoilement en mars 2026 du modèle *Claude Mythos* par la start-up américaine d'IA, Anthropic, risque de rapidement faire bouger les lignes. En effet, ***Claude Mythos*** **est un modèle d'IA capable de découvrir et d'exploiter des vulnérabilités dites « *zero-day* » dans les logiciels et systèmes informatiques, c'est-à-dire des failles de sécurité dans un logiciel qui ne sont pas connues publiquement et dont le fournisseur n'a pas connaissance**. D'autres modèles d'IA concurrents pourraient en outre aboutir aux mêmes résultats, voire à des menaces plus importantes encore.

Alors que plusieurs pays (États-Unis, Canada, Angleterre) ont entrepris dès avril 2026 des démarches pour préparer les institutions, notamment bancaires, à cette nouvelle menace, la Commission européenne n'a réagi aussi rapidement. Auditionnée le 16 avril 2026 par la commission des affaires juridiques (JURI) du Parlement européen, Mme Henna Virkkunen, vice-présidente exécutive de la Commission européenne chargée de la souveraineté technologique, de la sécurité et de la démocratie, n'a pas donné de détails quant aux mesures envisagées par l'UE à ce stade. Le commissaire européen à l'économie, M. Valdis Dombrovskis, a annoncé le 4 mai 2026 que des premiers échanges avaient eu lieu entre la Commission européenne et Anthropic et que la Commission européenne évaluait actuellement « les implications possibles à la lumière des politiques et de la législation de l'UE » en termes de risques cyber, notamment pour le secteur bancaire.

Face aux risques élevés auxquels est exposé le secteur bancaire, qui structure l'intégralité de nos économies aujourd'hui, **cette situation conduit à s'interroger sur la capacité de réponse rapide de l'UE aux menaces cyber**, dont l'évolution est elle-même très rapide, **et donc sur la pertinence d'une centralisation de la réponse européenne, que la Commission entend renforcer** à travers le paquet « cybersécurité 2 ».

II - La modernisation du cadre sur la cybersécurité proposée par la Commission européenne et son appréciation au regard du principe de subsidiarité

a) Présentation générale des propositions de la Commission européenne

Présentée le 20 janvier 2026, la proposition de la Commission, dite « règlement sur la cybersécurité 2 », entend :

- **renforcer la sécurité des chaînes d'approvisionnement** des technologies de l'information et de la communication (TIC) de l'UE, dans 18 secteurs jugés critiques, afin d'atténuer les dépendances et donc les risques non techniques ;

- **réformer le cadre européen de certification de cybersécurité** (ECCF) en révisant les procédures de certification pour les produits, services et processus TIC, dans l'objectif de les rendre plus efficaces et transparentes. *In fine*, il s'agit d'assurer la cybersécurité des produits fournis aux citoyens européens dès leur conception, grâce à un processus de certification simplifié ;

- **introduire des mesures de simplification** pour faciliter le respect des règles de cybersécurité de l'UE et des exigences en matière de gestion des risques, notamment pour les PME. Les mesures envisagées viendraient en complément du point de contact unique proposé dans le train de mesures omnibus sur le numérique[6], concernant le signalement des incidents de cybersécurité ;

- enfin, **réformer le mandat de l'Agence de l'Union européenne pour la cybersécurité (ENISA)**, notamment en accroissant ses prérogatives concernant la gestion des menaces en matière de cybersécurité.

---

[6] *Proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024].*

La **proposition de directive** présentée concomitamment par la Commission européenne décline la proposition de règlement. Elle entend réviser la directive (UE) 2022/2555 sur la sécurisation des réseaux et des systèmes d'information (ci-après la « directive SRI 2 »), **laquelle n'est toujours pas transposée en droit français, alors que la date limite pour sa transposition était fixée au 17 octobre 2024.**

Dans son principe, la proposition de règlement de la Commission européenne est accueillie favorablement par les parties prenantes dans l'objectif de renforcer la résilience de l'UE face aux menaces en matière de cybersécurité. La proposition de révision de la directive SRI 2 est quant à elle reçue de manière plus mitigée, notamment par les parties prenantes.

Eu égard à l'importance de la cybersécurité pour la sécurité nationale, la commission des affaires européennes du Sénat a souhaité approfondir l'examen de ces textes sur le plan de leur respect des principes de subsidiarité et de proportionnalité.

b) Appréciation générale des propositions du point de vue du respect des principes de subsidiarité et de proportionnalité

L'unique base légale sur laquelle se fonde la Commission européenne pour ces deux propositions est l'article 114 du traité sur le fonctionnement de l'Union européenne, qui porte sur le fonctionnement du marché unique.

Concernant le règlement cybersécurité 2, la Commission européenne justifie, dans son étude d'impact, l'intérêt européen à agir comme suit : « Les menaces en matière de cybersécurité transcendent les frontières nationales ; une approche unifiée est donc essentielle pour une réponse efficace. Une intervention au niveau de l'UE garantit une protection cohérente, renforce la compétitivité en assurant des conditions de concurrence équitables et facilite la libre circulation des services et produits numériques au sein du marché unique. L'harmonisation au niveau de l'UE réduit également les charges administratives grâce à des procédures de conformité simplifiées et rationalisées ».

Si une telle analyse apparaît fondée en première lecture, au regard du caractère par nature transfrontalier des menaces cyber, la cybersécurité, de par l'importance qu'elle revêt pour la sécurité des États membres, relève par plusieurs aspects de la souveraineté nationale.

Or, même si l'on peut admettre la nécessité de renforcer les capacités européennes en matière de cybersécurité, la Commission européenne propose de renforcer davantage les prérogatives de l'ENISA, une agence aux missions déjà larges, avec le risque à terme qu'elle se substitue aux États membres dans certaines fonctions, notamment à travers ses nouvelles compétences en matière de supervision transfrontalière.

Comme le soulignait déjà la commission des affaires européennes du Sénat en 2017, « la cybersécurité c'est autant la sécurité des États que celle des entreprises. En outre, quand ces dernières relèvent de secteurs sensibles comme par exemple l'énergie, les transports ou le secteur bancaire, c'est bien de sécurité nationale dont il s'agit ». Ce point avait également été soulevé dans la résolution européenne sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir - COM(2023) 209 final[7].

À cet égard, l'article 4 du traité sur l'Union européenne établit que l'UE « respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre ».

Le fait que la France se trouve aujourd'hui en défaut pour ne pas avoir encore transposé la directive SRI 2, alors que le délai de transposition est largement dépassé, ne change rien à cet enjeu de compétence.

De ce point de vue, **plusieurs mesures contenues dans les deux propositions présentées par la Commission**, présentées ci-après, **soulèvent des difficultés au regard du respect des principes de subsidiarité et de proportionnalité**.

c) La réforme du mandat de l'ENISA au détriment des capacités des États membres

La proposition de réforme du mandat de l'ENISA présentée par la Commission se traduirait par l'abrogation du règlement existant sur la cybersécurité (le règlement (UE) 2019/881), lequel serait remplacé par un nouveau règlement sur la cybersécurité (dit « règlement sur la cybersécurité

[7] *Voir notamment l'exposé des motifs de la proposition de résolution n° 207 (2023-2024) de Mmes Audrey LINKENHELD, Catherine MORIN-DESAILLY et M. Cyril PELLEVAT, devenue résolution du Sénat le 19 janvier 2024 (résolution n° 52 (2023-2024)).*

2 »). Pour autant, la Commission n'explique pas dans le détail les raisons du choix de l'option de « réforme complète du mandat de l'ENISA » en lieu et place d'amendements au mandat actuel défini par le règlement de 2019.

Bien que le véhicule réglementaire retenu soit inchangé (un règlement remplace un règlement), et comme l'avait déjà souligné le Sénat dans sa résolution portant avis motivé sur la proposition de règlement sur la cybersécurité, le 6 décembre 2017 : « Considérant que les propositions présentées par la Commission européenne tendent au renforcement des compétences de l'ENISA, au détriment des agences nationales, et dans la mesure où la sécurité nationale reste de la seule responsabilité de chaque État membre en application de l'article 4 du traité sur l'Union européenne, elles apparaissent susceptibles de porter atteinte aux principes de subsidiarité et de proportionnalité ».

Ainsi, la commission des affaires européennes estime que deux points concernant le renforcement des compétences de l'ENISA soulèvent des difficultés particulières.

Tout d'abord, le renforcement des prérogatives de l'ENISA dans la gouvernance des systèmes de certification en matière de cybersécurité ne laisse qu'une place résiduelle aux États membres.

Entendue par les rapporteures de la commission des affaires européennes le 29 avril 2026, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a rappelé l'importance pour les États membres de conserver des marges de manœuvre suffisantes pour assurer au niveau national un pilotage de leur stratégie de cybersécurité.

Il faut en effet rappeler que **la défense et la sécurité intérieure sont des prérogatives nationales et qu'il convient donc de préserver la responsabilité exclusive qui revient aux États membres en ces domaines**.

Aussi le renforcement du mandat de l'ENISA – jugé nécessaire et utile – **ne doit-il pas se faire au détriment des prérogatives des États membres**. Le rôle de l'ENISA doit rester cantonné à un soutien aux États membres, à la définition de standards techniques pour assurer que les États membres puissent appliquer les règles européennes et à l'animation des échanges d'information entre les États membres en matière de cybersécurité. En revanche, **l'ENISA ne saurait exercer des compétences relevant des autorités nationales**, notamment en matière de réponse aux incidents cyber, sans créer de la redondance et de la complexité, ni contrevenir au principe de subsidiarité.

Or, les rapporteures considèrent que le mandat élargi proposé pour l'ENISA s'aventure sur ce terrain, bien que de manière incomplète, en proposant un guichet unique, notamment pour la menace de rançongiciel.

Ainsi, elles s'opposent de manière ferme à l'article 16 de la proposition de règlement sur la cybersécurité 2 (COM(2026) 11 final). Cet article prévoit en effet une centralisation des vulnérabilités non corrigées au sein d'une base de données européenne gérée de manière centralisée par l'ENISA. En l'espèce, cette proposition nuit à la capacité des États membres à maîtriser de manière souveraine les failles affectant les infrastructures critiques nationales. Cette prérogative qui relève évidemment de la sécurité nationale doit rester opérée en France sous le contrôle strict de l'ANSSI.

Les rapporteures soulignent en outre que la logique de guichet unique, de surcroît pour un seul axe de la menace cyber, risquerait de **créer une confusion pour les entreprises et entités confrontées à des incidents de cybersécurité**, lesquels ne sauraient plus à qui s'adresser pour demander de l'aide et déclarer les incidents.

Au lieu de créer une simplification, cette proposition crée au contraire un risque d'inefficacité de la réponse proposée à l'incident cyber rencontré.

Par ailleurs, les rapporteures de la commission des affaires européennes jugent contestable le choix de centraliser l'expertise humaine au sein de l'ENISA, au détriment du renforcement de la main d'œuvre compétente dans les États membres. Conformément à son mandat élargi, l'ENISA est censée contribuer « à la croissance de la main-d'œuvre dans le domaine de la cybersécurité dans l'Union[8] ». Dès lors, l'augmentation envisagée des moyens de l'ENISA (+ 50 équivalents temps plein (ETP)) et la demande faite aux États membres de fournir chacun « au moins deux agents de liaison » en complément des experts nationaux détachés déjà mis à disposition auprès de l'ENISA par les agences nationales (article 58), apparaissent – au moins à court et moyen termes – de nature à amplifier le déficit de professionnels de la cybersécurité disponibles au sein des États membres. Ceci **apparaît contraire à l'objectif poursuivi**.

Enfin, les rapporteures de la commission des affaires européennes tiennent à souligner que **la Commission européenne n'a pas profité de la refonte complète du règlement sur la cybersécurité et du mandat de l'ENISA pour prendre acte de la complexité du cadre de gouvernance de la cybersécurité de l'UE** (réseau CSIRT[9], réseau EU-CyCLONe[10],

[8] *Article 4, point 5 « Objectifs de l'ENISA » de la proposition de règlement sur la cybersécurité 2.*
[9] *Équipe d'intervention en cas d'incident de sécurité informatique*.
[10] *Réseau européen des organisations de liaison en cas de crise cybernétique (*EU-CyCLONe*).*

CERT-UE[11], GECC[12], SCCG[13], groupe de coopération, réserve de cybersécurité, Europol…) et proposer sa simplification.

La commission des affaires européennes du Sénat avait pourtant déjà **dénoncé la complexification de l'architecture européenne de cybersécurité sans valeur ajoutée flagrante**, dans la proposition de résolution n° 207 (2023-2024) de Mmes Audrey LINKENHELD, Catherine MORIN-DESAILLY et M. Cyril PELLEVAT, sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir - COM(2023) 209 final, devenue résolution du Sénat le 19 janvier 2024.

Les rapporteures considèrent ainsi que la Commission européenne aurait pu saisir l'opportunité de réformer le mandat de l'ENISA pour rationaliser cette architecture, sans nuire aux prérogatives et aux ressources humaines des agences nationales compétentes en la matière.

d) Une évolution du cadre de certification qui risque de placer au second rang les États membres, en dépit de leur expertise de premier rang

Auditionnée par les rapporteures le 29 avril 2026, l'ANSSI – si elle se réjouit de certaines mesures permettant l'amélioration de l'efficacité du cadre de certification européen telles les dispositions visant à accélérer le processus d'édiction des schémas de certification (ajouts de délais, transparence du processus) – souligne néanmoins que certaines évolutions proposées en matière de certification (titre III) relèguent au second rang l'expertise des États membres et de leurs agences nationales compétentes.

Or, en la matière, ce sont les agences nationales qui exercent les missions opérationnelles relative à la prévention des risques cyber et à la remédiation des incidents. Elles bénéficient dès lors d'une expérience précieuse pour la définition des cadres de certification.

Cette analyse converge avec l'avis n° 2026-06 du 6 mai 2026 de la Commission supérieure du numérique et des postes (CSNP) sur la proposition de règlement sur la cybersécurité 2, rendu dans le cadre de la consultation publique ouverte par la Commission européenne jusqu'au 12 mai 2026. Cet avis du CSNP soulève plusieurs points d'attention quant

[11] *Service de cybersécurité pour les institutions, organes et organismes de l'Union*.
[12] *Groupe européen de certification de cybersécurité.*
[13] *Groupe de certification de cybersécurité des parties prenantes.*

aux évolutions proposées en matière de certification, y compris concernant la certification de sécurité des services *cloud*, dans la suite du projet de schéma européen de certification de sécurité des services *cloud* (EUCS), lequel se trouve aujourd'hui dans une impasse.

Les évolutions proposées pourraient ainsi limiter la possibilité pour la France de maintenir sa qualification SecNumCloud, qui ne saurait être remise en cause, sauf si un schéma européen de certification offrant un niveau de protection équivalent, notamment en termes d'immunité aux législations non européennes à portée extraterritoriale, était effectivement adopté au niveau européen.

Les rapporteures considèrent dès lors que l'expertise et l'expérience des États membres doivent être au cœur des dispositifs de l'ensemble des dispositifs et schémas de certification. Il en va de la proportionnalité de l'action européenne en la matière eu égard à la gouvernance des dispositifs de certifications, et du respect du principe de subsidiarité en lien avec les données ou secteurs qui peuvent relever de la défense et de la sécurité nationale.

Par conséquent, la commission des affaires européennes estime que la proposition de règlement ne respecte pas le principe de subsidiarité et a donc adopté la proposition de résolution portant avis motivé suivante :

LISTE DES PERSONNES ENTENDUES

Mercredi 29 avril 2026

- *Agence nationale de la sécurité des systèmes d'information (ANSSI)*

M. Vincent STRUBEL, directeur général, **Mme Juliette PÉRON**, conseillère**, M. Robin MASSON**, chargé de mission affaires politiques européennes et internationales.

CONTRIBUTION ÉCRITE

Secrétariat général des affaires européennes (SGAE).

Proposition de résolution européenne portant avis motivé sur la conformité au principe de subsidiarité et de proportionnalité de la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2) – COM(2026) 11 final et de la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2] – COM(2026) 13 final

① Vu l'article 88-6 de la Constitution,

② Vu l'article 73 *octies* du Règlement du Sénat,

③ Vu la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), au cadre européen de certification de cybersécurité et à la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881 (règlement sur la cybersécurité 2), du 20 janvier 2026, COM(2026) 11 final,

④ Vu la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne l'introduction de mesures de simplification et l'alignement sur [la proposition de règlement sur la cybersécurité 2], du 20 janvier 2026, COM(2026) 13 final,

⑤ Le Sénat émet les observations suivantes :

⑥ Le Sénat soutient l'objectif de renforcer la préparation et la résilience de la société et de l'économie de l'Union européenne en matière de cybersécurité, ainsi que l'objectif du développement et du renforcement de la main-d'œuvre dans le domaine de la cybersécurité ;

⑦ Cependant, il estime que – eu égard à l'importance de ces sujets pour la sécurité nationale – l'Union européenne doit veiller à agir de manière équilibrée et proportionnée ;

⑧ L'article 5 du traité sur l'Union européenne (TUE) stipule que l'Union européenne ne peut intervenir, en vertu du principe de subsidiarité, que « *si, et dans la mesure où les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union* » ; il précise qu'en application du principe de proportionnalité, « *le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités* » ; ceci implique d'examiner, non seulement si l'objectif de l'action envisagée peut être mieux réalisé au niveau européen, mais également si l'intensité de l'action entreprise n'excède pas la mesure nécessaire pour atteindre l'objectif que cette action vise à réaliser ;

⑨ L'article 5 du protocole n° 2 sur l'application des principes de subsidiarité et de proportionnalité annexé au TUE et au traité sur le fonctionnement de l'Union européenne (TFUE) prévoit que « *les raisons permettant de conclure qu'un objectif de l'Union peut être mieux atteint au niveau de celle-ci s'appuient sur des indicateurs qualitatifs et, chaque fois que c'est possible, quantitatifs* » ; ceci implique que les projets d'actes législatifs européens soient suffisamment motivés et circonstanciés ;

⑩ L'analyse d'impact qui précède la proposition de règlement COM(2026) 11 final précitée ne détaille pas les raisons du choix de l'option de « *réforme complète du mandat de l'ENISA* » en lieu et place d'amendements au mandat actuel défini dans le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité). En conséquence, la motivation de cette proposition apparaît présenter des limites et ne permet pas la bonne compréhension des modifications envisagées au mandat de l'ENISA ;

⑪ Le Sénat rappelle, comme il l'avait fait dans sa résolution n° 25 (2017-2028), du 6 décembre 2017, portant avis motivé sur la conformité au principe de subsidiarité de la proposition de règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité), COM (2017) 477 final, ainsi que dans sa résolution n° 52 (2023-2024), du 19 janvier 2024, sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, COM(2023) 209 final, que la cybersécurité, de par l'importance qu'elle revêt pour la sécurité des États membres, relève par plusieurs aspects de la souveraineté nationale ;

⑫ La cybersécurité ne peut relever uniquement de l'article 114 du TFUE, qui porte sur le fonctionnement du marché intérieur. Dès lors qu'elle est fondamentale du point de vue de la sécurité nationale, elle relève également de l'article 4 du TUE qui stipule que l'Union européenne « *respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale* » et précise : « *En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre* » ;

⑬ Pour atteindre les objectifs en matière de cyberrésilience et de renforcement des capacités des États membres, la Commission européenne propose de renforcer le mandat de l'ENISA (« *The European Union Agency for Cybersecurity* » – « *ENISA* »), ce qui implique le renforcement de ses moyens financiers et humains ; Pour ce faire, demande est faite aux États membres de fournir chacun « *au moins deux agents de liaison* » en complément des experts nationaux détachés déjà mis à disposition auprès de l'ENISA (article 58). Ces agents étant issus des autorités nationales compétentes, et face au déficit d'experts techniques de la cybersécurité, cette mesure est de nature à centraliser l'expertise humaine au sein de l'ENISA, au détriment du renforcement de la main d'œuvre compétente dans les États membres, ce qui apparaît contraire à l'objectif poursuivi ;

⑭ Le Sénat estime que les États membres doivent tous disposer de capacités techniques et opérationnelles suffisantes en matière de cybersécurité et qu'il est bienvenu que l'ENISA les aide dans cette démarche, sans toutefois que l'ENISA se substitue aux capacités opérationnelles des États membres. Or, l'obligation de transferts de ressources humaines et de compétences du niveau national vers l'ENISA est de nature à contrarier les efforts de construction de capacités opérationnelles au sein des agences nationales ;

⑮ Le Sénat estime que le renforcement du mandat de l'ENISA ne doit pas se faire au détriment des prérogatives des États membres établies par les traités. Le rôle de l'ENISA doit ainsi rester cantonné à un soutien aux États membres, à la définition de standards techniques pour assurer qu'ils puissent appliquer les règles européennes et à l'animation des échanges d'information entre les États membres en matière de cybersécurité. En revanche, le mandat de l'ENISA ne saurait porter sur des compétences exercées par les autorités nationales, sur le plan opérationnel, notamment en matière de réponse aux incidents cyber, sans créer de la redondance et de la complexité, ni contrevenir aux principes de subsidiarité et de proportionnalité ;

⑯ À cet égard, le Sénat juge disproportionnée la proposition de créer un guichet unique au niveau de l'ENISA, en particulier eu égard à la menace des rançongiciels ;

⑰ Le Sénat estime en outre que certaines évolutions proposées en matière de certification (titre III) relèguent au second rang l'expertise des États membres et de leurs agences nationales compétentes, alors même que ce sont elles qui disposent de la connaissance des enjeux de terrain. À cet égard, le Sénat considère que l'ENISA devrait se fonder sur des référentiels nationaux existants qui – à l'instar du référentiel « SecNumedu » en matière de formation – ont fait leurs preuves, plutôt que de chercher à réguler directement les marchés concernés ;

⑱ Concernant la certification de sécurité des services *cloud*, compte tenu de l'impasse dans laquelle se trouve aujourd'hui le projet de schéma européen de certification de sécurité des services *cloud* (« *The European Union Cloud Services Scheme* » – « *EUCS* »), le Sénat estime que les référentiels nationaux existants (la qualification SecNumCloud, délivrée par l'Agence nationale de la sécurité des systèmes d'information – ANSSI –, pour la France) doivent pouvoir être préservés et pérennisés, dans l'attente de l'adoption d'un schéma européen de certification de sécurité offrant au moins le même niveau de protection, notamment en termes d'immunité aux législations non européennes à portée extraterritoriale ;

*

⑲ En conséquence, pour ces motifs, le Sénat considère que les propositions d'actes législatifs COM(2026) 11 final et COM(2026) 13 final précitées ne sont pas conformes à l'article 5 du TUE et au protocole n° 2 sur l'application des principes de subsidiarité et de proportionnalité annexé au TUE et au TFUE.